Prezes
Rady Ministrów

Mateusz Morawiecki

Warszawa, dnia /elektroniczny znacznik czasu/

RM-0610-14-23
UD402

Pani Elżbieta WITEK
Marszałek Sejmu

Szanowna Pani Marszałek,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej.
Projekt ma na celu wykonanie prawa Unii Europejskiej.
Został notyfikowany Komisji Europejskiej 23 lutego 2023 r. pod numerem 2023/083/PL.
Wyznaczony okres tzw. *standstill* upływa 24 maja 2023 r. o godzinie 23.59.
Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem
Mateusz Morawiecki
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
wnioskodawca

tel. +48 (22) 694 75 00
dkpl@kprm.gov.pl
gov.pl/premier

Al. Ujazdowskie 1/3; 00-583
Warszawa

Projekt

U S T A W A

z dnia

o zwalczaniu nadużyć w komunikacji elektronicznej[1), 2), 3)]

Art. 1. Ustawa określa:

1) prawa i obowiązki przedsiębiorców telekomunikacyjnych związane z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich zwalczaniem;
2) kompetencje Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE", związane z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich zwalczaniem;
3) zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej;
4) zasady wnoszenia sprzeciwu przez podmiot posiadający tytuł prawny do domeny wobec wpisania domeny internetowej na listę ostrzeżeń;
5) obowiązki dostawcy poczty elektronicznej oraz podmiotu publicznego związane ze świadczeniem i korzystaniem z poczty elektronicznej w celu zapobiegania nadużyciom w komunikacji elektronicznej;
6) szczególne zasady przetwarzania informacji objętych tajemnicą telekomunikacyjną związane z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich zwalczaniem.

Art. 2. Określenia użyte w ustawie oznaczają:

---

1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej (Dz. Urz. UE L 321 z 17.12.2018, str. 36, Dz. Urz. UE L 334 z 27.12.2019, str. 164 oraz Dz. Urz. UE L 419 z 11.12.2020, str. 36).

2) Niniejsza ustawa została notyfikowana Komisji Europejskiej w dniu 23 lutego 2023 r. pod numerem 2023/083/PL, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), które wdraża postanowienia 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 (Dz. Urz. UE L 241 z 17.09.2015, str. 1).

3) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

1) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, w rozumieniu art. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666);
2) dostawca poczty elektronicznej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadzi, chociażby ubocznie, działalność zarobkową lub zawodową związaną ze świadczeniem poczty elektronicznej;
3) informacja adresowa – numer telefonu lub identyfikator użytkownika wysyłającego komunikat;
4) komunikat – komunikat w rozumieniu art. 2 pkt 17 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581);
5) lista ostrzeżeń – jawną listę ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzenia mieniem użytkowników internetu;
6) nadużycie w komunikacji elektronicznej – świadczenie lub korzystanie z usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści dla podmiotu dopuszczającego się nadużycia w komunikacji elektronicznej, innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej;
7) operator – operatora w rozumieniu art. 2 pkt 27 lit. b ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
8) poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie komunikatu z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), IMAP4 (Internet Message Access Protocol) lub innego standardu zapewniającego te same funkcje;
9) podmiot publiczny – podmiot, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
10) przedsiębiorca telekomunikacyjny – przedsiębiorcę w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
11) połączenie głosowe – połączenie ustanowione za pomocą publicznie dostępnej usługi komunikacji interpersonalnej pozwalające na dwukierunkową komunikację głosową;
12) sieć telekomunikacyjna – sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

13) tajemnica telekomunikacyjna – tajemnicę telekomunikacyjną, o której mowa w art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
14) uprawnione podmioty – uprawnione podmioty, o których mowa w art. 179 ust. 3 pkt 1 lit. a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
15) urządzenie telekomunikacyjne – urządzenie telekomunikacyjne w rozumieniu art. 2 pkt 46 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
16) usługa komunikacji interpersonalnej – usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej;
17) usługa komunikacji interpersonalnej niewykorzystująca numerów – usługę komunikacji interpersonalnej, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji;
18) usługa telekomunikacyjna – usługę telekomunikacyjną w rozumieniu art. 2 pkt 48 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
19) użytkownik – użytkownika w rozumieniu art. 2 pkt 49 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
20) użytkownik końcowy – użytkownika końcowego w rozumieniu art. 2 pkt 50 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Art. 3. 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności:
1) wysyłanie lub odbieranie komunikatów lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (generowanie sztucznego ruchu);
2) wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania (smishing);

3) nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania (CLI spoofing);
4) nieuprawnione modyfikowanie informacji adresowej uniemożliwiające lub istotnie utrudniające ustalenie przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu informacji adresowej, przy użyciu której nastąpiło wysłanie komunikatu (nieuprawniona zmiana informacji adresowej).

2. Przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.

Art. 4. 1. CSIRT NASK na podstawie krótkich wiadomości tekstowych (SMS) otrzymanych od odbiorców oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów monitoruje występowanie smishingu.

2. CSIRT NASK na podstawie wyników monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu, zwany dalej „wzorcem wiadomości”.

3. CSIRT NASK zapewnia funkcjonowanie systemu teleinformatycznego służącego do udostępniania i przekazywania informacji o wystąpieniu smishingu wraz ze wzorcem wiadomości oraz jest administratorem danych przetwarzanych w tym systemie.

4. CSIRT NASK za pośrednictwem systemu teleinformatycznego zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi UKE i przedsiębiorcom telekomunikacyjnym.

5. CSIRT NASK za pośrednictwem systemu teleinformatycznego przekazuje przedsiębiorcy telekomunikacyjnemu informacje o występowaniu smishingu wraz ze wzorcem wiadomości.

6. Podmioty, o których mowa w ust. 4, w celu wymiany informacji są obowiązane do korzystania z systemu.

7. Wzorzec wiadomości, o którym mowa w ust. 2, CSIRT NASK udostępnia na swojej stronie internetowej, nie wcześniej niż 14 dni i nie później niż 21 dni od dnia jego przekazania przedsiębiorcy telekomunikacyjnemu w sposób, o którym mowa w ust. 5.

8. CSIRT NASK, w przypadku gdy uzna, że:

1) treść zawarta we wzorcu wiadomości nie stanowi smishingu lub
2) niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zgodnych ze wzorcem wiadomości

– niezwłocznie informuje o tym podmioty, o których mowa w ust. 4, oraz zamieszcza na swojej stronie internetowej informacje o okresie, w jakim wzorzec wiadomości obowiązywał.

9. CSIRT NASK przetwarza dane pozyskane w związku z monitorowaniem występowania smishingu na zasadach określonych w art. 39 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 5. Przedsiębiorca telekomunikacyjny po otrzymaniu informacji, o której mowa w art. 4 ust. 5 lub 8, niezwłocznie:

1) blokuje krótkie wiadomości tekstowe (SMS) zawierające treści zawarte we wzorcu wiadomości, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (SMS);
2) zaprzestaje blokowania krótkich wiadomości tekstowych (SMS) w przypadku uznania, że treść zawarta we wzorcu wiadomości nie nosi znamion smishingu lub niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zawierających treści wskazane we wzorcu wiadomości.

Art. 6. 1. Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec zablokowania, o którym mowa w art. 5 pkt 1.

2. Sprzeciw zawiera:

1) pełną treść krótkiej wiadomości tekstowej (SMS);
2) uzasadnienie wyjaśniające, dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu;
3) wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS);
4) dane identyfikujące nadawcę:
   a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych,

b) nazwę (firmę) podmiotu, adres siedziby, numer z właściwego rejestru – w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej,

c) imię i nazwisko osoby uprawnionej do reprezentowania nadawcy wraz z upoważnieniem – jeżeli dotyczy.

3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się na adres do doręczeń elektronicznych Prezesa UKE.

4. Sprzeciw niespełniający wymagań, o których mowa w ust. 2 i 3, pozostawia się bez rozpoznania.

Art. 7. 1. Prezes UKE:

1) rozpatruje sprzeciw, w terminie 14 dni od dnia jego otrzymania oraz

2) niezwłocznie informuje nadawcę krótkiej wiadomości tekstowej (SMS) o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył nadawca krótkiej wiadomości tekstowej (SMS), wnosząc sprzeciw.

2. Prezes UKE, rozpatrując sprzeciw:

1) uwzględnia sprzeciw, jeżeli treść krótkiej wiadomości tekstowej (SMS) zawierająca treści wskazane we wzorcu wiadomości nie wyczerpuje znamion smishingu, albo

2) nie uwzględnia sprzeciwu, jeżeli treść krótkiej wiadomości tekstowej (SMS) zawierająca treści wskazane we wzorcu wiadomości wyczerpuje znamiona smishingu.

3. W przypadku uwzględnienia sprzeciwu, Prezes UKE nakazuje CSIRT NASK niezwłoczną, nie później niż w terminie 3 dni od dnia uwzględnienia sprzeciwu, zmianę wzorca wiadomości w taki sposób, aby krótka wiadomość tekstowa (SMS) o treści, o której mowa w art. 6 ust. 2 pkt 1, nie była blokowana.

4. Prezes UKE może pisemnie upoważnić pracownika Urzędu Komunikacji Elektronicznej do wykonywania czynności, o których mowa w ust. 1–3.

5. Do postępowania w sprawie rozpatrzenia sprzeciwu nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego (Dz. U. z 2022 r. poz. 2000 i 2185).

Art. 8. 1. Przedsiębiorca telekomunikacyjny może blokować krótkie wiadomości tekstowe (SMS), zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości, o którym mowa w art. 4 ust. 5, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich krótkich wiadomości tekstowych (SMS).

2. Przedsiębiorca telekomunikacyjny może blokować wiadomości multimedialne (MMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania. Blokowanie odbywa się za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich wiadomości.

Art. 9. W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo ukrywa identyfikację numeru wywołującego dla użytkownika końcowego.

Art. 10. 1. Prezes UKE prowadzi, przy pomocy systemu teleinformatycznego, jawny wykaz numerów służących wyłącznie do odbierania połączeń głosowych i udostępnia ten wykaz w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

2. Prezes UKE dokonuje wpisu numeru do wykazu, o którym mowa w ust. 1, na wniosek:

1) banku, w rozumieniu art. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2022 r. poz. 2324, 2339, 2640 i 2707 oraz z 2023 r. poz. 180),
2) firmy inwestycyjnej, w rozumieniu art. 3 pkt 33 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2022 r. poz. 1500, 1488, 1933, 2185 i 2640 oraz z 2023 r. poz. 180),
3) funduszu inwestycyjnego, w rozumieniu art. 3 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (Dz. U. z 2022 r. poz. 1523, 1488, 1933, 2185 i 2640),
4) instytucji płatniczej, w rozumieniu art. 2 pkt 11 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2022 r. poz. 2360 i 2640),
5) jednostki sektora finansów publicznych, o której mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, z późn. zm.[4)]),
6) Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej,
7) oddziału instytucji kredytowej, w rozumieniu art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,

---

4) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1692, 1725, 1747, 1768, 1964 i 2414.

8) spółdzielczej kasy oszczędnościowo-kredytowej, o której mowa w art. 1 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2022 r. poz. 924, z późn. zm.[5)]),

9) towarzystwa funduszy inwestycyjnych, w rozumieniu art. 38 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi,

10) zakładu reasekuracji, o którym mowa w art. 6 ust. 2 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2022 r. poz. 2283 i 2640),

11) zakładu ubezpieczeń, o którym mowa w art. 6 ust. 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej

– w zakresie wykorzystywanych przez te podmioty numerów.

3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykazu, o którym mowa w ust. 1, numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego wyłącznie na potrzeby własnego biura obsługi klientów lub infolinii.

4. Wniosek, o którym mowa w ust. 2 i 3, zawiera:

1) dane wnioskodawcy:
   a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych,
   b) nazwę (firmę) wnioskodawcy, adres siedziby, numer z właściwego rejestru w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej,
   c) imię i nazwisko osoby uprawnionej do reprezentowania wnioskodawcy wraz z upoważnieniem – jeżeli dotyczy;
2) wskazanie numeru, który ma służyć wyłącznie do odbierania połączeń głosowych;

5. Do wniosku, o którym mowa w ust. 2 i 3, dołącza się dokument potwierdzający prawo do dysponowania numerem.

6. W przypadku gdy wniosek, o którym mowa w ust. 2 i 3, nie spełnia wymagań, o których mowa w ust. 4, Prezes UKE wzywa wnioskodawcę do uzupełnienia wniosku w terminie 7 dni od dnia otrzymania wezwania pod rygorem pozostawienia wniosku bez rozpoznania.

7. Prezes UKE dokonuje wpisu numeru do wykazu, o którym mowa w ust. 1, w terminie 5 dni od dnia otrzymania wniosku spełniającego wymagania, o których mowa w ust. 4 i 5.

8. Wpis do wykazu, o którym mowa w ust. 1, jest czynnością materialno-techniczną.

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1358, 1488, 1933, 2339 i 2640 oraz z 2023 r. poz. 180.

9. Prezes UKE pozostawia wniosek o wpis do wykazu, o którym mowa w ust. 1, bez rozpoznania, jeżeli wniosek został złożony przez podmiot nieuprawniony albo dotyczy on numeru niewykorzystywanego przez wnioskodawcę. Prezes UKE niezwłocznie informuje wnioskodawcę o pozostawieniu wniosku bez rozpoznania.

10. Wnioskodawca, który złożył wniosek, o którym mowa w ust. 2 i 3, lub podmiot, który aktualnie korzysta z numeru wpisanego do wykazu, o którym mowa w ust. 1, może w każdym czasie złożyć wniosek o wycofanie numeru z wykazu.

11. Do wniosku o wycofanie numeru z wykazu przepisy ust. 4 i 5 stosuje się odpowiednio.

12. W przypadku, o którym mowa w ust. 10, Prezes UKE niezwłocznie, jednak nie później niż w terminie 5 dni od dnia otrzymania wniosku o wycofanie numeru z wykazu, o którym mowa w ust. 1, wykreśla go z tego wykazu.

13. Wniosek, o którym mowa w ust. 2, 3 i 10, opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE na adres do doręczeń elektronicznych Prezesa UKE.

14. Wniosek niespełniający wymagań, o których mowa w ust. 13, pozostawia się bez rozpoznania.

15. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu numeru do wykazu, o którym mowa w ust. 1, blokuje połączenia przychodzące do jego sieci z wykorzystaniem numeru wpisanego do tego wykazu.

16. Przedsiębiorca telekomunikacyjny zaprzestaje blokowania tego numeru w terminie 3 dni od dnia wykreślenia z wykazu.

Art. 11. Wykaz, o którym mowa w art. 10 ust. 1, obejmuje:

1) wskazanie numeru służącego wyłącznie do odbierania połączeń głosowych;
2) datę wpisania numeru, o którym mowa w pkt 1, do wykazu;
3) datę wykreślenia numeru, o którym mowa w pkt 1, z wykazu.

Art. 12. 1. W celu realizacji obowiązków, o których mowa w art. 9, przedsiębiorca telekomunikacyjny stosuje środki organizacyjne i techniczne służące monitorowaniu, wykrywaniu oraz wymianie informacji o CLI spoofing, a także blokowaniu połączenia głosowego albo ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego.

2. Dostawca publicznie dostępnych usług telekomunikacyjnych świadczący usługi telekomunikacyjne dla co najmniej 50 000 abonentów, będący jednocześnie operatorem, może

zawrzeć z Prezesem UKE porozumienie określające szczegółowe środki organizacyjne i techniczne, które będzie stosował przy realizacji obowiązków, o których mowa w art. 9.

3. Zawarcie porozumienia i jego prawidłowe wykonywanie stanowi spełnienie przez operatora będącego stroną porozumienia obowiązku podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie w zakresie, o którym mowa w art. 3 ust. 1 pkt 3.

4. Operator prawidłowo wykonujący porozumienie, o którym mowa w ust. 2, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem zastosowanych środków organizacyjnych i technicznych, o których mowa w ust. 1.

5. Prezes UKE kontroluje prawidłowość stosowania środków organizacyjnych i technicznych określonych w porozumieniu, o którym mowa w ust. 2. Do kontroli stosuje się przepisy działu X rozdziału 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

6. Dla przedsiębiorców telekomunikacyjnych innych niż określeni w ust. 2 Prezes UKE może wydać rekomendacje określające szczegółowe środki organizacyjne i techniczne służące realizacji obowiązków, o których mowa w art. 9. Rekomendacje są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa UKE.

7. Przedsiębiorca telekomunikacyjny inny niż określony w ust. 2, prawidłowo stosujący środki organizacyjne i techniczne określone w rekomendacjach, o których mowa w ust. 6, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem wprowadzenia środków.

Art. 13. 1. W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe, oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich mieniem, między Prezesem UKE, ministrem właściwym do spraw informatyzacji, Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym oraz przedsiębiorcą telekomunikacyjnym lub przedsiębiorcami telekomunikacyjnymi może zostać zawarte porozumienie dotyczące prowadzenia listy ostrzeżeń oraz uniemożliwienia dostępu do tych stron.

2. W przypadku zawarcia porozumienia podmiotem odpowiedzialnym za prowadzenie listy jest CSIRT NASK.

3. Na listę ostrzeżeń są wpisywane domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i doprowadzenie do wyłudzenia ich danych lub niekorzystnego rozporządzenia mieniem.

4. Każdy może zgłosić domenę internetową mogącą służyć do wyłudzeń danych i niekorzystnego rozporządzania mieniem do CSIRT NASK. Zgłoszenie domeny internetowej może zawierać uzasadnienie.

5. CSIRT NASK z inicjatywy własnej lub po otrzymaniu zgłoszenia wpisuje domenę internetową na listę ostrzeżeń, jeżeli spełnia ona przesłanki określone w ust. 3.

6. CSIRT NASK udostępnia na stronie podmiotowej Biuletynu Informacji Publicznej Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego informację określającą sposób dokonywania zgłoszeń.

7. Porozumienie określa co najmniej zasady współpracy stron porozumienia.

8. Przedsiębiorca telekomunikacyjny będący stroną porozumienia może uniemożliwić użytkownikom internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę ostrzeżeń, przez ich usunięcie z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych służących do zamiany nazw domen internetowych na adresy IP.

9. W przypadku skorzystania z uprawnienia, o którym mowa w ust. 8, przedsiębiorca telekomunikacyjny przekieruje połączenia odwołujące się do nazw domen internetowych wpisanych na listę ostrzeżeń do strony internetowej prowadzonej przez CSIRT NASK zawierającej informację skierowaną do użytkowników internetu zawierającą w szczególności informacje o lokalizacji listy ostrzeżeń, wpisaniu szukanej nazwy domeny internetowej na listę ostrzeżeń oraz o możliwej próbie wyłudzenia danych lub niekorzystnego rozporządzania mieniem.

Art. 14. 1. Podmiot posiadający tytuł prawny do domeny internetowej wpisanej na listę ostrzeżeń może wnieść do Prezesa UKE sprzeciw wobec wpisania domeny internetowej na listę ostrzeżeń.

2. Sprzeciw zawiera:

1) wskazanie domeny internetowej, której dotyczy;
2) uzasadnienie wyjaśniające, dlaczego wpisanie domeny na listę ostrzeżeń było niezasadne;
3) dane identyfikujące podmiot posiadający tytuł prawny do domeny internetowej:
   a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych,
   b) nazwę (firmę) podmiotu, adres siedziby, numer z właściwego rejestru – w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej,

c) imię i nazwisko osoby uprawnionej do reprezentowania podmiotu posiadającego tytuł prawny do domeny internetowej wraz z upoważnieniem – jeżeli dotyczy.

3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się na adres do doręczeń elektronicznych Prezesa UKE.

4. Sprzeciw niespełniający wymagań, o których mowa w ust. 2 i 3, pozostawia się bez rozpoznania.

Art. 15. 1. Prezes UKE:

1) rozpatruje sprzeciw w terminie 14 dni od dnia jego otrzymania oraz
2) niezwłocznie informuje podmiot wnoszący sprzeciw o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył podmiot, wnosząc sprzeciw.

2. Prezes UKE, rozpatrując sprzeciw:

1) uwzględnia sprzeciw, jeżeli domena internetowa nie służy do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników internetu;
2) nie uwzględnia sprzeciwu, jeżeli domena internetowa służy do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników internetu.

3. W przypadku uwzględnienia sprzeciwu Prezes UKE nakazuje CSIRT NASK niezwłoczne, nie później niż w terminie 3 dni od dnia uwzględnienia sprzeciwu, usunięcie domeny internetowej z listy ostrzeżeń.

4. Prezes UKE może pisemnie upoważnić pracownika Urzędu Komunikacji Elektronicznej do wykonywania czynności, o których mowa w ust. 1–3.

5. Do postępowania w sprawie rozpatrzenia sprzeciwu nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego.

Art. 16. 1. Prezes UKE może, gdy jest to uzasadnione ochroną użytkowników końcowych przed nadużyciami w komunikacji elektronicznej, nakazać przedsiębiorcy telekomunikacyjnemu, w drodze decyzji, zablokowanie dostępu do numeru lub usługi w terminie nie krótszym niż 6 godzin od momentu jej ogłoszenia oraz nałożyć obowiązek wstrzymania pobierania opłat za połączenia lub usługi zrealizowane po upływie tego terminu.

2. Decyzja, o której mowa w ust. 1, może być ogłoszona ustnie przedsiębiorcy telekomunikacyjnemu. Decyzja ogłoszona ustnie jest doręczana stronie na piśmie w terminie 14 dni od dnia jej ogłoszenia.

3. Decyzji, o której mowa w ust. 1, nadaje się rygor natychmiastowej wykonalności.

4. Do postępowania w sprawie wydania decyzji, o której mowa w ust. 1, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego, z wyjątkiem art. 107–113 oraz działu II rozdziału 12 i 13, które stosuje się odpowiednio.

Art. 17. 1. Dostawca poczty elektronicznej:

1) dla co najmniej 500 000 użytkowników poczty lub

2) dla podmiotu publicznego

– przy świadczeniu poczty elektronicznej ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail).

2. Podmiot publiczny jest obowiązany do korzystania z poczty elektronicznej wykorzystującej mechanizmy, o których mowa w ust. 1.

3. Prezes UKE może przeprowadzić kontrolę:

1) wykonywania obowiązku, o którym mowa w ust. 1, przez dostawcę poczty elektronicznej oraz

2) wykonywania obowiązku, o którym mowa w ust. 2, przez podmiot publiczny.

4. Do kontroli, o której mowa w ust. 3, stosuje się przepisy działu X rozdziału 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

5. CSIRT NASK udostępnia 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, o których mowa w ust. 1.

6. Dostawca poczty elektronicznej dla podmiotu publicznego oferuje pocztę elektroniczną umożliwiającą stosowanie metod uwierzytelniania wieloskładnikowego.

Art. 18. 1. Przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji informacji o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją:

1) obowiązku, o którym mowa w art. 5,

2) uprawnienia, o którym mowa w art. 8

– w zakresie umożliwiającym rozpatrzenie reklamacji, o której mowa w art. 106 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

2. Przedsiębiorca telekomunikacyjny przechowuje informacje, o których mowa w ust. 1, przez okres 12 miesięcy liczony od dnia, w którym usługa miała być wykonana, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu.

Art. 19. 1. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej.

2. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać komunikat w celu identyfikacji, zapobiegania i zwalczania smishingu oraz wiadomości multimedialnych (MMS), o których mowa w art. 8 ust. 2.

3. Przedsiębiorca telekomunikacyjny może przetwarzać:

1) treści krótkich wiadomości tekstowych (SMS),
2) treści wiadomości multimedialnych (MMS) oraz
3) informacje o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku, o którym mowa w art. 5 i art. 9, lub uprawnienia, o którym mowa w art. 8

– w celu realizacji obowiązku, o którym mowa w art. 3 ust. 2, art. 5 i art. 9, oraz realizacji uprawnienia, o którym mowa w art. 8, a także w celach związanych z dochodzeniem roszczeń.

4. Przetwarzanie, o którym mowa w ust. 3, jest dopuszczalne tylko do końca okresu, w którym jest możliwe dochodzenie roszczeń.

5. Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych przepisu art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[6)]), zwanego dalej „rozporządzeniem 2016/679”, nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.

6. Przedsiębiorca telekomunikacyjny może wykonać obowiązek, o którym mowa w art. 14 ust. 1 i 2 rozporządzenia 2016/679, przez udostępnienie informacji, o których mowa

---

[6)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

w tych przepisach, na swojej stronie internetowej lub przez umieszczenie stosownych informacji w miejscach widocznych w siedzibie lub miejscu działania administratora danych osobowych, w zakresie, w jakim dotyczy to danych osobowych pozyskanych w ramach identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.

Art. 20. 1. Przedsiębiorca telekomunikacyjny, który dokonuje następujących nadużyć w komunikacji elektronicznej:

1) generowania sztucznego ruchu,
2) smishingu,
3) CLI spoofingu,
4) nieuprawnionej zmiany informacji adresowej

– podlega karze pieniężnej.

2. Jeżeli czyn będący nadużyciem, o którym mowa w ust. 1, wyczerpuje jednocześnie znamiona przestępstwa, w stosunku do przedsiębiorcy telekomunikacyjnego będącego osobą fizyczną stosuje się wyłącznie przepisy o odpowiedzialności karnej.

3. Na przedsiębiorcę telekomunikacyjnego, który nie wypełnia obowiązków, o których mowa w:

1) art. 5,
2) art. 9,
3) art. 10 ust. 15 lub 16

– może zostać nałożona kara pieniężna, jeżeli przemawia za tym zakres lub charakter naruszenia.

4. Na dostawcę poczty elektronicznej, który nie wypełnia obowiązków, o których mowa w art. 17 ust. 1, może zostać nałożona kara pieniężna, jeżeli przemawia za tym zakres lub charakter naruszenia.

5. Kara pieniężna, o której mowa w ust. 1–4, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

6. Niezależnie od kary pieniężnej, o której mowa w ust. 3, Prezes UKE może, w drodze decyzji, nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop wypoczynkowy.

7. Prezes UKE może, w drodze decyzji, nałożyć karę pieniężną na kierownika podmiotu publicznego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 17 ust. 2. Kara pieniężna nakładana jest w wysokości do jednokrotności przeciętnego wynagrodzenia w gospodarce narodowej, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego, w ostatnim komunikacie, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504, 1504 i 2461).

8. Od decyzji Prezesa UKE w sprawie nałożenia kary pieniężnej przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

9. Kary pieniężne podlegają egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym.

Art. 21. 1. Karę pieniężną, o której mowa w art. 20 ust. 1, 3 i 4, nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.

2. W przypadku gdy podmiot w roku kalendarzowym poprzedzającym rok nałożenia kary pieniężnej nie osiągnął przychodu albo osiągnął przychód w wysokości nieprzekraczającej 500 000 zł, Prezes UKE, nakładając karę pieniężną, uwzględnia średni przychód osiągnięty przez podmiot w 3 kolejnych latach kalendarzowych poprzedzających rok nałożenia kary pieniężnej.

3. W przypadku gdy podmiot nie osiągnął przychodu w okresie, o którym mowa w ust. 2, albo gdy przychód podmiotu w tym okresie nie przekracza 500 000 zł, Prezes UKE może nałożyć na podmiot karę pieniężną w wysokości nieprzekraczającej 15 000 zł.

4. W przypadku gdy przed wydaniem decyzji o nałożeniu kary pieniężnej podmiot nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary pieniężnej, Prezes UKE, nakładając karę pieniężną, uwzględnia:

1) przychód osiągnięty przez podmiot w roku kalendarzowym poprzedzającym ten rok;
2) w przypadku, o którym mowa w ust. 2 – średni przychód osiągnięty przez podmiot w 3 kolejnych latach kalendarzowych poprzedzających ten rok; przepis ust. 3 stosuje się odpowiednio.

5. W przypadku gdy podmiot powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu, o którym mowa w ust. 1, Prezes UKE

uwzględnia przychód osiągnięty przez te podmioty w roku kalendarzowym poprzedzającym rok nałożenia kary.

6. Ustalając wysokość kary pieniężnej, Prezes UKE uwzględnia zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe.

7. Podmiot jest obowiązany do dostarczenia Prezesowi UKE, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku niedostarczenia danych lub gdy dostarczone dane uniemożliwiają ustalenie podstawy wymiaru kary, Prezes UKE może ustalić podstawę wymiaru kary pieniężnej w sposób szacunkowy, nie mniejszą jednak niż kwota 500 000 zł.

8. Jeżeli okres działania podmiotu jest krótszy niż rok kalendarzowy, za podstawę wymiaru kary przyjmuje się kwotę 500 000 zł.

9. Kary pieniężne, o których mowa w art. 20 ust. 1, 3 i 4, nakładane przez Prezesa UKE, stanowią dochód budżetu państwa.

Art. 22. 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody wysyła lub odbiera komunikaty lub połączenia głosowe w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe

– podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 23. 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody wysyła krótką wiadomość tekstową (SMS), wiadomość multimedialną (MMS) lub wiadomość za pośrednictwem innych usług komunikacji interpersonalnej, w której podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego, instalacji oprogramowania, przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej

– podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3. Jeżeli czyn, o którym mowa w ust. 1, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Art. 24. 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody, przy wywoływaniu połączenia głosowego posługuje się, nie będąc do tego uprawnionym, informacją adresową wskazującą na inną osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, aby podszyć się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania, przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej

– podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3. Jeżeli czyn, o którym mowa w ust. 1, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Art. 25. 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody dokonuje nieuprawnionej modyfikacji informacji adresowej uniemożliwiającej lub istotnie utrudniającej ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu, numeru telefonu lub identyfikatora, przy użyciu którego nastąpiło wysłanie komunikatu

– podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 26. 1. Prezes UKE przedstawia sejmowej komisji właściwej w sprawach telekomunikacji oraz ministrowi właściwemu do spraw informatyzacji roczne sprawozdanie z wykonywania swoich obowiązków i uprawnień określonych w niniejszej ustawie.

2. Prezes UKE składa sprawozdanie do dnia 31 marca danego roku kalendarzowego, za rok poprzedni.

Art. 27. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581) w art. 192 w ust. 1 w pkt 2 w lit. b w tiret czwartym średnik zastępuje się przecinkiem i dodaje się tiret piąte w brzmieniu:

„– z dnia …. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. ...);”.

Art. 28. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57) w art. 4 po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) obowiązku stosowania, w zakresie korzystania, przy realizacji zadań publicznych, poczty elektronicznej wykorzystującej mechanizmy uwierzytelniania, o których mowa w art. 17 ust. 1 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. ….);”.

Art. 29. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666) w art. 26 w ust. 6 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) monitorowanie występowania smishingu oraz tworzenie wzorca wiadomości wyczerpującej znamiona smishingu, o którym mowa w art. 4 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …).”.

Art. 30. 1. CSIRT NASK w terminie 3 miesięcy od dnia wejścia w życie ustawy uruchamia system, o którym mowa w art. 4 ust. 3, i informuje ministra właściwego do spraw informatyzacji o jego uruchomieniu.

2. Minister właściwy do spraw informatyzacji niezwłocznie po otrzymaniu informacji, o której mowa w ust. 1, udostępnia, w Biuletynie Informacji Publicznej na swojej stronie podmiotowej, informację o uruchomieniu systemu, o którym mowa w art. 4 ust. 3.

3. Komendant Centralnego Biura Zwalczania Cyberprzestępczości, Prezes UKE i przedsiębiorcy telekomunikacyjni są obowiązani 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.

Art. 31. Przedsiębiorcy telekomunikacyjni są obowiązani do wdrożenia proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie, o których mowa w art. 3 ust. 1:

1) pkt 1 i 2 – w terminie 6 miesięcy od dnia wejścia w życie ustawy;
2) pkt 3 i 4 – w terminie 12 miesięcy od dnia wejścia w życie ustawy.

Art. 32. 1. W terminie miesiąca od dnia wejścia w życie niniejszego przepisu strony porozumienia o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe, oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, zawartego w dniu 23 marca 2020 r., zwanego dalej „Porozumieniem z 23 marca 2020 r.", mogą złożyć oświadczenie woli o uznaniu Porozumienia z 23 marca 2020 r. za porozumienie, o którym mowa w art. 13 ust. 1.

2. W przypadku złożenia w terminie, o którym mowa w ust. 1, oświadczeń woli przez wszystkie strony Porozumienia z 23 marca 2020 r. staje się ono porozumieniem, o którym mowa w art. 13 ust. 1, z dniem złożenia oświadczenia woli przez ostatnią ze stron. W takim przypadku postanowienia Porozumienia z 23 marca 2020 r. ograniczające stosowanie tego porozumienia do stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej stają się bezskuteczne.

3. Z dniem uznania Porozumienia z 23 marca 2020 r. za porozumienie, o którym mowa w art. 13 ust. 1, lista ostrzeżeń dotycząca domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników internetu, prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie Porozumienia z 23 marca 2020 r. staje się listą, o której mowa w art. 13 ust. 1.

Art. 33. 1. Dostawca poczty elektronicznej, który świadczy pocztę elektroniczną na podstawie umowy, której stroną jest podmiot publiczny, obowiązującej w dniu wejścia w życie ustawy, jest obowiązany w terminie 3 miesięcy od dnia wejścia w życie ustawy do spełnienia obowiązku, o którym mowa w art. 17 ust. 1.

2. Jeżeli dostawca poczty elektronicznej nie spełni wymagań w terminie, o którym mowa w ust. 1, umowa może zostać jednostronnie rozwiązana przez podmiot publiczny, a dostawcy poczty elektronicznej nie przysługują roszczenia z tego tytułu.

Art. 34. W terminie 6 miesięcy od dnia wejścia w życie ustawy dostawca poczty elektronicznej, który zawarł umowę z podmiotem publicznym o świadczenie poczty elektronicznej, przedstawi ofertę poczty elektronicznej umożliwiającej stosowanie metod uwierzytelniania wieloskładnikowego, chyba że świadczona przez tego dostawcę poczta elektroniczna umożliwia stosowanie tych metod.

Art. 35. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem:

1) art. 2 pkt 1, 5 i 10, art. 13–15 oraz art. 32, które wchodzą w życie z dniem następującym po dniu ogłoszenia;
2) art. 20 ust. 3 pkt 1, który wchodzi w życie po upływie 6 miesięcy od dnia wejścia w życie ustawy;
3) art. 20 ust. 3 pkt 2, który wchodzi w życie po upływie 12 miesięcy od dnia wejścia w życie ustawy.

UZASADNIENIE

Komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych codziennie 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 lub osiągnięcia nienależnych korzyści.

W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych[1]. 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 bądź w niektórych przypadkach próbowali nawet ich zastraszyć. Zjawisko to występuje pod nazwą CLI spoofing. Polega ono na nieuprawnionym posłużeniu się przez użytkownika wywołującego połączenie głosowe (często przestępcę) numerem wskazującym na inną osobę lub instytucję, po to, aby podszyć się pod tę osobę albo instytucję i dzięki temu móc łatwiej nakłonić ofiarę (tj. odbiorcę takiego połączenia) do określonego działania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji złośliwego oprogramowania.

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 przez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu.

W tej sytuacji konieczne jest wprowadzenie odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. W ramach obecnych przepisów nie ma możliwości skutecznego przeciwdziałania nadużyciom 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. Projekt ustawy ma na celu

---

[1] Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021, s. 81, https://cert.pl/uploads/docs/Raport_CP_2021.pdf.

wdrożenie przepisu art. 97 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz. Urz. UE L 321 z 17.12.2018, str. 36, z późn. zm.), zgodnie z którym organy mogą wymagać od podmiotów udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej zablokowania w indywidualnych przypadkach dostępu do numerów lub usług, w przypadku gdy jest to uzasadnione ze względu na oszustwo lub nadużycie. Szybki wzrost liczby tego typu przestępstw oraz fakt, że regulowana materia znajduje się na styku dziedziny prawa telekomunikacyjnego i wyodrębniającego się materialnego prawa administracyjnego z zakresu cyberbezpieczeństwa, sprawia, że konieczne jest ujęcie tego zagadnienia w odrębnej ustawie. Aby uniknąć konieczności szybkiej nowelizacji ustawy i związanej z tym niepewności prawnej, projektodawca zdecydował się posłużyć w pewnym zakresie pojęciami z Europejskiego kodeksu łączności elektronicznej. Równocześnie, w wielu definicjach, projekt ustawy odwołuje się do ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, z późn. zm.), tak aby umożliwić jej wykonanie od razu po wejściu w życie.

Uzasadnienie poszczególnych przepisów materialnych

Art. 1.

Przepis art. 1 ustawy określa zakres przedmiotowy ustawy. Przede wszystkim nowe przepisy zawierają prawa i obowiązki przedsiębiorców telekomunikacyjnych oraz kompetencje Prezesa Urzędu Komunikacji Elektronicznej związane z zapobieganiem i zwalczaniem nadużyć w komunikacji elektronicznej. Określone zostały również zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS) wobec uznania treści krótkiej wiadomości tekstowej (SMS) za wyczerpującą znamiona nadużycia w komunikacji elektronicznej, zasady wnoszenia sprzeciwu wobec wpisania domeny internetowej na listę ostrzeżeń, obowiązki dostawcy poczty elektronicznej oraz podmiotu publicznego związane ze świadczeniem i korzystaniem z poczty elektronicznej w celu zapobiegania nadużyciom w komunikacji elektronicznej, a także szczególne zasady przetwarzania informacji objętych tajemnicą telekomunikacyjną związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej.

Art. 2.

Przepis art. 2 zawiera słowniczek ustawowy. Wskazano w nim 20 definicji.

Do najważniejszych definicji należy definicja CSIRT NASK. Projekt odwołuje się tutaj do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666). Zgodnie z art. 2 pkt 3 tej ustawy jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Definicja dostawcy poczty elektronicznej nawiązuje do definicji usługodawcy w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), ponieważ poczta elektroniczna jest według tej ustawy usługą świadczoną drogą elektroniczną. Dostawcą poczty jest więc osoba fizyczną, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadzi, chociażby ubocznie, działalność zarobkową lub zawodową związaną ze świadczeniem poczty elektronicznej.

Definicja informacji adresowej obejmuje numery lub identyfikator użytkownika wysyłającego komunikat. Identyfikatorem mogą być znaki identyfikujące abonenta (o których mowa w art. 130 ustawy dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, np. adresy elektroniczne, nazwy, kody, radioamatorskie znaki identyfikujące stację) oraz adresy IP.

Kolejną istotną definicją jest definicja komunikatu. Definicja ta stanowi odwołanie do definicji komunikatu zawartej w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Oznacza on każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych; nie obejmuje on informacji przekazanej jako część transmisji radiowych lub telewizyjnych transmitowanych przez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację. Takie rozwiązanie zapewnia spójność systemu prawnego.

Wprowadza się definicję listy ostrzeżeń – jest to jawna lista ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzenia mieniem użytkowników internetu.

Kluczową definicją jest także definicja nadużycia w komunikacji elektronicznej. W pierwszej kolejności opisano czynność będącą nadużyciem. Jest to świadczenie lub korzystanie z usługi telekomunikacyjnej[2] lub korzystanie z urządzeń telekomunikacyjnych[3] niezgodnie z ich

[2] Jest to usługa polegająca głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej.

[3] Urządzeniem telekomunikacyjnym jest urządzenie elektryczne lub elektroniczne przeznaczone do zapewniania telekomunikacji.

przeznaczeniem lub przepisami prawa. Działania tego może się dopuścić zarówno przedsiębiorca telekomunikacyjny, jak i użytkownik końcowy. Jednak nie każde takie działanie powinno być automatycznie uznane za nadużycie. Dlatego kolejnym elementem definicji jest wskazanie celu lub skutku tego działania w postaci wyrządzenia szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści dla siebie lub innej osoby.

Przy szeregu definicji projekt odwołuje się do ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (np. definicja przedsiębiorcy telekomunikacyjnego, operatora, usługi telekomunikacyjnej). Odesłanie do tego aktu prawnego ma na celu zapewnienie spójności definicji w systemie prawa. Podkreślić należy, że ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne jest obecnie głównym aktem prawnym dla dziedziny telekomunikacji.

Definicja poczty elektronicznej wskazuje, że jest to usługa komunikacji interpersonalnej niewykorzystującej numerów, która umożliwia przekazywanie komunikatu elektronicznego, z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol[4]), POP3 (Post Office Protocol[5]), IMAP4 (Internet Message Access Protocol) lub innego zapewniającego analogiczną funkcjonalność. Należy mieć również na uwadze, że będzie to również usługa świadczona drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Definicja podmiotu publicznego odwołuje się z kolei do zbioru podmiotów wskazanych w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Należy przy tym podkreślić, że jest to definicja wyłącznie na potrzeby niniejszej ustawy.

Wprowadzono definicję usługi komunikacji interpersonalnej – jest to usługa umożliwiająca bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej. Z kolei przy definicji usługi komunikacji interpersonalnej niewykorzystującej numerów wskazano, że jest to usługa, która nie umożliwia realizacji

---

[4] J.C. Klensin, Simple Mail Transfer Protocol, Request for Comments, RFC 5321, Internet Engineering Task Force, 2008. https://datatracker.ietf.org/doc/html/rfc5321.

[5] M.T. Rose, J.G. Myers, *Post Office Protocol – Version 3*, Request for Comments, RFC 1939, Internet Engineering Task Force, 1996.

połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji. Te dwie definicje dodano na potrzeby definicji poczty elektronicznej.

Wprowadzono również definicję uprawnionych podmiotów, przez odwołanie do art. 179 ust. 3 pkt 1 lit. a ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne. Są to Policja, Biuro Nadzoru Wewnętrznego, Straż Graniczna, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne i Krajowa Administracja Skarbowa. Podmioty te są uprawnione do uzyskiwania od przedsiębiorców telekomunikacyjnych przekazów telekomunikacyjnych, nadawanych lub odbieranych przez użytkownika końcowego lub telekomunikacyjne urządzenie końcowe. Odwołanie do ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne zapewni spójność regulacji, zwłaszcza w przypadku, gdyby katalog tych podmiotów został poszerzony, decyzją ustawodawcy.

Art. 3.

W art. 3 wprowadzona została generalna reguła stanowiąca, że nadużycia w komunikacji elektronicznej są zakazane. Ustawa wprowadza otwarty katalog nadużyć w komunikacji elektronicznej, ponieważ wobec postępu technologicznego nie jest możliwe zidentyfikowanie wszystkich form nadużyć. Dookreślono natomiast cztery szczególne (podstawowe) formy nadużyć w komunikacji elektronicznej. Są to:

1) generowanie sztucznego ruchu – jest to wysyłanie lub odbieranie komunikatów lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe;
2) smishing – jest to wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania;
3) CLI spoofing – jest to nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca

telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu lub poczucia zagrożenia, lub nakłonienia odbiorcy tego połączenia do określonego działania, zwłaszcza przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania;

4) nieuprawniona zmiana informacji adresowej – jest to nieuprawnione modyfikowanie informacji adresowej uniemożliwiające lub istotnie utrudniające ustalenie przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu numeru telefonu lub identyfikatora, przy użyciu którego nastąpiło wysłanie komunikatu elektronicznego.

Sztuczny ruch (Artificial Traffic Generating) polega na tym, że automatycznie inicjowane są połączenia (lub wysyłane są komunikaty) z jednego lub wielu numerów na inny numer/numery. Są to wielogodzinne połączenia, które nie niosą za sobą żadnej treści – tak naprawdę nie służą do komunikowania się, tylko zarejestrowaniu na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe. Przedsiębiorca telekomunikacyjny obserwuje wtedy znaczny wzrost wolumenu ruchu niedający się uzasadnić wzrostem ruchu wynikającym z normalnej aktywności użytkowników końcowych. Jest wiele scenariuszy sztucznego ruchu. Dla przykładu można wskazać sytuację, w której ruch głosowy lub sms'owy jest generowany masowo z ofert nielimitowanych, co powoduje zwiększenie płatności w rozliczeniach międzyoperatorskich. Często ten rodzaj nadużycia jest realizowany przez zorganizowane grupy, które korzystają z usług nielimitowanych, a następnie wykonują masowe połączenia na z góry zdefiniowane/przygotowane numery odbierające sztuczny ruch, aby wpłynąć na zwiększenie ruchu rejestrowanego na punktach styku międzyoperatorskich. W tej sytuacji tracą przedsiębiorcy telekomunikacyjni, którzy w ramach rozliczeń międzyoperatorskich płacą stawki za zakańczanie połączeń w sieciach stacjonarnych (FTR) oraz mobilnych (MTR). Przychód z usług nielimitowanych nie jest w stanie pokryć znacznie zwiększonych kosztów za zakańczanie połączeń (stawki są za każdą minutę połączenia). Korzysta na tym oczywiście operator, w którego sieci jest zakańczane połączenie – przedsiębiorca, u którego było inicjowane połączenie mające charakter sztucznego ruchu, musi zapłacić fakturę za zakończenie połączenia.

Jako inny przykład sztucznego ruchu można wskazać sytuację, w której ruch głosowy lub sms'owy jest generowany masowo na kierunki o podwyższonej opłacie (w tym na kierunki

międzynarodowe, które zgodnie z cennikiem są wysokopłatne), a wykonany w wyniku włamania do urządzeń klienckich, które nie były wystarczająco zabezpieczone lub były zainfekowane złośliwym oprogramowaniem.

Możliwa jest również sytuacja, w której ktoś włamuje się na centralkę telefoniczną PBX klienta operatora i w ramach włamania wykonuje ogromną liczbę połączeń na kierunki egzotyczne. Poszkodowany jest klient, który miał włamanie, i operator, bo najczęściej klient nie jest w stanie ponieść pełnej opłaty za wykonane połączenia, a operator w rozliczeniach międzyoperatorskich musi zapłacić za połączenia. W takiej sytuacji zyskuje operator zagraniczny, który ostatecznie terminuje ruch i wystawia za to fakturę.

Sztuczny ruch może narażać operatorów na straty od kilku do kilkudziesięciu milionów złotych rocznie. Zjawisko to również negatywnie wpływa na użytkowników końcowych – wskutek działań oszustów zmniejsza się przepustowość sieci telekomunikacyjnych. Z tych powodów zasadne jest wyodrębnienie tego nadużycia.

Oszuści często próbują wykorzystać krótkie wiadomości tekstowe (SMS) i podszyć się pod zaufane instytucje. Dla przykładu można wskazać sytuację, w której oszust podszywał się pod firmy energetyczne i rozsyłał wiadomości o rzekomo nieopłaconych rachunkach za prąd[6]. W takiej wiadomości znajdował się np. powszechnie znany skrót firmy energetycznej oraz link do strony internetowej, na której rzekomo można było opłacić zaległy rachunek. Strona może być łudząco podobna do prawdziwej strony internetowej danej firmy. Różnice są trudno zauważalne. Adres fałszywej strony może być łudząco podobny do adresu właściwej strony internetowej: może różnić się od prawdziwego znakami interpunkcyjnymi czy użyciem znaków diakrytycznych nieużywanych w alfabecie polskim. Strona może „zachęcać" do przelania opłaty na podany rachunek czy wykorzystania w tym celu innej formy płatności. Taka „fałszywa" strona może przekierować nieświadomą ofiarę na inną, łudząco podobną stronę banku, która

[6] https://strefabiznesu.pl/dostales-smsa-o-niezaplaconym-rachunku-za-energie-elektryczna-to-pulapka-na-twoje-dane-i-pieniadze-zignoruj-wiadomosc/ar/c3-16891001.

w rzeczywistości służy oszustowi do uzyskania danych logowania do bankowości elektronicznej.

Otwarcie linku zawartego w SMS może również powodować ukrytą instalację oprogramowania szpiegującego, które może wykraść np. dane logowania do bankowości elektronicznej[7].

Opisane wyżej scenariusze nie są jedynymi możliwymi. Oszuści mogą podszywać się pod banki[8] albo firmy kurierskie[9]. Dlatego w definicji smishingu wskazano, że jest to wysłanie choćby jednej krótkiej wiadomości tekstowej, w której nadawca podszywa się pod inny podmiot (osobę fizyczną, prawną czy ułomną osobę prawną), aby nakłonić nadawcę do konkretnego zachowania. Katalog tych zachowań jest otwarty – w przepisie wskazano przykładowe zachowania, takie jak: przekazanie danych osobowych, niekorzystne rozporządzenie mieniem, otwarcie strony internetowej, inicjowanie połączenia głosowego lub instalację oprogramowania.

Usługa Caller ID pozwala na wyświetlenie numeru użytkownika dzwoniącego na telefonie odbiorcy, dzięki czemu odbiorca może zdecydować o odebraniu połączenia. Numer ten jest przekazywany między przedsiębiorcami bez mechanizmów uwierzytelniania tej informacji[10] – obecne standardy budowy sieci telekomunikacyjnych nie przewidują takich mechanizmów. Z tego powodu bardzo łatwo jest oszustom podszyć się pod konkretny numer, korzystając z internetowych bramek VoIP. Oszuści podszywają się pod różne numery, np. instytucji publicznych czy banków, które są dostępne w Internecie. Zdarza się, że podszywają się pod numery osób publicznych – ich numery mogły zostać zdobyte np. w wyniku wycieku danych z serwisów społecznościowych czy ze sklepów internetowych. Przestępcy używają ich, aby zastraszyć konkretne osoby[11], nakłonić do instalacji oprogramowania, które pozwoli na zdobycie danych logowania do bankowości

---

7 International Telecommunication Union, *Recommendation X.Sup29 (09/17) : ITU-T X.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks* https://www.itu.int/rec/T-REC-X.Sup29-201709-I str. 3-4.

8 https://cert.pl/posts/2022/04/banki-phishing/.

9 https://cert.pl/posts/2022/04/flubot-smishing/.

10 International Interconnection Forum for Services over IP (i3 FORUM), *Technical Report Calling Line Identification (CLI) spoofing (Release 1.0) October 2020, str. 13* https://i3forum.org/public_html/wp-content/uploads/2020/11/i3f-Technical-Report-CLI-spoofing-Technical-Report-final.pdf.

11 https://www.telepolis.pl/wiadomosci/wydarzenia/rzecznik-uke-witold-tomaszewski-grozba-telefoniczna-spoofing.

elektronicznej[12] czy przekazanie danych osobowych, które pozwolą na np. zaciągnięcie kredytu. Zdarzały się sytuacje, w których oszuści podszywali się pod osoby publiczne, aby zastraszyć członków ich rodziny[13].

Zjawisko to wywołuje powszechne oburzenie. Wśród społeczeństwa powoduje osłabienie zaufania do usług telekomunikacyjnych. Podmioty, pod które podszyli się oszuści, w niezawiniony przez siebie sposób tracą na wiarygodności. Często są zmuszone zmienić numer telefonu. Wizerunkowo tracą również przedsiębiorcy telekomunikacyjni – *CLI spoofing* dokonuje się za pomocą świadczonych przez nich usług. Przedsiębiorcy ci mogą także tracić przychody, ponieważ część osób może rezygnować z odbioru połączeń głosowych.

Przykładem takich połączeń głosowych, w których oszuści podszywają się pod inną osobę, są m.in.:

- połączenia, które przychodzą z zagranicy, a ich informacja adresowa wskazuje na numer użytkownika, który przebywa w kraju,
- połączenia głosowe, które podszywają się pod numer alarmowy (np. 112),
- połączenia głosowe, które podszywają się pod numer niezgodny z Planem numeracji krajowej.

W przepisie wskazano, że CLI spoofing polega na nieuprawnionym posłużeniu się lub korzystaniu przez użytkownika lub przedsiębiorcę telekomunikacyjnego informacją adresową, które służy podszyciu się pod inny podmiot. Przedsiębiorcy telekomunikacyjni będą mogli w wielu przypadkach wykryć podejrzane połączenia, monitorując ruch w sieci telekomunikacyjnej.

W celach informacyjnych dla obywateli w przepisie dodano również otwarty katalog działań, jakie oszuści mogą podejmować przez CLI spoofing. Będzie to wywołanie strachu, poczucia zagrożenia lub nakłonienie odbiorcy połączenia do określonego

---

[12] https://www.kzbs.pl/ZBP-Zagrozenia-zwiazane-z-instalacja-zdalnego-pulpitu.html, https://nowy-sacz.policja.gov.pl/kn/prewencja/jak-unikac-zagrozen-por/8538,Spoofing-telefoniczny-na-Sadecczyznie-Ostrzegamy-przed-oszustwem-na-zdalny-doste.html.

[13] https://wiadomosci.onet.pl/kraj/atak-na-prof-marcina-matczaka-dostal-telefon-ze-jego-syn-raper-mata-nie-zyje/dhpxq1d, https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/spoofing-ponownie-w-akcji-corka-bylego-szefa-cba-uslyszala-ze-tata-nie-zyje/m7zh79j.

zachowania, zwłaszcza przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania.

Nazwa CLI spoofing pochodzi od skrótu *CLI* (*calling line identification*) oraz wyrazu *spoofing*[14].

Informacja adresowa o numerze abonenta wywołującego powinna być zasadniczo niezmienna na całej drodze połączeniowej, o czym stanowi obecne brzmienie § 1 załącznika pn. „Szczegółowe wymagania dotyczące zasad adresowania dla właściwego kierowania połączeń" do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 12 grudnia 2014 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania połączeń dla właściwego kierowania połączeń (Dz. U. z 2015 r. poz. 12). Wskazany rodzaj nadużycia polega na niedozwolonym oddziaływaniu na urządzenia telekomunikacyjne i zmianę danych rejestrowych np. połączenia międzynarodowego wywołującego (numeru A) oraz takim kierowaniu ruchu telekomunikacyjnego z/do innych sieci telekomunikacyjnych lub za pośrednictwem sieci operatorów, aby zgubić źródło ruchu i zakończyć połączenie po stawkach krajowych. Zasadniczym celem podmiany numeru jest wprowadzenie w błąd (co do źródła ruchu) systemów operatora, do którego powinien trafić ruch. W wyniku powyżej opisanej działalności operatorzy telekomunikacyjni nie są w stanie przedstawić prawdziwych i kompletnych informacji o tym, kto faktycznie dzwonił na podany numer. Co za tym idzie, utrudnia to uprawnionym podmiotom w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne ustalenie sprawcy np. fałszywych alarmów bombowych. Nieuprawniona zmiana informacji adresowej utrudnia także rozliczanie się między operatorami za realizację połączeń.

Przepis odnosi się do modyfikacji informacji adresowej, przy użyciu której nastąpiło wysłanie komunikatu. Definicja komunikatu jest bardzo pojemna, obejmuje każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych. Przepis więc będzie dotyczył modyfikacji informacji adresowej krótkich wiadomości tekstowych, wiadomości multimedialnych MMS, a także informacji adresowej połączenia głosowego.

Wskazane w art. 3 ust. 1 pkt 1–4 opisy sztucznego ruchu, smishingu, CLI spoofignu, nieuprawnionej zmiany informacji adresowej będą miały także charakter dydaktyczny.

[14] https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/832-spoofing.

Przedsiębiorcy telekomunikacyjni będą mogli użyć tych pojęć w umowach międzyoperatorskich w postanowieniach dotyczących nadużyć w komunikacji elektronicznej. Dzięki temu zostanie zapewnione jednolite rozumienie tych pojęć w obrocie prawnym.

Użycie w projekcie wyrażeń obcojęzycznych jest uzasadnione, ponieważ nie mają one dokładnego odpowiednika w języku polskim. Jest to zgodne z § 8 ust. 2 pkt 2 *in fine* Zasad techniki prawodawczej stanowiących załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. z 2016 r. poz. 283). Należy ponadto zauważyć, że te wyrażenia należą do zwyczajowo stosowanej terminologii technicznej, a stosowanie takiej terminologii obcojęzycznej dopuszcza ustawa z dnia 7 października 1999 r. o języku polskim (Dz. U. z 2021 r. poz. 672).

Proponowany art. 3 ust. 2 nakłada na przedsiębiorcę telekomunikacyjnego ogólny obowiązek podejmowania proporcjonalnych działań mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Istotne jest, że mają to być działania proporcjonalne do wyników przeprowadzonej oceny ryzyka, gdyż wśród przedsiębiorców telekomunikacyjnych znajdują się zarówno duzi przedsiębiorcy dostarczający sieci mobilne, jak i mali i średni przedsiębiorcy. Działania podejmowane przez te podmioty będą więc zależne od wielkości podmiotu, posiadanej infrastruktury czy charakteru świadczonych usług. Przykładowo jako jeden ze środków można wskazać monitorowanie usług telekomunikacyjnych w celu wykrywania przypadków CLI spoofingu. W przypadku sztucznego ruchu przedsiębiorcy telekomunikacyjni będą mogli korzystać np. z systemów klasy Fraud Management System lub Anti Fraud System (FMS/AFS)[15]. Przy określaniu proporcjonalnych środków można posiłkować się uznanymi międzynarodowymi standardami w zakresie zarządzania ryzykiem, np. COSO II czy ISO 31000.

Nadużycia w komunikacji elektronicznej mają zgoła różny i często skomplikowany charakter, a co za tym idzie, przeciwdziałanie i zwalczanie ich wymaga podejmowania różnych (odmiennych) środków organizacyjnych i technicznych. W związku z tym konieczne jest również wprowadzenie ogólnego obowiązku przedsiębiorców telekomunikacyjnych do przeciwdziałania nadużyciom telekomunikacyjnym. Będzie to dawało podstawę prawną do reagowania na nowe rodzaje nadużyć. Ze względu na ogólny charakter tego obowiązku nie

[15] https://www.pwc.pl/pl/artykuly/2017/naduzycia-w-telekomach-czesc1.html.

wiąże się on z jakąkolwiek sankcją. Równocześnie stanowi to jasny sygnał, że działania przestępcze wykorzystujące sieci telekomunikacyjne nie będą tolerowane.

Art. 4 oraz art. 5.

W celu zapobiegania oraz zwalczania smishingu proponuje się wprowadzenie zautomatyzowanego blokowania, przez przedsiębiorców telekomunikacyjnych, krótkich wiadomości tekstowych (SMS), zawierających treści zgodne ze wzorcem wiadomości wyczerpującej znamiona smishingu.

Projekt zakłada, że monitorowaniem występowania smishingu będzie zajmował się zespół CSIRT NASK, który działa w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym. Zespół posiada niezbędną wiedzę i doświadczenie do podjęcia się takiego zadania – w kwietniu 2021 r. uruchomił usługę polegającą na możliwości zgłoszenia przez odbiorców podejrzanego SMS-u.

CSIRT NASK będzie monitorował występowanie zjawiska smishingu na podstawie danych dobrowolnie 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 – przez przekazanie SMS na specjalny numer[16] albo przez formularz na stronie internetowej[17]. Należy też wskazać, że NASK będzie obsługiwał wszystkie takie zgłoszenia, niezależnie od sposobu, w jaki zostanie ono przekazane. Niniejszy projekt ustawy nie przyznaje CSIRT NASK uprawnienia do żądania przedstawienia informacji stanowiących tajemnicę przedsiębiorstwa, a także tajemnicy telekomunikacyjnej w celu monitorowania smishingu.

Na podstawie wyników monitorowania smishingu CSIRT NASK tworzyłby wzorzec wiadomości wyczerpującej znamiona smishingu. Wzorzec ten byłby przekazywany przedsiębiorcom telekomunikacyjnym za pomocą nowego systemu teleinformatycznego. Następnie ci przedsiębiorcy, za pomocą własnych systemów teleinformatycznych, blokowaliby automatycznie SMS, których treść byłaby zgodna ze wzorcem. Dzięki temu możliwe będzie zwalczanie smishingu w oparciu o analizę dotychczasowych praktyk oszustów. Odbiorcy SMS nie otrzymają treści, które mogłyby ich nakłonić do niekorzystnego dla nich działań. Za

[16] https://www.nask.pl/pl/aktualnosci/4183,Teraz-jeszcze-latwiej-zglosic-incydent-bezpieczenstwa-przez-SMS.html.
[17] https://incydent.cert.pl/#!/lang=pl,entityType=notObligatedEntity,easyIncidentType=email.

pomocą tego systemu będzie możliwe także przekazywanie wiadomości o występowaniu smishingu – chodzi tutaj o możliwość np. ostrzegania o nowych kampaniach smishingowych.

Wprowadza się również przepis wskazujący CSIRT NASK jako odpowiedzialny za funkcjonowanie systemu teleinformatycznego służącego do udostępniania i przekazywania informacji o wystąpieniu smishingu wraz ze wzorcem wiadomości. Ponadto CSIRT NASK będzie administratorem danych przetwarzanych w tym systemie. Przepisy te jasno określą, kto jest odpowiedzialny za system i przetwarzane w nim dane.

Dostęp do systemu teleinformatycznego CSIRT NASK będzie również zapewniał:

- Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości – z uwagi na to, że Policja zajmuje się zwalczaniem przestępczości, a nadużycia w komunikacji elektronicznej bardzo często mogą wyczerpywać znamiona przestępstw,
- Prezesowi Urzędu Komunikacji Elektronicznej – z uwagi na jego zadania przy procedurze sprzeciwu wobec zablokowania krótkiej wiadomości tekstowej.

Komendant Centralnego Biura Zwalczania Cyberprzestępczości, Prezes Urzędu Komunikacji Elektronicznej, zwany dalej „Prezesem UKE”, i przedsiębiorcy telekomunikacyjni będą obowiązani do dostosowania i podłączenia swoich systemów teleinformatycznych do wskazanego systemu w terminie 3 miesięcy od dnia zamieszczenia w Biuletynie Informacji Publicznej przez ministra właściwego do spraw informatyzacji informacji o jego uruchomieniu. Podmioty te będą miały obowiązek korzystania z tego systemu w celu wymiany informacji o wystąpieniu smishingu, w tym przekazywania wzorców wiadomości wyczerpującej znamiona smishingu.

Wzorce wiadomości będą udostępniane na stronie internetowej NASK-PIB nie wcześniej niż 14 dni i nie później niż 21 dni od dnia udostępnienia wzorca w systemie teleinformatycznym. Z jednej strony przepis ten zapewnia jawność działania państwa w zakresie zwalczania smishingu, z drugiej zaś nie jest celowe publikowanie wzorców od razu, po ich przekazaniu do przedsiębiorców telekomunikacyjnych, ponieważ dzięki temu przestępcy byliby w stanie zmienić używane szablony krótkich wiadomości tekstowych (SMS), aby ominąć wzorce.

Projektodawca przewidział sytuację, gdy treść zawarta we wzorcu nie stanowi smishingu[18]. Może zachodzić także sytuacja, gdy nie jest celowe dalsze blokowanie takich wiadomości. Może się tak wydarzyć na przykład, jeżeli:

- mimo przekazania wzorca smishing dociera do użytkowników i wzorzec musi zostać poprawiony,
- wzorzec jest zbyt szeroki i blokuje także SMS-y niemające charakteru smishingu,
- oszuści już nie korzystają z wcześniejszych metod w smishingu, np. nie używają sformułowań związanych ze szczepieniem – w tej sytuacji wzorzec może być wycofany.

W tej sytuacji CSIRT NASK poinformuje o wycofaniu wzorca, a przedsiębiorca telekomunikacyjny przestanie blokować takie wiadomości. W takim przypadku CSIRT NASK będzie również zamieszczał na stronie internetowej informacje o okresie, w jakim wycofany wzorzec obowiązywał.

SMS zawierający link do złośliwej strony internetowej stanowi zagrożenie cyberbezpieczeństwa w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zaś zgodnie z art. 26 ust. 3 pkt 1 tej ustawy do zadań CSIRT NASK należy m.in. monitorowanie zagrożeń cyberbezpieczeństwa na poziomie krajowym. Przepis art. 39 ust. 1 ww. ustawy uprawnia CSIRT NASK do przetwarzania danych pozyskanych w związku z zagrożeniami cyberbezpieczeństwa, w tym danych osobowych, w zakresie i w celu niezbędnym do realizacji zadań określonych m.in. w art. 26 tej ustawy. Z tego powodu, aby zapewnić spójność projektowanych przepisów z systemem prawa, dodano przepis, zgodnie z którym CSIRT NASK będzie przetwarzał dane pozyskane w związku z monitorowaniem występowania smishingu na zasadach określonych w art. 39 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 6.

Projekt przewiduje dla nadawcy krótkiej wiadomości tekstowej (SMS) możliwość wniesienia sprzeciwu do Prezesa UKE wobec zablokowania krótkiej wiadomości tekstowej (SMS) zawierającej treści zawarte we wzorcu wiadomości wyczerpującej znamiona smishingu.

[18] Przepis art. 4 ust. 8 pkt 1 posługuje się wyrażeniem „treści zawartej we wzorcu", ponieważ istotne przy autokontroli jest sprawdzenie poszczególnych wyrazów czy znaków i weryfikacja, czy rzeczywiście obejmują one treści mające charakter smishingu.

Sprzeciw będzie zawierał:

1) pełną treść zablokowanej krótkiej wiadomości tekstowej (SMS);

2) uzasadnienie wyjaśniające, dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu;

3) wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS);

4) dane identyfikujące nadawcę:

   a) imię (imiona) i nazwisko, adres zamieszkania - w przypadku osób fizycznych,

   b) nazwę (firmę) podmiotu, adres siedziby, numer z właściwego rejestru – w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej,

   c) imię i nazwisko osoby uprawnionej do reprezentowania nadawcy wraz z upoważnieniem – w przypadku, w którym nadawca działa przez pełnomocnika.

Informacje te będą niezbędne dla Prezesa UKE przy dokonywaniu oceny, czy rzeczywiście krótka wiadomość tekstowa miała charakter smishingu.

Sprzeciw będzie opatrywany kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Wnoszony będzie na adres do doręczeń elektronicznych Prezesa UKE[19]. Rozwiązanie to usprawni rozpatrywanie spraw, jak również umożliwi precyzyjne wskazanie momentu, od którego liczą się terminy na rozpatrzenie sprzeciwu.

Sprzeciw niespełniający powyższych wymagań Prezes UKE pozostawi bez rozpoznania.

Art. 7.

Przepis zawiera obowiązki Prezesa UKE oraz CSIRT NASK związane z procedurą rozpatrywania sprzeciwu dla nadawcy zablokowanej krótkiej wiadomości tekstowej (SMS). Prezes UKE będzie obowiązany rozpatrzyć sprzeciw w terminie 14 dni od dnia jego

[19] Zgodnie z art. 147 ust. 2 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285) doręczenie korespondencji nadanej przez osobę fizyczną lub podmiot niebędący podmiotem publicznym, będące użytkownikami konta w ePUAP, do podmiotu publicznego posiadającego elektroniczną skrzynkę podawczą w ePUAP, w ramach usługi udostępnianej w ePUAP, jest równoważne w skutkach prawnych z doręczeniem przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego, do czasu zaistnienia obowiązku stosowania ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych przez ten podmiot publiczny. Innymi słowy do czasu rozpoczęcia stosowania przez Prezesa UKE przepisów ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych sprzeciw będzie mógł być złożony na elektroniczną skrzynkę podawczą ePUAP Prezesa UKE.

otrzymania, a następnie poinformować niezwłocznie nadawcę o sposobie rozpatrzenia sprzeciwu.

Prezes UKE, rozpatrując sprzeciw, może go:

1) uwzględnić, jeżeli treść krótkiej wiadomości tekstowej (SMS) zawierająca treści wskazane we wzorcu wiadomości nie wyczerpuje znamion smishingu; w tej sytuacji Prezes UKE nakaże CSIRT NASK niezwłoczną zmianę wzorca wiadomości w taki sposób, aby treść zablokowanej wiadomości tekstowej (SMS) nie była dalej blokowana;

2) nie uwzględnić, jeżeli treść krótkiej wiadomości tekstowej (SMS) zawierająca treści wskazane we wzorcu wiadomości wyczerpuje znamiona smishingu.

Wprowadzenie decyzji administracyjnej jako instytucji prawnej wysoko sformalizowanej przy sprzeciwie od uznania SMS za smishing jest skrajnie nieadekwatne, biorąc pod uwagę m.in. skalę. CSIRT NASK od kwietnia 2021 r. do końca maja 2022 r. zidentyfikował ok. 31 000 złośliwych wiadomości SMS. Dla przykładu można założyć, że od 1% tych wiadomości zostałby złożony sprzeciw. Oznaczałoby to 310 postępowań administracyjnych prowadzonych przez Prezesa UKE. Byłoby to znaczne obciążenie organizacyjne dla tego organu. Z tego powodu zdecydowano się wyłączyć stosowanie ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego (Dz. U. z 2022 r. poz. 2000 i 2185) przy rozpatrywaniu sprzeciwu. Jednocześnie wprowadza się możliwość upoważnienia przez Prezesa UKE pracownika urzędu go obsługującego do wykonywania czynności przy rozpatrywaniu sprzeciwu. Co istotne, odformalizowana procedura sprzeciwu zapewni szybkość procedowania sprawy. Zdaniem projektodawcy sprzeciw będzie tzw. inną czynnością z zakresu administracji publicznej, która podlega kontroli sądu administracyjnego.

Art. 8.

Przepis art. 8 dotyczy sytuacji, w której przedsiębiorca zidentyfikował krótką wiadomość tekstową, zawierającą treści wyczerpujące znamiona smishingu, które jednak nie zostały wskazane we wzorcu wiadomości przekazanym przez CSIRT NASK. Przepis uprawnia przedsiębiorcę telekomunikacyjnego do zablokowania takiej wiadomości za pomocą systemu teleinformatycznego umożliwiającego automatyczną identyfikację takich wiadomości.

Jednakże przedsiębiorca telekomunikacyjny nadal będzie podlegał odpowiedzialności za niewykonanie usługi, jeżeli SMS został niezasadnie zablokowany.

Użytkownik, którego SMS został zablokowany na podstawie projektowanego art. 8, będzie mógł dochodzić swoich praw w drodze postępowania reklamacyjnego, o którym mowa w art. 106 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Użytkownik będzie mógł także skorzystać z uprawnień wynikających z art. 109 tej ustawy, czyli dochodzić swoich praw w drodze postępowania w sprawie pozasądowego rozwiązywania sporów konsumenckich. W przepisie art. 18 ust. 1 pkt 2 projektu nałożono na przedsiębiorcę telekomunikacyjnego obowiązek rejestracji informacji o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją uprawnienia, o którym mowa w art. 8. Innymi słowy prawa użytkownika, którego SMS został niezasadnie zablokowany na podstawie art. 8, są chronione przez postępowanie reklamacyjne oraz postępowanie w sprawie pozasądowego rozwiązywania sporów konsumenckich. Ponadto użytkownik będzie mógł zwrócić się do Prezesa UKE o interwencję w myśl art. 192 ust. 1 pkt 5 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Blokowanie SMS na podstawie projektowanego przepisu ma umożliwić przedsiębiorcom telekomunikacyjnym ochronę adresatów, konsumentów przed złośliwymi SMS-ami, które przedsiębiorca telekomunikacyjny wykrył wcześniej, niż CSIRT NASK przygotował wzorzec wiadomości o charakterze smishingu. Przepis ten, wspólnie z art. 4 i art. 5, realizuje rekomendacje Międzynarodowego Związku Telekomunikacyjnego (ITU), zgodnie z którymi dostawcy usług telefonii komórkowych powinni zapewnić system przeciwdziałania atakom typu smishing[20].

Podkreślić należy, że przedsiębiorca telekomunikacyjny nie jest zainteresowany blokowaniem SMS uczciwego konsumenta. W takiej sytuacji niewykonana zostaje usługa telekomunikacyjna, w związku z czym przedsiębiorca nie będzie zarabiał. Zauważyć też należy, że na obecnym rynku telekomunikacyjnym istnieje duża konkurencja – jeżeli więc przedsiębiorca telekomunikacyjny będzie niezasadnie blokował SMS, to będzie musiał liczyć się z tym, że abonent zrezygnuje z jego usług.

[20] Pkt 8.3: *Cell service providers should provide a countering system for preventing smishing attacks.* ITU-TX.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks.

Przepis art. 8 ust. 2 umożliwia przedsiębiorcy telekomunikacyjnemu blokowanie wiadomości multimedialnych MMS, w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania. Jest to sytuacja podobna do smishingu. Jednakże wyodrębniono ją, ponieważ identyfikowanie i blokowanie takich wiadomości MMS, z uwagi na ich charakter (mogą to być np. obrazy), wymaga innej technologii niż przy blokowaniu SMS.

Art. 9.

Przepis nakłada obowiązek na przedsiębiorcę telekomunikacyjnego zablokowania połączenia głosowego albo ukrycia identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia CLI spoofing. Blokowanie połączenia głosowego powinno być stosowane, kiedy prawdopodobieństwo, że dochodzi do CLI spoofingu, jest bardzo wysokie lub wysokie. W pozostałych przypadkach przedsiębiorca telekomunikacyjny powinien ukryć identyfikację numeru wywołującego dla użytkownika końcowego. Ukrycie identyfikacji numeru wywołującego oznacza w praktyce, że odbiorcy wyświetli się, że dzwoni do niego nieznany numer, a nie np. informacja, że dzwoni osoba bliska, której numer jest wpisany na liście kontaktów. Pozwoli to zapobiec takim atakom jak np. podszycie się pod byłego szefa Centralnego Biura Antykorupcyjnego Pawła Wojtunika[21].

Obowiązek ten należy odczytywać łącznie z art. 3 ust. 2 projektu ustawy, zgodnie z którym przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Doprecyzowanie środków organizacyjnych i technicznych będzie miało miejsce przez zawarcie porozumienia operatorów z Prezesem UKE.

Art. 10.

Niektórzy oszuści podszywają się pod jednostki sektora finansów publicznych czy przedsiębiorców, wykorzystując numery infolinii tych podmiotów. Numery te nie są wykorzystywane do wykonywania połączeń do konsumentów czy obywateli. Jednakże nieświadomy użytkownik końcowy, widząc numer takiego podmiotu, może mieć wrażenie, że

[21] https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-pomowmy-o-spoofingu-jak-sie-chronic.

rzeczywiście ktoś dzwoni do niego m.in. z urzędu lub z banku. Oszuści zyskują wtedy zaufanie ofiary i są w stanie nakłonić ją do niekorzystnego dla niej działania[22].

Dlatego przepis art. 10 zawiera obowiązek dla Prezesa UKE do prowadzenia jawnego wykazu numerów, które służą wyłącznie do odbierania połączeń głosowych. Rozwiązanie to ograniczy możliwość podszywania się oszustów pod numery infolinii urzędów czy innych podmiotów. Chodzi tutaj o to, aby połączenie było inicjowane tylko w jednym kierunku przez np. konsumenta, który ze swojego numeru dzwoni na numer infolinii np. banku. Numer ten nie będzie służył do inicjowania połączenia przez przykładowy bank. Oszust, próbując wykorzystać numer wpisany do wykazu do oszustwa, również nie osiągnie swojego celu, ponieważ połączenie to zostanie od razu zablokowane. Wykaz będzie prowadzony w systemie teleinformatycznym Prezesa UKE i udostępniany na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej. Dzięki temu przedsiębiorcy telekomunikacyjni będą mieli wygodny dostęp do tego wykazu i będą mogli efektywnie wykorzystać go przy zwalczaniu nadużyć w komunikacji elektronicznej.

Co najważniejsze, skutek wpisu numeru do wykazu aktualizuje obowiązek po stronie przedsiębiorcy telekomunikacyjnego świadczącego usługę połączeń głosowych do blokowania połączenia inicjowanego z wykorzystaniem numeru wpisanego do wykazu, w terminie 3 dni od wpisu. Również w terminie 3 dni od wykreślenia numeru z wykazu przedsiębiorca telekomunikacyjny zaprzestanie blokowania tego numeru.

Wniosek o wpis numeru do wykazu będzie mógł być złożony przez jednostki sektora finansów publicznych, banki, inne instytucje finansowe lub ubezpieczeniowe. W przypadku przedsiębiorcy telekomunikacyjnego uprawnienie to będzie dotyczyło numerów wyłącznie wykorzystywanych na potrzeby biura obsługi klientów lub infolinii przez tego przedsiębiorcę. Rozwiązanie to jest słuszne, ponieważ przedsiębiorca telekomunikacyjny dysponuje dużą pulą numeracji na potrzeby swoich klientów – umożliwienie wpisywania tych numerów do wykazu byłoby nieuzasadnione.

Wniosek o wpis do wykazu będzie musiał zawierać:

---

[22] Jako przykład można wskazać sytuację, w której oszust podszył się pod jeden z banków, używając do tego numeru infolinii. Następnie próbował uzyskać zaufanie klientki banku, twierdząc, że jest pracownikiem banku odpowiedzialnym za bezpieczeństwo – podał numer identyfikacyjny, oraz wysyłając wiadomości sms rzekomo z działu technicznego banku. Zachęcał również do instalacji oprogramowania, a finalnie do wysłania hasła do konta bankowego przez sms. https://www.telepolis.pl/fintech/bezpieczenstwo/pko-bp-spooinfg-atak-cyber-przestepcow-jak-sie-bronic.

1) dane wnioskodawcy:

   a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych,

   b) nazwę (firmę) wnioskodawcy, adres siedziby, numer z właściwego rejestru – w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej,

   c) imię i nazwisko osoby uprawnionej do reprezentowania wnioskodawcy wraz z upoważnieniem;

2) wskazanie numeru, który ma służyć wyłącznie do odbierania połączeń głosowych;

3) dokument potwierdzający prawo do dysponowania numerem.

W przypadku gdy wniosek nie spełnia ww. wymagań, Prezes UKE wzywa wnioskodawcę do uzupełnienia wniosku w terminie 7 dni od dnia otrzymania wezwania pod rygorem pozostawienia wniosku bez rozpoznania.

Wniosek wnoszony będzie na adres do doręczeń elektronicznych Prezesa UKE. Rozwiązanie to usprawni rozpatrywanie spraw, jak również umożliwi precyzyjne wskazanie momentu, od którego liczą się terminy na rozpatrzenie wniosku.

Prezes UKE wpisze numer do wykazu w terminie 5 dni od dnia otrzymania wniosku spełniającego ww. wymagania. Projekt przesądza, że wpis do wykazu będzie miał charakter czynności materialno-technicznej – sama ta czynność jest skutkiem uprawnienia podmiotu do złożenia wniosku o wpis do wykazu. Wniosek zostanie pozostawiony bez rozpoznania, jeżeli będzie złożony przez podmiot nieuprawniony albo będzie dotyczył numeru, który nie jest wykorzystywany przez wnioskodawcę. W takiej sytuacji Prezes UKE niezwłocznie poinformuje wnioskodawcę o pozostawieniu wniosku bez rozpoznania. Wprowadza się także możliwość złożenia wniosku o wycofanie numeru z wykazu. Będzie mógł go złożyć pierwotny wnioskodawca, ale również inny podmiot, który aktualnie korzysta z numeru, który jest wpisany do wykazu. W takim przypadku Prezes UKE niezwłocznie, najpóźniej w terminie 5 dni od dnia otrzymania wniosku o wycofanie numeru z wykazu, dokona wykreślenia numeru z wykazu.

Projekt wprowadza obowiązkową elektronizację tych wniosków – powinny być opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Wniosek, który nie spełni tych wymogów, będzie pozostawiony bez rozpoznania.

Art. 11.

W art. 11 określono, że wykaz numerów, które służą wyłącznie do odbierania połączeń głosowych, zawiera:

1) wskazanie numeru, który służy wyłącznie do odbierania połączeń głosowych;
2) datę wpisania tego numeru do wykazu;
3) datę wykreślenia numeru z wykazu.

Wskazanie w wykazie dat wpisania numeru do wykazu oraz jego wykreślenia jest konieczne z uwagi na obowiązek blokowania połączeń inicjowanych z tego numeru i związane z tym terminy dla przedsiębiorcy telekomunikacyjnego.

Art. 12.

Aby móc skutecznie zwalczać CLI spoofing, przedsiębiorca musi mieć możliwość monitorowania ruchu w sieci telekomunikacyjnej w celu wykrycia podejrzanych połączeń głosowych. Potrzebne są także środki umożliwiające wymianę informacji o takich połączeniach między przedsiębiorcami – ruch w sieci telekomunikacyjnej jest często tranzytowany przez sieci telekomunikacyjne różnych operatorów. W końcu potrzebne są środki wobec podejrzanych połączeń – środki służące blokowaniu takiego połączenia albo ukryciu identyfikacji numeru wywołującego dla użytkownika końcowego (CLIR). Dlatego przepis ust. 1 wskazuje ogólnie, że w celu zwalczania CLI spoofing (obowiązek z art. 9) przedsiębiorca telekomunikacyjny stosuje środki organizacyjne i techniczne, które służą monitorowaniu, wykrywaniu oraz wymianie informacji o tym nadużyciu, a także blokowaniu połączenia głosowego albo ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego. Konstruując ten przepis, oparto się na rekomendacjach M.3362 Międzynarodowego Związku Telekomunikacyjnego[23], które dzielą na funkcje wykrywania, monitorowania, mitygacji oszustw oraz wymianie informacji o nadużyciach telekomunikacyjnych. Zrezygnowano przy

[23] International Telecommunication Union, *Recommendation M.3362 (06/20) : Requirements for telecommunication anti-fraud management in the telecommunication management network* , str. 5 https://www.itu.int/rec/T-REC-M.3362-202006-I/en.

tym z wprowadzenia pojęcia „mitygacji nadużycia” czy „mitygacji CLI spoofing”, ponieważ samo pojęcie mitygacji nie jest aż tak oczywiste jak np. pojęcie obsługi incydentu.

Przepis ust. 1 wprowadza ogólne wymagania co do środków organizacyjnych i technicznych stosowanych przez przedsiębiorców telekomunikacyjnych przy zwalczaniu CLI spoofing. Szczegółowe środki mogą się zmieniać w toku postępu technologicznego. Dlatego projekt, w ust. 2, wprowadza możliwość zawarcia przez dostawców publicznie dostępnych usług telekomunikacyjnych świadczących usługi dla co najmniej 50 000 abonentów porozumienia z Prezesem UKE, w którym będą określone szczegółowe środki organizacyjne i techniczne, stosowane przez tych przedsiębiorców przy blokowaniu połączenia lub ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego, w przypadku gdy połączenie wyczerpuje znamiona CLI spoofingu. Projekt przesądza, że przez zawarcie tego porozumienia oraz jego prawidłowe wykonywanie operatorzy spełnią obowiązek podejmowania proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie CLI spoofing. Proponowane rozwiązanie ma na celu ułatwienie operatorom skutecznego wykonywania tych obowiązków oraz ma zapewnić im pewność regulacyjną. Wprowadza się wyłączenie odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej tych operatorów, którzy prawidłowo wykonują ww. porozumienie (ust. 3 i 4).

Kontrolę prawidłowości stosowania przez operatorów telekomunikacyjnych środków organizacyjnych i technicznych określonych porozumieniem będzie sprawował Prezes UKE. Do kontroli będą stosowane przepisy rozdziału 2 działu X ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (ust. 5).

Dzięki takiemu rozwiązaniu najwięksi operatorzy telekomunikacyjni, przy wsparciu i nadzorze Urzędu Komunikacji Elektronicznej, będą mogli wypracować najlepsze rozwiązania organizacyjne i techniczne, które pozwolą im zwalczać nadużycia w komunikacji elektronicznej. Zwolnienie z odpowiedzialności w przypadku prawidłowego wykonywania porozumienia będzie stanowiło silny bodziec do dołączenia do porozumienia.

Dla mniejszych przedsiębiorców telekomunikacyjnych, którzy mogliby nie być w stanie wypełnić obowiązków, które będą określone w porozumieniu, Prezes UKE będzie wydawał rekomendacje określające środki organizacyjne i techniczne służące realizacji obowiązków związanych ze zwalczaniem CLI spoofing. Prawidłowe wykonywanie rekomendacji Prezesa UKE będzie wyłączało odpowiedzialność tych operatorów za niewykonanie lub nienależyte

wykonanie usługi telekomunikacyjnej będące skutkiem wprowadzenia tych środków (ust. 6 i 7).

Art. 13.

Przepis art. 13 konstytuuje możliwość zawarcia przez:

- Prezesa Urzędu Komunikacji Elektronicznej,
- ministra właściwego do spraw informatyzacji,
- Naukową i Akademicką Sieć Komputerowa – Państwowy Instytut Badawczy,
- przedsiębiorcę lub przedsiębiorców telekomunikacyjnych

porozumienia dotyczącego prowadzenia listy ostrzeżeń w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzenia mieniem użytkowników internetu. Obecnie funkcjonuje podobne porozumienie, które umożliwia w okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego prowadzenie przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy , dalej jako „NASK-PIB", jawnej listy ostrzeżeń. Porozumienie to spełniło swoją rolę w okresie pandemii COVID-19, chroniąc użytkowników internetu przed utratą danych i środków finansowych. Zasadne jest umożliwienie, aby również poza okresami stanów nadzwyczajnych czy tymi związanymi z epidemią mogło obowiązywać podobne porozumienie. W przypadku zawarcia porozumienia CSIRT NASK będzie odpowiedzialny za prowadzenie jawnej listy ostrzeżeń dotyczącej niebezpiecznych domen internetowych.

Na listę ostrzeżeń będą wpisywane domeny internetowe, których podstawowym celem działania jest wprowadzenie w błąd użytkowników internetu i doprowadzenie do wyłudzenia ich danych lub niekorzystnego rozporządzenia mieniem.

Z reguły oszust tworzy stronę internetową podobną do np. strony banku. Może korzystać z tej samej lub bardzo podobnej grafiki. Może zawierać hiperłącza do prawdziwych, innych stron internetowych, aby zmylić nieświadomą ofiarę. Nazwa domeny może być bardzo podobna do prawdziwej. Oszust może korzystać z wielu nazw domenowych, aby wydłużyć istnienie fałszywej strony. Ponadto oszust może tak przygotować kod źródłowy strony (HTML), aby zmylić programy antywirusowe. Po utworzeniu strony oszust propaguje adres przez pocztę

elektroniczną, krótkie wiadomości tekstowe (SMS) czy inne środki komunikacji elektronicznej[24].

Jako przykład można wskazać domeny internetowe podszywające się pod Pocztę Polską – są podobne wizualnie i stosują podobny adres[25]. Takie fałszywe strony mogą zachęcać do logowania, przelania rzekomej dodatkowej opłaty za dostarczenie paczki czy listu czy przekazania danych w celu uzyskania zysków z rzekomej inwestycji[26]. Takie działania oszustów powodują szkody po stronie nieświadomych konsumentów. Przechwycone przez oszustów dane konsumentów mogą być wykorzystane wiele miesięcy po usunięciu strony. Wizerunkowo tracą również podmioty, pod które oszust podszywał się przez fałszywą stronę, jak i dostawcy internetu.

Raport CERT Polska wskazał dla przykładu 5 podmiotów, pod które najczęściej przestępcy podszywali się w 2021 r. wraz z liczbą odnotowanych prób wejścia na taką stronę:

	Orlen	**PGNiG**	**Tesla**	**Lotos**	**KGHM**
Liczba domen ze stronami podszywającymi się pod dany podmiot wpisanymi na Listę ostrzeżeń	3 939	564	529	282	79
Liczba odnotowanych prób wejścia na strony podszywające się pod dany podmiot	269 397	26 469	25 673	23 302	19 999

Źródło: Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021 str. 75.

Dane te pokazują, jak często nieświadomi użytkownicy internetu są wprowadzani w błąd, myśląc, że np. wchodzą na stronę ich dostawcy energii.

W samym tylko okresie od stycznia 2022 r. do listopada 2022 r. CSIRT NASK zidentyfikował łącznie 38 999 domen, które mają na celu wprowadzenie w błąd użytkowników internetu i wyłudzenie ich danych i środków finansowych.

---

[24] International Telecommunication Union, *Recommendation X.1235 (01/22) : Technologies in countering website spoofing for telecommunication organizations*, str. 3-4. https://www.itu.int/rec/T-REC-X.1235-202201-I.

[25] https://www.telepolis.pl/wiadomosci/bezpieczenstwo/poczta-polska-phishing-oszustwo-przesylka-sms.

[26] https://www.dobreprogramy.pl/padl-ofiara-oszustwa-na-orlen-zachecony-twarza-polityka-stracil-majatek,6804549571336928a, https://prnews.pl/co-robic-gdy-padniemy-ofiara-phishingu-445337, https://kartuzy.naszemiasto.pl/trzy-osoby-padly-ofiara-oszustow-schemat-dzialania-byl-za/ar/c1-9002019.

Rok	Miesiąc	Liczba szkodliwych domen wpisanych na listę ostrzeżeń[27]
2022	Styczeń	4260
	Luty	3163
	Marzec	2335
	Kwiecień	2093
	Maj	3677
	Czerwiec	3520
	Lipiec	4395
	Sierpień	4832
	Wrzesień	4261
	Październik	3886
	Listopad	2577
	suma:	38 999

Źródło: Dane.gov.pl[28]

Lista ostrzeżeń będzie przeciwdziałała również sytuacjom, w których oszust nie podszywa się pod inną osobę, lecz bezpośrednio kontaktuje się z ofiarą (dzwoniąc, wysyłając wiadomości tekstowe, pocztę elektroniczną), podając jej link do fałszywej strony.

Projekt wprowadza regulację, zgodnie z którą każdy będzie mógł zgłosić do CSIRT NASK domenę internetową mogącą służyć do wyłudzeń danych i niekorzystnego rozporządzania mieniem. Możliwe będzie dodanie uzasadnienia do zgłoszenia. Odstąpiono od obowiązku dołączania uzasadnienia, aby uprościć zgłoszenia. CSIRT NASK będzie mógł wpisać domenę na listę ostrzeżeń po zweryfikowaniu, że rzeczywiście podstawowym celem domeny jest wprowadzenie w błąd oraz wyłudzenia danych użytkowników internetu lub doprowadzenie do niekorzystnego rozporządzenia mieniem. Do ustalenia „podstawowego celu" strony internetowej można posłużyć się mechanizmem zaproponowanym przez Międzynarodowy Związek Telekomunikacyjny[29]. Mechanizm ten polega na analizie:

- porównawczej adresów URL podejrzanej strony i adresu prawdziwej strony - analiza polega na obliczeniu stopnia podobieństwa między tymi adresami; ponadto można skorzystać z danych od np. dostawców usług bezpieczeństwa dot. statystyk ruchu na

[27] https://cert.pl/posts/2020/03/ostrzezenia_phishing/.
[28] https://dane.gov.pl/pl/dataset/2740,lista-ostrzezen-cert-polska-przed-niebezpiecznymi/resource/43118/table.
[29] International Telecommunication Union, Recommendation X.1235 (01/22) : Technologies in countering website spoofing for telecommunication organizations, str. 3-4. https://www.itu.int/rec/T-REC-X.1235-202201-I.

stronie, jej reputacji, informacji o domenie czy też o certyfikatach bezpieczeństwa domeny,

- porównawczej oficjalnego logo prawdziwej strony internetowej i logo widniejącego na podejrzanej stronie,
- kodu źródłowego strony internetowej – kod podejrzanej strony może zawierać złośliwy kod,
- formularzy logowania,
- hiperłączy - podejrzana strona internetowa może wykorzystywać do swojego działania te same hiperłącza jak prawdziwa strona, mimo, że powinna wykorzystywać inne, zgodne z własnym adresem.

Po dokonaniu powyższych analiz będzie możliwa odpowiedź na pytanie, czy jest to strona podszywająca się pod inną stronę (tj., czy wprowadza w błąd użytkownika internetu). Taka strona internetowa dodatkowo zawierająca złośliwy kod czy formularze logowania np. do bankowości elektronicznej niewątpliwie będzie miała na celu wyłudzenie danych oraz środków finansowych użytkowników internetu.

Ogólna redakcja przepisu pozwala CSIRT NASK na wpisanie domeny po otrzymaniu zgłoszenia, ale również z własnej inicjatywy. Sposób dokonywania zgłoszeń zostanie określony przez CSIRT NASK i opublikowany w BIP NASK-PIB, dzięki czemu każdy będzie mógł się z tym zapoznać.

Porozumienie będzie określało co najmniej zasady współpracy stron porozumienia – mogą to być m.in. szczegółowe kwestie techniczne.

Przedsiębiorca telekomunikacyjny będący stroną porozumienia będzie miał uprawnienie do uniemożliwienia użytkownikom internetu dostępu do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę ostrzeżeń. Będzie to polegało na usunięciu nazw domenowych z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych, służących do zamiany nazw domen internetowych na adresy IP. W takim przypadku przedsiębiorca telekomunikacyjny przekieruje połączenia odwołujące się do nazw domenowych wpisanych na listę ostrzeżeń do strony internetowej prowadzonej przez CSIRT NASK zawierającej komunikat skierowany do użytkowników internetu, zawierający w szczególności informacje o lokalizacji listy ostrzeżeń, wpisaniu szukanej nazwy domeny internetowej na listę ostrzeżeń oraz o możliwej próbie wyłudzenia danych lub niekorzystnego

rozporządzania mieniem. Użytkownik internetu uzyska wtedy informację o zablokowaniu domeny i przyczynie zablokowania.

Zdecydowano się wprowadzić uprawnienie do blokowania domen internetowych na listę ostrzeżeń, ponieważ wprowadzenie obowiązku blokowania domen wpisanych na dwóch różnych listach[30] mogłoby spowodować niejasność co do wykonywania tego obowiązku, jeżeli z jednej listy ta sama domena byłaby wpisywana, a z drugiego wypisywana.

Art. 14.

Projekt przewiduje procedurę odwoławczą dla podmiotu posiadającego tytuł prawny do domeny internetowej, która została wpisana na listę ostrzeżeń. W ten sposób zabezpieczone zostaną prawa podmiotów, których domeny zostały niezasadnie wpisane na listę ostrzeżeń.

Sprzeciw będzie zawierał:

1) wskazanie domeny internetowej, której dotyczy,
2) uzasadnienie wyjaśniające, dlaczego wpisanie domeny na listę ostrzeżeń było niezasadne oraz
3) dane identyfikujące podmiot składający sprzeciw:
    a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych,
    b) nazwę (firmę) podmiotu, adres siedziby, numer z właściwego rejestru, w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej,
    c) imię i nazwisko osoby uprawnionej do reprezentowania podmiotu posiadającego tytuł prawny do domeny internetowej wraz z upoważnieniem.

Informacje te będą niezbędne dla Prezesa UKE przy dokonywaniu oceny, czy rzeczywiście dana domena internetowa stanowi zagrożenie.

Sprzeciw będzie opatrywany kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Wnoszony będzie na adres do doręczeń elektronicznych Prezesa

[30] Jedna z projektowanej ustawy, a druga to funkcjonujący na podstawie art. 15f ustawy z dnia 19 listopada 2009 r. o *grach hazardowych* (Dz. U. z 2023 r. poz. 227) Rejestr domen służących do oferowania gier hazardowych niezgodnie z ustawą.

UKE. Rozwiązanie to usprawni rozpatrywanie spraw, jak również umożliwi precyzyjne wskazanie momentu, od którego liczą się terminy na rozpatrzenie sprzeciwu.

Sprzeciw niespełniający powyższych wymagań Prezes UKE pozostawi bez rozpoznania.

Art. 15.

Przepis określa obowiązki Prezesa UKE oraz CSIRT NASK związane z procedurą odwoławczą dotyczącą domeny internetowej wpisanej na listę ostrzeżeń. Prezes UKE będzie obowiązany rozpatrzyć sprzeciw co do zasady w terminie 14 dni od dnia jego otrzymania. W ramach tej procedury Prezes UKE będzie dokonywał oceny, czy dana domena internetowa rzeczywiście służy do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników internetu. W przypadku gdyby okazało się, że domena internetowa nie służy do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników internetu, Prezes UKE, uwzględniając sprzeciw, nakaże CSIRT NASK usunięcie domeny z listy ostrzeżeń.

To rozwiązanie stanowi gwarancję, że na liście ostrzeżeń nie będą znajdowały się strony błędnie zidentyfikowane jako niebezpieczne.

Tak jak w przypadku sprzeciwu, o którym mowa w art. 7 projektu, wyłącza się stosowanie przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego do sprzeciwów od wpisania domeny na listę ostrzeżeń. Zdecydowanie przyśpieszy to rozpatrywanie danej sprawy. Wskazać należy, że w samym tylko okresie od stycznia 2022 r. do listopada 2022 r. CSIRT NASK zidentyfikował łącznie 38 999 domen, które mają na celu wprowadzenie w błąd użytkowników internetu i wyłudzenie ich danych i środków finansowych. Dla przykładu można założyć, że od wpisania 1% tych domen zostałby złożony sprzeciw. Oznaczałoby to 390 postępowań administracyjnych prowadzonych przez Prezesa UKE. Byłoby to znaczne obciążenie organizacyjne dla tego organu – z tego powodu wyłącza się stosowanie przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeksu postępowania administracyjnego do tych spraw. Zdaniem projektodawcy sprzeciw będzie tzw. inną czynnością z zakresu administracji publicznej, która podlega kontroli sądu administracyjnego. Prawa podmiotów dysponujących tytułem prawnym do domeny, która została wpisana niezasadnie na listę ostrzeżeń, będą chronione przez możliwość złożenia skargi na sprzeciw do sądu administracyjnego.

Art. 16.

W art. 16 uregulowana została kwestia ochrony użytkowników końcowych przed nadużyciami komunikacji elektronicznej przez nakazanie, w drodze decyzji, zablokowania dostępu do numeru lub usługi w terminie nie krótszym niż 6 godzin od ogłoszenia tej decyzji, a także wstrzymania pobierania opłat za połączenia lub usługi zrealizowane po upływie tego terminu. Powyższe obowiązki nakładane są w drodze decyzji Prezesa UKE, której nadaje się rygor natychmiastowej wykonalności. Decyzja w powyższym zakresie może być ogłoszona ustnie przedsiębiorcy komunikacji elektronicznej. Decyzja ogłoszona ustnie doręczana jest stronie na piśmie w terminie 14 dni od dnia jej ogłoszenia. Wprowadzenie możliwości ustnego ogłoszenia decyzji ma za zadanie umożliwienie Prezesowi UKE i przedsiębiorcy komunikacji elektronicznej szybkiego reagowania na pojawiające się nadużycia.

Art. 17.

Jak wynika z danych statystycznych, 68,3% Polaków w przedziale wiekowym 16–74 lata korzysta z poczty elektronicznej[31]. Oprócz korzyści z tego środka komunikacji elektronicznej, na użytkowników poczty czyhają również zagrożenia. Protokół SMTP, używany do wysyłania poczty elektronicznej, nie zakładał pierwotnie możliwości uwierzytelnienia wysyłanych wiadomości. W konsekwencji jest możliwa sytuacja, w której nadawca wiadomości może wskazać inny adres zwrotny (*From adres)* niż jego prawdziwy adres. Często wykorzystują to oszuści, próbując podszyć się pod zaufane instytucje i wyłudzić dane od użytkowników poczty elektronicznej, stosując ataki phishingowe. Możliwy jest również atak typu *man in the middle,* w którym przestępca modyfikuje treść wiadomości w trakcie jej przesyłania[32].

Mechanizm SPF - Sender Policy Framework[33] jest jednym ze środków przeciwdziałania tego typu zagrożeniom. Polega on na wpisaniu w DNS odpowiedniego rekordu, w którym wskazane zostaną adresy IP lub nazwy domenowe serwera, które mogą wysyłać pocztę elektroniczną z danej domeny. Serwer pocztowy odbiorcy, odbierając wiadomość, sprawdza, czy adres IP lub

---

[31] Mały rocznik statystyczny Polski 2022, str. 259, https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/maly-rocznik-statystyczny-polski-2022,1,24.html.

[32] Stephen J. Nightingale. Email Authentication Mechanisms: DMARC, SPF and DKIM. US Department of Commerce, National Institute of Standards and Technology, 2017, str. 4 https://doi.org/10.6028/NIST.TN.1945.

[33] S. Kitterman, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, Request for Comments, RFC 7208, Internet Engineering Task Force, 2014. https://datatracker.ietf.org/doc/html/rfc7208.

nazwa domenowa serwera, z których została wysłana wiadomość, zgadza się z rekordem SPF dla danej domeny. Jeżeli nie, to taka wiadomość może być oznaczona jako spam albo zablokowana przez serwer odbiorcy. Kolejnym mechanizmem uwierzytelniania jest DKIM - DomainKeys Identified Mail[34]. Pozwala on na cyfrowe podpisanie wiadomości email pochodzącej z konkretnej domeny. Klucz publiczny, niezbędny do uwierzytelnienia wiadomości, zostanie zawarty w odpowiednim rekordzie DNS, właściwym dla danej domeny. Sprawdzając podpis, serwer odbiorcy jest w stanie sprawdzić, czy wiadomość nie została zmodyfikowania podczas przesyłania. Jeżeli klucz publiczny nie pasuje do klucza prywatnego, którym została podpisana otrzymana wiadomość, oznacza to jej nieuprawnioną modyfikację[35].

Mechanizm DMARC - *Domain-based Message Authentication Reporting and Conformance*[36] korzysta z dwóch poprzednich mechanizmów. Pozwala on na uwierzytelnienie wiadomości email, określenie zalecanych działań, które ma podjąć serwer odbiorcy z wiadomością, która nie zostanie uwierzytelniona, zbiera także informacje o wiadomościach wysłanych z konkretnych domen. Dzięki temu może automatycznie przekazywać administratorom tych domen raporty o nieuprawnionym wykorzystaniu tych domen do przesłania fałszywych wiadomości. Co za tym idzie, administratorzy tych domen mogą zorientować się, czy mechanizmy SPF/DKIM/DMARC zostały odpowiednio skonfigurowane i ewentualnie wprowadzić poprawki[37].

Są to powszechnie uznane i skuteczne mechanizmy uwierzytelniania poczty elektronicznej. Wskazać należy, że Departament Bezpieczeństwa Narodowego USA nakazał agencjom federalnym stosowanie mechanizmu uwierzytelniania poczty elektronicznej DMARC[38]. Ponadto brytyjskie[39], australijskie[40] oraz duńskie[41] służby odpowiedzialne za cyberbezpieczeństwo zalecają stosowanie tych mechanizmów.

Z tych powodów projekt ustawy proponuje nałożenie na dostawców poczty elektronicznej dla:

---

34 M. Kucherawy, D. Crocker, T. Hansen, DomainKeys Identified Mail (DKIM) Signatures, Request for Comments, RFC 6376, Internet Engineering Task Force, 2011. https://datatracker.ietf.org/doc/html/rfc6376.

35 Stephen J. Nightingale, *op. cit.*, str. 6-7.

36 M. Kucherawy, E. Zwicky, *Domain-based Message Authentication, Reporting, and Conformance (DMARC)*, Request for Comments, RFC 7489, Internet Engineering Task Force, 2015. https://datatracker.ietf.org/doc/html/rfc7489.

37 Stephen J. Nightingale, *op. cit.*, str. 7.

38 https://www.cisa.gov/sites/default/files/bod-18-01.pdf.

39 https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/configure-anti-spoofing-controls-.

40 https://www.cyber.gov.au/acsc/view-all-content/publications/how-combat-fake-emails.

41 https://www.cfcs.dk/da/nyheder/2017/vejledning-dmarc-kan-reducere-antallet-af-falske-mails/.

- co najmniej 500 000 użytkowników,
- podmiotów publicznych

obowiązku stosowania mechanizmów SPF, DKIM oraz DMARC (ust. 1) przy świadczeniu poczty elektronicznej.

Obowiązek ten nie wyklucza stosowania uzupełniająco innych mechanizmów uwierzytelniania poczty elektronicznej.

Ponadto na podmiot publiczny zostanie nałożony obowiązek korzystania z poczty elektronicznej wykorzystującej powyższe mechanizmy (ust. 2).

Nałożenie tych obowiązków efektywnie przełoży się na zmniejszenie liczby incydentów związanych z phishingiem stosowanym wobec użytkowników poczty elektronicznej, a w szczególności pracowników podmiotów publicznych, którzy są wysoce narażeni na phishing z uwagi na pełnione przez nich funkcje. Dzięki wprowadzonym rozwiązaniom zmniejszy się także liczba oszustw związanych z podszywaniem się pod inne instytucje przy wysyłaniu wiadomości email.

Kontrolę realizacji ww. obowiązków zarówno przez dostawców poczty elektronicznej, jak i podmiotów publicznych, będzie sprawować Prezes UKE. Kontrola będzie prowadzona zgodnie z przepisami rozdziału 2 działu X ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (ust. 3 i 4).

Mechanizmy SPF/DKIM/DMARC zostały ustandaryzowane w formie dokumentów *Request for Comments* wydawanych przez międzynarodową organizację *Internet Engineering Task Force*. Co jakiś czas dokumentacja jest aktualizowana i wydawana jest nowa wersja dokumentacji – stąd też zasadne jest, aby na CSIRT NASK został nałożony obowiązek wskazania na swojej stronie internetowej ostatniej aktualnej wersji tej dokumentacji. Przełoży się to na klarowność obowiązków dla dostawców poczty elektronicznej (ust. 5).

Uzyskanie dostępu do wielu usług komunikacji elektronicznej, w tym do poczty elektronicznej, wymaga identyfikacji, czyli zadeklarowania tożsamości podmiotu, uwierzytelnienia, czyli potwierdzenia tej tożsamości, oraz autoryzacji, czyli udzielenia prawa dostępu do danych. Do korzystania z poczty elektronicznej powszechnie wykorzystywane jest uwierzytelnianie jednoskładnikowe, za pomocą loginu i hasła. Jest ono niewystarczające. Przestępcy mogą użyć wielu rodzajów cyberataków w celu uzyskania dostępu do konta poczty elektronicznej – np. ataki typu *brute force* czy *phishing*. Często użytkownicy poczty elektronicznej korzystają z

bardzo podobnych haseł, co osłabia ich skuteczność. Dlatego wiele organizacji zajmujących się cyberbezpieczeństwem zaleca stosowanie uwierzytelniania wieloskładnikowego. Wyróżnia się trzy rodzaje składników uwierzytelniania:

1) coś co wiesz – np. hasło lub numer PIN;

2) coś, co posiadasz – karty inteligentne, tokeny, urządzenia kryptograficzne;

3) coś, czym jesteś – odciski palców, wizerunek, głos.

Szczególnie zagrożone na ataki ukierunkowane na przejęcie dostępu do poczty elektronicznej są podmioty publiczne. Realizują one każdego dnia wiele zadań publicznych na rzecz obywateli. Przejęcie przez przestępców dostępu do poczty elektronicznej tych podmiotów może w znaczący sposób utrudnić realizację zadań oraz narazić dane o obywatelach na upublicznienie.

Z tego powodu proponuje się nałożenie obowiązku po stronie dostawcy poczty elektronicznej dla podmiotu publicznego, aby oferował pocztę elektroniczną z możliwością stosowania metod uwierzytelniania wieloskładnikowego (ust. 6). Nie chodzi tutaj o zapewnienie przez tego dostawcę fizycznych kluczy typu U2F czy aplikacji z kodami uwierzytelniającymi, a jedynie o możliwość ich wdrożenia. Przepis nie nakłada obowiązku świadczenia konkretnej metody uwierzytelniania wieloskładnikowego. Może to być dwuskładnikowe uwierzytelnianie lub uwierzytelnianie z wykorzystaniem większej liczby składników. Powyższe obowiązki nie są równoznaczne z obowiązkiem korzystania przez podmiot publiczny z poczty elektronicznej posiadającej te funkcjonalności – istotne jest, aby dostawca poczty elektronicznej miał w swoim portfolio tego rodzaju usługi.

Art. 18.

Przepis art. 18 nakłada na przedsiębiorców telekomunikacyjnych obowiązek rejestracji danych o niewykonanych usługach w związku z blokowaniem krótkich wiadomości tekstowych, w zakresie umożliwiającym rozpatrzenie reklamacji. Przedsiębiorca będzie przechowywać te dane przez okres 12 miesięcy, a w przypadku gdy zostanie wniesiona reklamacja – przez cały okres niezbędny do rozstrzygnięcia sporu. Bieg terminu 12 miesięcy będzie się rozpoczynał od

dnia, w którym usługa miała być wykonana. Przepis ten umożliwi skuteczne przeprowadzenie postępowania reklamacyjnego.

Art. 19.

W art. 19 ust. 1 projektu wskazano, jakie uprawnienia przysługują przedsiębiorcom telekomunikacyjnym w zakresie przetwarzania i wzajemnego udostępniania informacji, w tym informacji objętych tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. Przetwarzanie komunikatu i wzajemne jego udostępnianie będzie natomiast możliwe w celu identyfikacji, zapobiegania i zwalczania smishingu, a także złośliwych wiadomości MMS, o których mowa w art. 8 ust. 2 projektu.

W tym miejscu należy podkreślić, że przetwarzanie treści komunikatu może stanowić bardzo istotną ingerencję w prawo do prywatności. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201 z 31.7.2002, s. 37, z późn. zm.) w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadki wynikające z prawa Unii Europejskiej lub prawa krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 ww. dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej. Mając na względzie powyższe, zdecydowano się na ograniczenie możliwości przetwarzania komunikatu wyłącznie do nadużycia w postaci smishingu, a także złośliwych wiadomości MMS, o których mowa w art. 8 ust. 2. W przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-u jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do celu, jakim jest ochrona przed nadużyciami. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Dodatkowo w

przypadku smishingu – jako nadużycia zdefiniowanego i szerzej opisanego w projekcie ustawy, wprowadza się regulację „wzorca wiadomości", wraz z należytymi uprawnieniami podmiotów (CSIRT NASK). Przedsiębiorcy uprawnieni będą do blokowania wiadomości SMS po porównaniu jej ze wzorcem określonym przez CSIRT NASK lub po automatycznej identyfikacji wykonywanej w oparciu o system informatyczny przedsiębiorcy. Przetwarzanie komunikatu elektronicznego będzie zatem ograniczone wyłącznie do zwalczania nadużyć ściśle w ustawie określonych.

Zgodnie z ust. 2 przetwarzanie treści SMS oraz MMS będzie następowało w celu realizacji obowiązków blokowania w zakresie smishingu, uprawnienia do blokowania złośliwych wiadomości MMS, a także na cele związane z dochodzeniem roszczeń. Nie podlega ingerencji treść wiadomości.

W ust. 3 i 4 wymienione zostały informacje, do przetwarzania których przedsiębiorca telekomunikacyjny jest uprawniony, wraz ze wskazaniem celu przetwarzania oraz okresu, do kiedy ich przetwarzanie jest dopuszczalne – jako moment graniczny wskazując koniec terminu, w którym możliwe jest dochodzenie roszczeń.

Przepis ust. 5 zawiera wyłączenie stosowania art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 2016/679", w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. Przepis ten jest bezpośrednio powiązany z przepisem ust. 3 dotyczącym możliwości wymiany informacji między przedsiębiorcami i bazuje na podobnych rozwiązaniach z rynku bankowego (art. 106e ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2022 r. poz. 2324, z późn. zm.) oraz ubezpieczeń (art. 35a ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2022 r. poz. 2283, z późn. zm.), które to rozwiązania zostały wprowadzone w ramach tzw. ustawy wdrażającej rozporządzenie 2016/679 (ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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. U. poz. 730). Proponowany ustęp wyłącza stosowanie art. 14 i art. 15 rozporządzenia 2016/679.

Przepis art. 15 rozporządzenia 2016/679 ustanawia natomiast prawo osoby, której dane dotyczą, do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, prawo do uzyskania dostępu do tych danych oraz innych informacji (m.in. o celach przetwarzania, odbiorcach, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle). Wyłączenie stosowania art. 15 rozporządzenia 2016/679 będzie miało zastosowanie jedynie w przypadku, gdy przetwarzanie danych będzie niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. Nadużycia w komunikacji elektronicznej stanowią z perspektywy prawa karnego przestępstwa, z tego względu proponowane wyłączenie jest zgodne z art. 23 ust. 1 lit. d oraz e rozporządzenia 2016/679. Brak wprowadzonego wyłączenia i realizowanie obowiązku powiadomienia osób działających w celach przestępczych o przetwarzaniu ich danych osobowych mógłby niweczyć cel ustawy (jakim jest walka z nadużyciami). Realizacja prawa dostępu do informacji o przetwarzanych danych mogłaby dostarczyć potencjalnemu podmiotowi, który dopuszcza się nadużyć, informacji o podejmowanych przez przedsiębiorców działaniach mających na celu wykrycie nadużycia. Narażałoby również administratora na zarzut utrudnienia prowadzonego, wobec osób dopuszczających się nadużyć, postępowania karnego. Z tego względu wprowadzone wyłączenie należy uznać za niezbędne i proporcjonalne do celu, jakim jest walka z nadużyciami.

Ponadto należy wskazać, że art. 23 ust. 2 rozporządzenia 2016/679 określa przepisy, jakie powinien zawierać akt prawny, który ogranicza stosowanie m.in. art. 15 tego rozporządzenia. Zgodnie z tym przepisem akt prawny, który ma wprowadzać ograniczenia w przepisach dotyczących zakresu praw i obowiązków, w tym art. 15 rozporządzenia 2016/679, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – dotyczące: celów przetwarzania lub kategorii przetwarzania, kategorii danych osobowych, zakresu wprowadzonych ograniczeń, zabezpieczeń zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, określenia administratora lub kategorii administratorów, okresów przechowywania oraz mających zastosowanie zabezpieczeń z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania, ryzyk

naruszenia praw lub wolności osoby, której dane dotyczą, oraz prawa osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Wymogi z art. 23 ust. 2 rozporządzenia 2016/679, w odniesieniu do wyłączenia stosowania art. 15 tego rozporządzenia w projektowanym przepisie, będą spełnione zasadniczo w oparciu o zabezpieczenia i ochronę wynikającą z przepisów o tajemnicy telekomunikacyjnej. W tym względzie należy wskazać, że w celu wykrywania i zwalczania nadużyć przedsiębiorcy telekomunikacyjni będą przetwarzać dane objęte tajemnicą telekomunikacyjną (których katalog znajduje się w art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne). Będą to zatem dane dotyczące użytkownika, treść indywidualnych komunikatów, dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów elektronicznych w sieciach telekomunikacyjnych lub naliczania opłat za usługi komunikacji elektronicznej, dane o lokalizacji, a także dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń. Przetwarzanie będzie następowało, jak wskazano w projektowanym przepisie, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. Przepis ust. 5 wyraźnie wskazał zakres wprowadzanych ograniczeń, tj. wyłączenie stosowania art. 15 rozporządzenia 2016/679. Dane będą przetwarzane przez przedsiębiorców telekomunikacyjnych, a także organy uprawnione do ścigania przestępstw, na podstawie odrębnych przepisów. Kwestie dotyczące zabezpieczenia danych przed nadużyciami, niezgodnym z prawem dostępem, ryzyka naruszenia praw wynikać będą z generalnego zakazu przetwarzania informacji objętych tajemnicą komunikacji elektronicznej, o którym mowa w art. 159 ust. 2 pkt d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, przez osoby inne niż nadawca i odbiorca komunikatu elektronicznego, z wyjątkami wskazanymi w tej ustawie, lub gdy będzie to konieczne z innych powodów przewidzianych przepisami odrębnymi (jako przepisy odrębne należy uznać niniejszą ustawę). Ochronę przed niezgodnym z prawem dostępem zapewnia również przepis art. 174^1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, zgodnie z którym dostawca usług komunikacji elektronicznej obowiązany jest wdrożyć odpowiednie organizacyjne i techniczne środki ochrony zapewniające bezpieczeństwo przetwarzania danych osobowych. Przepis wymienia przy tym środki ochrony jakie należy wdrożyć, niezależnie od wymogów wskazanych w rozporządzeniu 2016/679. Okres przechowywania danych wynika z ogólnych

przepisów dotyczących retencji danych wskazanych w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, a dodatkowo z regulacji art. 18 i art. 19 projektowanej ustawy.

W odniesieniu natomiast do wymogu zawarcia przepisu o prawie osoby, której dane dotyczą, do uzyskania informacji o ograniczeniach, należy wskazać, że z brzmienia samego już ust. 5 wynika zakres i cel ograniczenia prawa do informacji. Ponadto przepis art. 23 ust. 2 lit. h rozporządzenia 2016/679 zawiera dopisek „o ile nie narusza to celu ograniczenia". Celem wprowadzanego ograniczenia, tj. wyłączenia prawa dostępu do informacji o przetwarzanych danych, jest uniemożliwienie dostarczenia potencjalnemu podmiotowi, który dopuszcza się nadużyć informacji o podejmowanych przez przedsiębiorców działaniach mających na celu wykrycie nadużycia. Udzielanie informacji o przetwarzaniu jego danych osobowych mogłoby niweczyć cel, jakim jest walka z nadużyciami. Wydaje się zatem, że również udzielenie szczegółowej informacji o samych ograniczeniach mogłoby także naruszać cel tego ograniczenia.

Przepis art. 14 rozporządzenia 2016/679 zawiera katalog informacji podawanych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą. Podczas działań mających na celu zwalczanie nadużyć i zapobieganie im w komunikacji elektronicznej przedsiębiorca telekomunikacyjny może pozyskać wiele tego rodzaju danych osobowych. Poinformowanie każdej takiej osoby odrębnie może być niemożliwe do wykonania. Dlatego przepis ust. 6 pozwala przedsiębiorcy telekomunikacyjnemu na podanie informacji wymaganych przez art. 14 rozporządzenia 2016/679 na swojej stronie internetowej lub przez umieszczenie stosownych informacji w miejscach widocznych w siedzibie lub miejscu działania administratora danych osobowych, w zakresie, w jakim dotyczy to danych osobowych pozyskanych w ramach identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.

Art. 20.

Przepis art. 20 zawiera przepisy związane z administracyjnymi karami pieniężnymi.

Sztuczny ruch, smishing, CLI spoofing czy nieuprawniona zmiana informacji adresowej powodują istotne szkody po stronie użytkowników końcowych oraz przedsiębiorców telekomunikacyjnych. Dlatego zakaz tych nadużyć powinien być obwarowany sankcją. Z tego powodu uprawnia się Prezesa UKE do nakładania administracyjnej kary pieniężnej na przedsiębiorców telekomunikacyjnych, którzy dopuszczają się tych nadużyć. Dzięki temu

Prezes UKE będzie w stanie reagować na pojawiające się nadużycia (ust. 1). Kara ta będzie miała charakter odstraszający oraz represyjny. Jednocześnie wyłącza się nakładanie tej kary na przedsiębiorcę telekomunikacyjnego, który jest osobą fizyczną – wprowadza się przepis, zgodnie z którym osoba fizyczna, za czyn wyczerpujący znamiona nadużycia w komunikacji elektronicznej oraz przestępstwa, podlega wyłącznie odpowiedzialności karnej (ust. 2)[42]. Jest to spowodowane tym, że tacy przedsiębiorcy będą odpowiadali karnie za dopuszczanie się nadużyć z art. 22–25 niniejszego projektu ustawy oraz z innych artykułów ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2022 r. poz. 1138, z późn. zm.) (np. art. 286 – oszustwo, art. 287 – oszustwo komputerowe). Gdyby jeszcze Prezes UKE nakładał za ten sam czyn na tę samą osobę administracyjną karę pieniężną, to doszłoby do naruszenia konstytucyjnej zasady *ne bis in idem* oraz zasady proporcjonalnej reakcji państwa na naruszenie prawa, wynikających z art. 2 Konstytucji Rzeczypospolitej Polskiej[43].

Administracyjną karę pieniężną wprowadza się za cztery wyżej nazwane nadużycia w komunikacji elektronicznej, ponieważ są to obecnie najczęściej występujące postaci nadużyć. Za pozostałe przypadki nadużyć konkretny podmiot będzie mógł, na zasadach ogólnych, podlegać odpowiedzialności karnej, jeżeli będzie to przestępstwo, np. oszustwo. Zdaniem projektodawcy możliwa jest też odpowiedzialność cywilna, także na zasadach ogólnych określonych w ustawie z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2022 r. poz. 1360, z późn. zm.).

Fakultatywnej administracyjnej karze pieniężnej będą podlegali:

- przedsiębiorca telekomunikacyjny, który nie wypełnia obowiązków wskazanych w art. 5, art. 9 i art. 10 ust. 15 lub 16,
- dostawca poczty elektronicznej, który nie wypełnia obowiązków wskazanych w art. 17 ust. 1,

jeżeli przemawia za tym zakres lub charakter naruszenia. Takie określenie jest niezbędne, aby zapewnić proporcjonalność w rozumieniu konieczności i adekwatności nakładanej kary do zakresu naruszenia. Może się również okazać, że działanie bądź zaniechanie podmiotu przejawia znikomą szkodliwość społeczną, wobec czego niecelowe byłoby obligatoryjne

[42] Przepis opracowano, wzorując się na art. 92a ust. 9 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2022 r. poz. 2201).

[43] Por. wyrok Trybunału Konstytucyjnego z dnia 20 czerwca 2017 r. sygn. akt P 124/15.

karanie kierującego podmiotem. Wyjaśnienia wymagają jednak pojęcia „zakres naruszenia" oraz „charakter naruszenia". Zakres naruszenia można zdefiniować jako rozmiar naruszenia oraz częstotliwość naruszeń. Zakres naruszenia jest niezbędny do określenia stopnia szkodliwości społecznej czynu sprawcy, a więc pozwala na określenie rzeczywistych oraz potencjalnych skutków naruszenia prawa. Ze względu na to, że jest to pojęcie o charakterze stopniowalnym, dokonując oceny, organ nakładający karę administracyjną powinien brać pod uwagę w szczególności podstawowe cele ustawy oraz szkodliwość naruszenia, tj. rodzaj naruszonych obowiązków i dóbr, intensywność naruszenia, następstwa oraz wysokość wyrządzonej szkody[44]. Charakter naruszenia należy rozumieć jako stopień zawinienia osoby podlegającej odpowiedzialności karnoadministracyjnej, tj. czy czyn został przez nią popełniony z winy umyślnej lub nieumyślnej[45]. Określając zatem charakter naruszenia, organ obowiązany jest do ustalenia, czy osoba podlegająca odpowiedzialności karnoadministracyjnej w tym przypadku popełniła ten czyn w zamiarze bezpośrednim, ewentualnym, poprzez lekkomyślność albo niedbalstwo. Od tego ustalenia zależeć będzie właśnie decyzja o odstąpieniu od nałożenia kary bądź o jej nałożeniu oraz wysokości.

Wzorem art. 209 ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne wprowadzono możliwość nałożenia kary na kierującego przedsiębiorstwem telekomunikacyjnym za niewykonanie obowiązków związanych ze zwalczaniem smishingu oraz CLI spoofing (ust. 6). Takie rozwiązanie ma charakter prewencyjny – poprzez widmo grożącej kary kierujący przedsiębiorstwem telekomunikacyjnym będzie mniej skłonny do zaniedbywania obowiązków wynikających z ustawy.

Ponadto w art. 20 ust. 7 wprowadzona została możliwość nałożenia kary na kierownika podmiotu publicznego – piastuna funkcji, jeżeli nie zostały wdrożone mechanizmy uwierzytelniania poczty elektronicznej SPF/DKIM/DMARC. Można sobie wyobrazić sytuację, w której mimo nałożenia kary na podmiot publiczny obowiązek nadal nie jest wykonywany. Dlatego powinna być możliwość ukarania kierownika tego podmiotu, co powinno wywołać odpowiedni efekt prewencyjny.

Należy jednak zauważyć, że odpowiedzialność kierownika podmiotu w myśl tego przepisu jest odpowiedzialnością na zasadzie winy. Nie powinien podlegać odpowiedzialności kierownik

---

[44] M. Czyżak, Fakultatywna odpowiedzialność karnoadministracyjna w świetle nowelizacji prawa telekomunikacyjnego z 10 maja 2018 r, internetowy Kwartalnik Antymonopolowy i Regulacyjny, nr 3(8), 2019, s. 69-70.

[45] Ibidem, s. 70.

podmiotu, który dołożył należytej staranności i zawarł umowę z dostawcą poczty elektronicznej, a dostawca ten zaprzestał stosowania mechanizmów SPF/DKIM/DMARC.

Do postępowania w sprawie nałożenia kar pieniężnych, o których mowa w art. 20 niniejszego projektu ustawy, będą stosowane przepisy działu Administracyjne kary pieniężne ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Dział IVA tej ustawy reguluje między innymi przesłanki nakładania administracyjnej kary pieniężnej, przesłanki odstąpienia od kary i skutki naruszenia prawa wywołanego działaniem siły wyższej. Niniejszy projekt ustawy nie wyłącza tych przepisów. Nakładając karę administracyjną pieniężną, organ właściwy zobowiązany jest zatem stosować przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Zastosowanie znajdą zatem przesłanki wymiaru kary (waga i okoliczność naruszenia prawa, stopień przyczynienia się strony do naruszenia prawa, jak również dobrowolne działania strony mające na celu uniknięcie skutków naruszenia prawa), wskazane w art. 189d ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, jak również wskazanie, że strona nie podlega ukaraniu, jeżeli naruszenie prawa spowodowane było działaniem siły wyższej[46] (art. 189e ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego). Możliwe jest również odstąpienie od nałożenia administracyjnej kary pieniężnej w drodze decyzji i poprzestanie na pouczeniu strony, jeżeli waga naruszenia prawa jest znikoma, a strona zaprzestała naruszania prawa albo za to samo zachowanie strona już została ukarana w innym trybie (art. 189f § 1 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego). W innych przypadkach (art. 189f § 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego) organ może wyznaczyć stronie (w drodze postanowienia) termin na przedstawienie dowodów potwierdzających usunięcie naruszenia prawa lub powiadomienia właściwych podmiotów o stwierdzonym naruszeniu prawa. Organ, w tym przypadku Prezes UKE, będzie mógł tak zrobić, jeżeli uważa, że będzie to lepsze ze względu na cele, dla których kara miała być nałożona. Po przedstawieniu dowodów wykonania tych czynności organ odstępuje od wymierzenia kary w drodze decyzji.

Tak jak w przypadku ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne od decyzji Prezesa UKE w sprawie nałożenia kar będzie przysługiwało odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

---

[46] Siłą wyższą jest nadzwyczajne, zewnętrzne i niemożliwe do zapobieżenia zdarzenie.

Art. 21.

Przepisy art. 21 dotyczą:

- sposobu nakładania kary – w drodze decyzji Prezesa UKE,
- wymiaru kary – do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym,
- przesłanek ustalenia wysokości kary – uwzględnianie zakresu naruszenia, dotychczasowej działalności podmiotu oraz jego możliwości finansowych,
- sposobu obliczenia przychodu podmiotu na potrzeby obliczenia wymiaru kary.

Przepisy te nawiązują do art. 210 ustawy dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Zakłada się, że decyzji o nałożeniu kary nie będzie nadawany rygor natychmiastowej wykonalności.

Wpływy z tych kar będą stanowiły dochód budżetu państwa, w myśl art. 111 pkt 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, z późn. zm.), (projektowany art. 21 ust. 9).

Przepisy ust. 3–8 regulują kwestie związane z określaniem wymiaru kary, w przypadku gdy organ nie dysponuje danymi finansowymi pozwalającymi obliczyć wysokość kary. W takim przypadku Prezes UKE, nakładając karę pieniężną, uwzględnia:

1) przychód osiągnięty przez podmiot w roku kalendarzowym poprzedzającym ten rok;
2) w przypadku, o którym mowa w ust. 2 – średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających ten rok.

Podmiot jest obowiązany do dostarczenia Prezesowi UKE, na każde jego żądanie, w terminie 30 dni od dnia otrzymania tego żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku niedostarczenia danych lub gdy dostarczone dane uniemożliwiają ustalenie podstawy wymiaru kary, Prezes UKE może ustalić podstawę wymiaru kary pieniężnej w sposób szacunkowy, nie mniejszą jednak niż kwota 500 000 zł.

W przypadku gdy podmiot nie osiągnął przychodu w okresie, o którym mowa w ust. 2, lub gdy przychód podmiotu w tym okresie nie przekracza 500 000 zł, Prezes UKE może nałożyć na podmiot karę pieniężną w wysokości nieprzekraczającej 15 000 zł.

W przypadku gdy podmiot powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu, określonego w art. 21 ust. 1, Prezes UKE uwzględnia przychód osiągnięty przez te podmioty w roku kalendarzowym poprzedzającym rok nałożenia kary.

Te rozwiązania gwarantują, że nie dojdzie do sytuacji, w której niemożliwe jest precyzyjne określenie wymiaru kary. Przy samym ustalaniu wymiaru kary Prezes UKE będzie brał pod uwagę zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe.

Art. 22–25.

Przepisy art. 22–25 wprowadzają nowy rodzaj przestępstwa, które może zostać popełnione przez każdego – jest to więc to przestępstwo powszechne. Ma ono charakter kierunkowy, ponieważ jest popełniane w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody. Dobrami chronionymi są w tym przypadku:

- mienie,
- bezpieczeństwo informacji oraz systemów informatycznych, teleinformatycznych lub sieci teleinformatycznej.

Stroną przedmiotową tych przestępstw jest dopuszczanie się sztucznego ruchu, smishingu, CLI spoofingu lub nieuprawnionej modyfikacji informacji adresowej. Przepisem tym wprowadza się penalizację ww. nadużyć w komunikacji elektronicznej. Sprawca wymienionych przestępstw będzie podlegał karze pozbawienia wolności od 3 miesięcy do lat 5 – analogicznie jak w przypadku kary za oszustwo komputerowe określone w art. 287 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. Jednocześnie wprowadza się typ uprzywilejowany tego przestępstwa: w wypadku mniejszej wagi[47] – sprawca podlega wtedy grzywnie, karze ograniczenia wolności

[47] Za orzecznictwem wskazać należy, że wypadek przestępstwa mniejszej wagi zachodzi wówczas, gdy znamiona przestępstwa, przede wszystkim przedmiotowe, cechują się niewysoką społeczną szkodliwością, zaś jego sprawca nie jest na tyle niebezpieczny dla społeczeństwa, aby stosować w stosunku do niego zwykłą karę przewidzianą za zrealizowane przez niego przestępstwo. Wyrok Sądu Apelacyjnego w Krakowie z dnia 6 listopada 2008 r. II Ka 163/08 w: Krakowskie Zeszyty Sądowe, Biuletyn Sądu Apelacyjnego w Krakowie w sprawach karnych, Rok XVIII, Grudzień 2008, nr 12, poz. 216, str. 25.

albo pozbawienia wolności do roku. Jeżeli nadużycia w komunikacji elektronicznej dokonano na szkodę osoby najbliższej[48], ściganie będzie następowało na wniosek pokrzywdzonego.

Dodać tutaj należy, że względem definicji smishingu oraz CLI spoofingu określonych w art. 3 ust. 1 pkt 2 i 3 projektu rozszerzono znamiona czynu. W obydwu przypadkach uwzględniono sytuację, w której przestępca podszywa się w celu nakłonienia odbiorcy do przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej. Ponadto w przypadku przestępstwa określonego w art. 23 projektu uwzględniono sytuację, w której przestępca wysyła wiadomości multimedialne MMS lub wiadomości za pośrednictwem innych usług komunikacji interpersonalnej. W szczególności chodzi tutaj o różnego rodzaju komunikatory internetowe czy pocztę elektroniczną.

Wskazać należy, że do tej pory czyny te były kwalifikowane w oparciu o przepisy ustawy z dnia 6 czerwca 1997 r. – Kodeks karny – przykładowo CLI spoofing był kwalifikowany jako czyn określony w art. 190a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. Wyodrębnienie tych czynów do odrębnego przepisu umożliwi prowadzenie statystyk występowania tych przestępstw, a co za tym idzie, umożliwi zmierzenie skuteczności działań państwa w zwalczaniu tego rodzaju czynów.

Art. 26.

Przepis art. 26 nakłada na Prezesa UKE obowiązek przedstawienia sejmowej komisji właściwej w sprawach telekomunikacji oraz ministrowi właściwemu do spraw informatyzacji rocznego sprawozdania z wykonywania zadań określonych w ustawie. Sprawozdanie będzie składane do 31 marca danego roku kalendarzowego, za rok poprzedni.

Zdaniem projektodawcy sprawozdanie powinno obejmować w szczególności informacje o:

- zgłaszanych do Prezesa UKE przypadkach nadużyć w komunikacji elektronicznej,
- liczbie numerów wpisanych do wykazu numerów służących wyłącznie do odbierania połączeń głosowych,

[48] Zgodnie z art. 116 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny przepisy części ogólnej tego kodeksu stosuje się do innych ustaw przewidujących odpowiedzialność karną. Znajdzie więc tutaj zastosowanie definicja osoby najbliższej zawarta w art. 115 § 11 tego kodeksu, zgodnie z którą osobą najbliższą jest małżonek, wstępny, zstępny, rodzeństwo, powinowaty w tej samej linii lub stopniu, osoba pozostająca w stosunku przysposobienia oraz jej małżonek, a także osoba pozostająca we wspólnym pożyciu.

- liczbie sprzeciwów, które wpłynęły do Prezesa UKE wraz z informacją o ich sposobie załatwienia,
- liczbie wydanych decyzji nakazujących przedsiębiorcy telekomunikacyjnemu zablokowanie dostępu do numeru,
- liczbie wszczętych postępowań w sprawie nałożenia administracyjnej kary pieniężnej za niewykonanie obowiązków wynikających z ustawy, w tym liczbie wydanych decyzji,
- wynikach przeprowadzonych kontroli wykonywania obowiązków z ustawy,
- działalności edukacyjnej Prezesa UKE w obszarze nadużyć w komunikacji elektronicznej,
- zawarciu porozumienia w sprawie listy ostrzeżeń lub jego modyfikacji,
- zawarciu porozumienia oraz wydaniu rekomendacji określających szczegółowe środki organizacyjne i techniczne służące zapobieganiu i zwalczaniu CLI spoofing.

Art. 27.

Przepis art. 27 zmienia art. 192 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, który określa zadania Prezesa UKE. W związku z tym, że niniejsza ustawa wyznacza dla Prezesa UKE szereg nowych zadań, konieczne było uwzględnienie ich w zakresie działań tego organu.

Art. 28.

Przepis zmienia ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57) , wskazując w niej, że przepisy tej ustawy nie naruszają obowiązku korzystania przez podmiot publiczny przy realizacji zadań publicznych z poczty elektronicznej wykorzystującej mechanizmy uwierzytelniania, SPF/DKIM/DMARC, o których mowa w art. 17 ust. 1 ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Rozgraniczenie to rozwiewa wątpliwości co do wzajemnej relacji tych ustaw.

Art. 29.

Konsekwencją nałożenia na CSIRT NASK nowych zadań jest wprowadzenie zmian w art. 26 ust. 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863, z późn. zm.) przez dodanie do katalogu zadań CSIRT NASK monitorowania

występowania smishingu oraz tworzenie wzorca wiadomości wyczerpującej znamiona smishingu.

Art. 30.

W art. 30 przewidziano czynności dostosowawcze związane z uruchomieniem systemu służącego udostępnianiu informacji o wzorcach wiadomości wyczerpujących znamiona smishingu. Określono trzymiesięczny termin, od dnia wejścia w życie ustawy, w jakim CSIRT NASK ma uruchomić ten system teleinformatyczny. W terminie tym CSIRT NASK również poinformuje ministra właściwego do spraw informatyzacji o uruchomieniu systemu. Następnie minister właściwy do spraw informatyzacji udostępni na swojej stronie podmiotowej w BIP informację o uruchomieniu systemu. Komendant Centralnego Biura Zwalczania Cyberprzestępczości, Prezes UKE i przedsiębiorcy będą mieli obowiązek podłączenia się do systemu w terminie 3 miesięcy od dnia udostępnienia informacji na BIP. Zakłada się, że podłączenie do systemu będzie stosunkowo proste – dostęp do niego będzie zapewniony przez specjalną stronę internetową.

Art. 31.

Przepis art. 31 wprowadza termin dla przedsiębiorców telekomunikacyjnych na wdrożenie proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.

Termin ten wynosi:

- w przypadku sztucznego ruchu oraz smishingu – 6 miesięcy,
- w przypadku CLI spoofingu oraz nieuprawnionej zmiany informacji adresowej – 12 miesięcy

od dnia wejścia w życie ustawy.

Art. 32.

Jest to przepis dostosowujący, w myśl którego strony Porozumienia o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia

epidemicznego w Rzeczypospolitej Polskiej[49], zwanego dalej „Porozumieniem z 23 marca 2020 r.", będą mogły, w terminie miesiąca od dnia wejścia w życie tego przepisu, złożyć oświadczenie woli o uznaniu tego porozumienia za porozumienie, o którym mowa w art. 13 ust. 1 projektu. Dniem uznania Porozumienia z 23 marca 2020 r. za porozumienie, o którym mowa w art. 13 ust. 1 projektu, będzie dzień złożenia oświadczenia woli przez ostatnią ze stron. Również lista ostrzeżeń[50] prowadzona przez NASK-PIB na podstawie ww. porozumienia powinna być prawnie uznana za listę, o której mowa w art. 13 ust. 1. Z uwagi na to, że powyższe porozumienie zostało zawarte na okres stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego, konieczne jest wprowadzenie przepisu uznającego postanowienia ograniczające stosowanie porozumienia do ww. stanów za bezskuteczne.

Uznanie Porozumienia z 23 marca 2020 r. za porozumienie, o którym mowa w art. 13 ust. 1 projektu, wynika z konieczności zapewnienia ciągłości funkcjonowania tej listy ostrzeżeń, na której jest wpisanych blisko 90 000 niebezpiecznych domen internetowych. Przerwa w funkcjonowaniu tej listy utrudniłaby identyfikację zagrożeń dla użytkowników internetu, co byłoby bardzo niekorzystne. Poza tym lista ta jest już ugruntowana w świadomości osób zajmujących się cyberbezpieczeństwem. Za utrzymaniem w mocy Porozumienia z 23 marca 2020 r. opowiadają się wszystkie strony tego porozumienia, wskazując na jego istotny wpływ na cyberbezpieczeństwo oraz wypracowane metody współpracy. Projektodawca, doceniając dotychczasowe działania stron Porozumienia z 23 marca 2020 r., postanowił wyjść naprzeciw postulatom zgłaszanym przez podmioty publiczne oraz prywatne i uwzględnić to porozumienie w projektowanej ustawie.

Należy zwrócić uwagę na to, że dotychczasowy stan powodował wątpliwości, która gałąź prawa reguluje porozumienia. Porozumienie można bowiem było odnieść i do umowy cywilnoprawnej i do porozumienia administracyjnoprawnego. Nadmienić należy, że zawarcie porozumienia wywoływało skutek władczy wobec podmiotu wpisanego na listę ostrzeżeń, co wskazywałoby na administracyjnoprawny charakter porozumienia. Warto jednak dodać, że tzw. porozumienie administracyjnoprawne zdaniem nauki prawa[51] powinno mieć podstawę w przepisie ustawy, np. normach kompetencyjnych. Natomiast tzw. porozumienia faktyczne, choć wywoływały skutek władczy, nie miały podstawy w przepisach ustaw czy w przepisach

[49] https://www.uke.gov.pl/akt/uke-przystapil-do-porozumienia-chroniacego-abonentow,300.html.
[50] https://cert.pl/posts/2020/03/ostrzezenia_phishing/.
[51] J. Zimmermann, Prawo administracyjne, Warszawa 2010, s. 334.

kompetencyjnych. Omawiany przepis jest tak ważny i konieczny, ponieważ jednoznacznie przesądza o administracyjnoprawnym charakterze porozumienia. Brak takiego rozwiązania powodowałby wątpliwość, czy porozumienie lub porozumienia, które zostały zawarte przed dniem wejścia w życie omawianej ustawy, są porozumieniami w rozumieniu ustawy. Z tego względu zasadne jest wprowadzenie przepisu dostosowującego, na mocy którego porozumienie faktyczne może zostać przekształcone w porozumienie prawne wolą jego stron. Takie rozwiązanie zapewni pełną zgodność działania organów państwa (i innych podmiotów) z przepisami Konstytucji Rzeczypospolitej Polskiej.

Art. 33.

W związku z wprowadzeniem obowiązków dotyczących bezpieczeństwa poczty elektronicznej konieczne było wprowadzenie przepisów regulujących kwestie umów, które podmioty publiczne już zawarły ze swoimi dostawcami. Zgodnie z art. 33 projektu dostawca poczty elektronicznej, który będzie świadczył pocztę elektroniczną na podstawie umowy, której stroną jest podmiot publiczny, obowiązującej w dniu wejścia w życie ustawy, będzie obowiązany w terminie 3 miesięcy od dnia wejścia w życie ustawy do spełnienia wymagań, o których mowa w art. 17 ust. 1 projektu, czyli wdrożenia mechanizmów SPF/DKIM/DMARC. W przypadku niespełnienia tych wymagań w tym terminie umowa ulegnie rozwiązaniu.

Art. 34.

Zgodnie z projektowanym art. 35 w terminie 6 miesięcy od wejścia w życie ustawy dostawca poczty elektronicznej, który zawarł umowę z podmiotem publicznym na świadczenie poczty elektronicznej, przedstawi ofertę poczty elektronicznej umożliwiającej stosowanie metod uwierzytelniania wieloskładnikowego, chyba że świadczona przez tego dostawcę poczta elektroniczna już umożliwia stosowanie tych metod.

Art. 35.

Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem

- art. 2 pkt 1, 5 i 10, art. 13–15 oraz art. 32, które wejdą w życie z dniem następującym po dniu ogłoszenia,
- art. 20 ust. 3 pkt 1, który wejdzie w życie po upływie 6 miesięcy od dnia wejścia w życie ustawy,

– art. 20 ust. 3 pkt 2, który wejdzie w życie po upływie 12 miesięcy od dnia wejścia w życie ustawy.

Projektowane przepisy zakładają, że podstawa prawna do nałożenia kary za niewykonanie obowiązku blokowania wiadomości wejdzie w życie po upływie 6 miesięcy od dnia wejścia w życie ustawy, a za niewykonywanie obowiązku blokowania połączeń głosowych albo ukrywania identyfikacji numeru wywołującego dla użytkownika końcowego po upływie 12 miesięcy. Terminy te są skorelowane z okresem, jaki przedsiębiorcy telekomunikacyjni mają na wdrożenie środków organizacyjnych i technicznych, które umożliwiają przeciwdziałanie odpowiednio smishingowi i spoofingowi. Wprowadzenie kar za okres poprzedzający wprowadzenie obowiązku byłoby sprzeczne z zasadą demokratycznego państwa prawnego.

Proponuje się, aby przepis (art. 32) umożliwiający złożenie oświadczenia woli przez strony Porozumienia z 23 marca 2020 r. celem uznania tego porozumienia za porozumienie z art. 13 wszedł w życie dzień po ogłoszeniu ustawy. Dzięki temu rozpocznie się bieg terminu na złożenie ww. oświadczenia woli. W przypadku uzyskania zgody wszystkich stron porozumienia taki model przyspieszy możliwość jego uznania za porozumienie z art. 13. Łącznie z omawianym przepisem wejdą w życie przepisy dotyczące listy ostrzeżeń, czyli art. 13, art. 14 oraz art. 15, a także przepisy zawierające definicje CSIRT NASK, listy ostrzeżeń oraz przedsiębiorcy telekomunikacyjnego.

Pozostałe informacje

Projekt nie jest sprzeczny z prawem Unii Europejskiej.

Projektowane przepisy zostały przeanalizowane pod kątem wpływu na małe i średnie przedsiębiorstwa.

Wpływ projektu ustawy na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych został omówiony w ocenie skutków regulacji.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2021 r. poz. 743 oraz z 2022 r. poz. 807).

Projektowana regulacja będzie poddana notyfikacji technicznej w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Projekt nie wymaga przedstawienia właściwym organom i instytucjom i Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt został udostępniony w Biuletynie Informacji Publicznej. Ponadto, z chwilą skierowania do uzgodnień, konsultacji publicznych lub opiniowania, projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny".

Nazwa projektu Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej **Ministerstwo wiodące i ministerstwa współpracujące** Kancelaria Prezesa Rady Ministrów **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa, Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** **08.02.2023 r.** **Źródło:** Inicjatywa własna Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz. Urz. UE. L 321 z 17.12.2018, str. 36, z późn. zm.) **Nr w Wykazie prac legislacyjnych i programowych RM** UD402

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych codziennie 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 lub osiągnięcie nienależnych korzyści.

W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych[1]. 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. Zjawisko to występuje pod nazwą CLI spoofing. Polega on na nieuprawnionym posłużeniu się przez użytkownika (często przestępcę) wywołującego połączenie głosowe numerem wskazującym na inną osobę lub instytucję, po to, aby wywołać strach, podszyć się pod tą osobę albo instytucję i dzięki temu móc łatwiej nakłonić ofiarę (tj. odbiorcę takiego połączenia) do określonego działania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji złośliwego oprogramowania.

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 przez kliknięcie w link w wiadomości[2]. Zjawisko to występuje pod nazwą smishingu. Od kwietnia 2021 r. do początku czerwca 2022 r. zespół CSIRT NASK zidentyfikował 31 054 krótkie wiadomości tekstowych, mające znamiona smishingu. Problem został także dostrzeżony na poziomie międzynarodowym. Międzynarodowy Związek Telekomunikacyjny (ITU) wydał rekomendacje, zgodnie z którymi dostawcy usług telefonii komórkowych powinni zapewnić system przeciwdziałania atakom typu smishing[3].

Z problemem złośliwych wiadomości SMS zmagają się także integratorzy usług SMS A2P (application to person). Są to masowo wysyłane SMS, przez aplikacje. Jako przykłady można wskazać powiadomienia bankowe, alerty, autoryzacje, automatyczne potwierdzenia rezerwacji, powiadomienia marketingowe. Liczba wysyłanych SMS A2P rośnie - w 2020 r. wyniosła 3,8 mld.

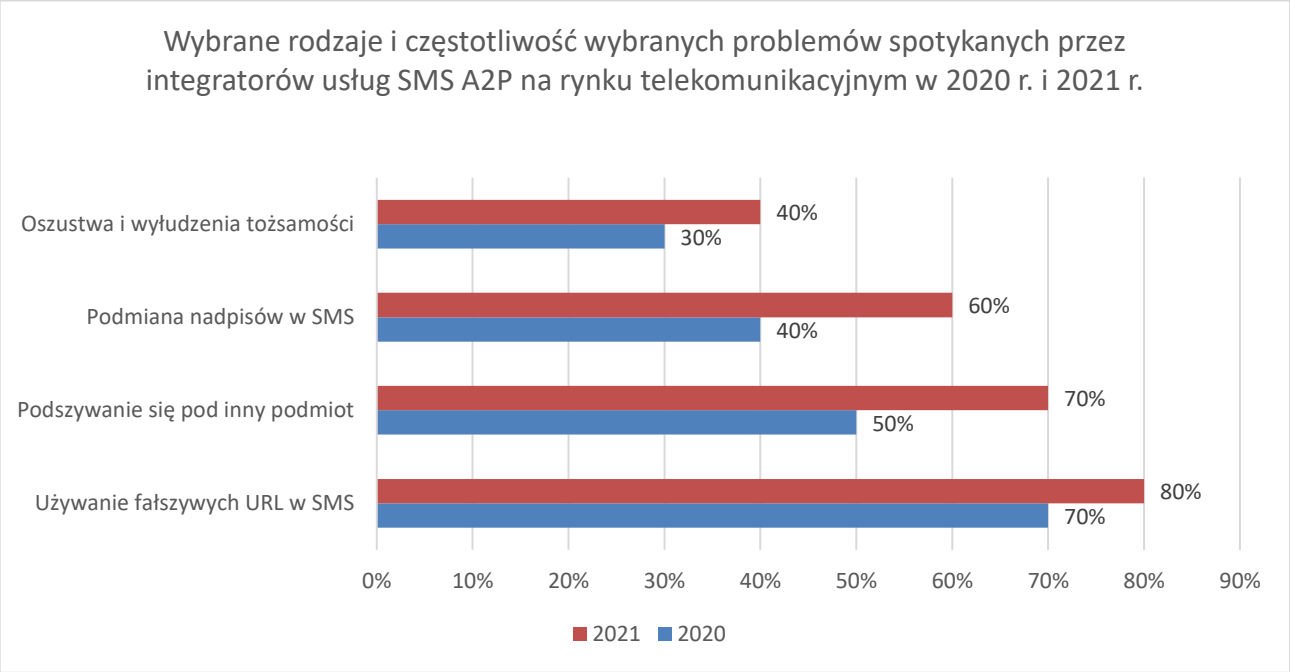
---

1 Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021 str. 81 https://cert.pl/uploads/docs/Raport_CP_2021.pdf.

2 https://cert.pl/posts/2022/04/smishing-pge/ ; https://cert.pl/posts/2022/04/flubot-smishing/

3 Pkt 8.3: *Cell service providers should provide a countering system for preventing smishing attacks.* ITU-T X.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks.

Integratorzy zwracają uwagę na szereg problemów, z jakimi muszą zmierzyć się w swojej działalności:



Procent oznacza procent integratorów usług SMS A2P, którzy spotkali się z danym problemem.

Źródło: Urząd Komunikacji Elektronicznej, *Rynek usług SMS A2P w Polsce,* Warszawa, styczeń 2022, str. 16[4].

Kolejnym zjawiskiem negatywnie wpływającym na dostępność usług oraz powodującym istotne szkody po stronie przedsiębiorców telekomunikacyjnych jest sztuczny ruch telekomunikacyjny. Propozycje uregulowania tego zjawiska są podnoszone od wielu lat[5].

Istotnym problemem są domeny internetowe, które mają na celu wprowadzenie w błąd użytkowników internetu i wyłudzenie ich danych i środków finansowych. Raport CERT Polska wskazał dla przykładu 5 podmiotów, pod które najczęściej przestępcy podszywali się w 2021 r. wraz z liczbą odnotowanych prób wejścia na taką stronę:

	Orlen	**PGNiG**	**Tesla**	**Lotos**	**KGHM**
Liczba domen ze stronami podszywającymi się pod dany podmiot wpisanymi na Listę ostrzeżeń	3 939	564	529	282	79
Liczba odnotowanych prób wejścia na strony podszywające się pod dany podmiot	269 397	26 469	25 673	23 302	19 999

Źródło: Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021 str. 75.

[4] https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/154/44/19/rynek_uslug_sms_a2p_w_polsce_2022_2.pdf

[5] Por. STANOWISKO Polskiej Izby Informatyki i Telekomunikacji (PIIT) w sprawie nadużyć telekomunikacyjnych https://www.piit.org.pl/__data/assets/pdf_file/0021/8553/Stanowisko_Naduzycia-PIIT-do-UKE_2018-03-19.pdf.

Dane te pokazują, jak często nieświadomi użytkownicy internetu są wprowadzani w błąd, myśląc, że np. wchodzą na stronę ich dostawcy energii.

Obecnie funkcjonuje *Porozumienie o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej*[6], które umożliwia w okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego prowadzenie przez NASK-PIB jawnej listy ostrzeżeń. Porozumienie to spełniło swoją rolę w okresie pandemii COVID-19, chroniąc użytkowników internetu przed utratą danych i środków finansowych. Zasadne jest umożliwienie, aby również poza okresami stanów nadzwyczajnych czy tymi związanymi z epidemią mogło obowiązywać podobne porozumienie.

W samym tylko okresie od stycznia 2022 r. do listopada 2022 r. CSIRT NASK zidentyfikował łącznie 38 999 domen, które mają na celu wprowadzenie w błąd użytkowników internetu i wyłudzenie ich danych i środków finansowych.

Rok	**Miesiąc**	**Liczba szkodliwych domen wpisanych na listę ostrzeżeń**[7]
2022	styczeń	4260
	luty	3163
	marzec	2335
	kwiecień	2093
	maj	3677
	czerwiec	3520
	lipiec	4395
	sierpień	4832
	wrzesień	4261
	październik	3886
	listopad	2577
	suma:	38 999

Źródło: Dane.gov.pl[8]

Na dzień 7 grudnia 2022 r. na liście ostrzeżeń było wpisanych ponad 81 000 domen.

W tej sytuacji konieczne jest wprowadzenie 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.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane ze zwalczaniem nadużyć telekomunikacyjnych.

Przedsiębiorcy telekomunikacyjnie będą obowiązani w szczególności do:

[6] https://www.uke.gov.pl/akt/uke-przystapil-do-porozumienia-chroniacego-abonentow,300.html.
[7] https://cert.pl/posts/2020/03/ostrzezenia_phishing/
[8] https://dane.gov.pl/pl/dataset/2740,lista-ostrzezen-cert-polska-przed-niebezpiecznymi/resource/43118/table

1) podejmowania proporcjonalnych środków organizacyjnych i technicznych mających na celu przeciwdziałać nadużyciom w komunikacji elektronicznej;

2) blokowania krótkich wiadomości tekstowych, które zawierają treści wyczerpujące znamiona smishingu zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK;

3) blokowania połączeń głosowych, które mają na celu podszywanie się pod inną osobę lub instytucję.

Ponadto projekt ustawy przyznaje przedsiębiorcom telekomunikacyjnym uprawnienie do samodzielnego blokowania:

1) krótkich wiadomości tekstowych, zawierających treści wyczerpujące znamiona smishingu, innych niż zawarte we wzorcu wiadomości, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich krótkich wiadomości tekstowych (SMS);
2) wiadomości multimedialnych MMS, w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania.

Blokowanie odbywa się za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich wiadomości.

Przedsiębiorcy telekomunikacyjni będą mogli przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej. Komunikat będzie mógł być przetwarzany jedynie w zakresie zwalczania i zapobiegania smishingu oraz złośliwych wiadomości multimedialnych MMS.

Prezes Urzędu Komunikacji Elektronicznej, dalej jako „Prezes UKE", będzie prowadził wykaz numerów służących wyłącznie do odbierania połączeń głosowych.

Zespół CSIRT NASK będzie monitorował występowanie smishingu i przekazywał przedsiębiorcom telekomunikacyjnym wzorce wiadomości wyczerpującej znamiona smishingu.

Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia SPF/DKIM/DMARC przy świadczeniu poczty elektronicznej.

Na poziomie ustawowym zostanie umocowana lista ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu[9]. Przedsiębiorcy telekomunikacyjni (strony porozumienia w sprawie funkcjonowania listy ostrzeżeń) będą mogli blokować dostęp do tych domen internetowych użytkownikom internetu.

Projekt ustawy penalizuje nadużycia w komunikacji elektronicznej – generowanie sztucznego ruchu, wysyłania smishingu lub dokonywania działań o charakterze CLI spoofingu w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osoby szkody.

Ustawa wprowadza administracyjne kary pieniężne, nakładane przez Prezesa UKE, za niewykonywanie obowiązków wynikających z projektowanych przepisów.

Oczekuje się, że skutkiem wejścia w życie przepisów ustawy będzie zmniejszenie liczby przypadków nadużyć w komunikacji elektronicznej oraz zwiększenie poczucia bezpieczeństwa osób korzystających z usług komunikacji elektronicznej.

Podkreślić należy, że nie ma innej możliwości rozwiązania problemu, jak tylko podjęcie działań na poziomie ustawowym. Co do zasady przedsiębiorcy telekomunikacyjni mają zapewnić ciągłość usług telekomunikacyjnych, które są podstawą współczesnego społeczeństwa informacyjnego. Blokowanie komunikatów elektronicznych powinno być uzasadnione szczególnymi okolicznościami. Takimi okolicznościami jest właśnie konieczność walki z nadużyciami w komunikacji elektronicznej.

[9] https://cert.pl/posts/2020/03/ostrzezenia_phishing/.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Wielka Brytania

Office of Communications (Ofcom) będący państwowym organem Wielkiej Brytanii kontrolującym i nadzorującym rynek mediów i telekomunikacji wraz z UK Finance utworzył w 2019 r. listę *Do Not Originate* (DNO). Oba te podmioty w celu utworzenia listy numerów, które nie są wykorzystywane do dzwonienia do konsumentów (są przeznaczone tylko do połączeń przychodzących), współpracowały m.in. z firmami telekomunikacyjnymi, agencjami rządowymi i innymi organami sektora publicznego. Lista DNO jest ponadto udostępniana dostawcom usług telekomunikacyjnych, dzięki czemu podmioty te mogą identyfikować oraz blokować połączenia z tych numerów, które znajdują się na liście. W celu zwalczania nadużyć w komunikacji elektronicznej dane, które zawiera lista DNO, wykorzystywane są również do blokowania i filtrowania niechcianych i uciążliwych połączeń w imieniu konsumenta. HMRC (HM Revenue & Customs – odpowiednik Urzędu Skarbowego w Polsce) odnotował znaczny spadek liczby fałszywych połączeń w wyniku dodania jego numerów do wykazu DNO, co wskazuje na skuteczność prowadzenia listy numerów przeznaczonych wyłącznie do połączeń przychodzących[10].

W Wielkiej Brytanii działa także National Cyber Security Centre (NCSC), które uruchomiło numer 7726. Jest to numer, pod który klienci sieci komórkowych w Wielkiej Brytanii mogą wysyłać SMS-y w celu zgłoszenia niechcianych wiadomości SMS lub połączeń telefonicznych. W przypadku podejrzenia oszustwa można dokonać zgłoszenia również do Action Fraud, które jest centrum zgłaszania oszustw i cyberprzestępczości w Anglii, Walii i Irlandii Północnej[11]. Zgodnie z danymi NCSC od lipca 2022 r. za pomocą numeru 7726[12] zostało usuniętych 14 tysięcy oszustw .

Irlandia

W Irlandii w celu zwalczania smishingu i spoofingu wprowadzono rejestr oszustów SMS-owych. *The SMS SenderID Protection Registry* ma na celu zmniejszenie wpływu fałszywych wiadomości SMS przy użyciu unikalnych identyfikatorów nadawcy dla zaufanych organizacji. Sprawdzając, czy użytkownik jest upoważniony do korzystania z określonego identyfikatora nadawcy, rejestr może odfiltrować oszustów od prawdziwych źródeł i zablokować nieuprawnionych użytkowników. Ma to na celu zapewnienie, że SMS pozostanie zaufanym i bezpiecznym kanałem, ponieważ wiele firm i organizacji rządowych nadal wykorzystuje to medium do komunikacji. W Irlandii rejestr wprowadzony przez Mobile Ecosystem Forum jest wspierany przez operatorów sieci komórkowych, agencje rządowe, banki i przedsiębiorstwa użyteczności publicznej[13].

Luksemburg

W Luksemburgu przyjęto ustawę z dnia 17 grudnia 2021 r., która transponuje do porządku krajowego dyrektywę Parlamentu Europejskiego i Rady z 11 grudnia 2018 r. nr 2018/1972 ustanawiającą Europejski kodeks łączności elektronicznej. Zgodnie z art. 109 ust. 2 tej ustawy Luksemburski Instytut Regulacji (*Institut Luxembourgeois de Régulation – ILR)* może wymagać od dostawców publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej zablokowania dostępu do numerów lub usług w poszczególnych przypadkach, gdy jest to uzasadnione ze względu na oszustwo lub niewłaściwe użycie, oraz może zażądać od dostawców usług łączności elektronicznej wstrzymania w takich przypadkach przychodów z połączeń wzajemnych lub innych usług[14].

---

[10] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-scam-calls-and-texts/do-not-originate.

[11] https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/7726-reporting-scam-texts-and-calls.

[12] https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-text-message.

[13] https://www.siliconrepublic.com/enterprise/smishing-spoofing-sms-scam-ireland-registry; https://mobileecosystemforum.com/2021/09/08/the-uks-mef-registry-launches-in-ireland-and-singapore-significantly-reducing-the-impact-of-smishing-spoofing-by-sms/.

[14] Art. 109 ust. 2, Loi du 17 décembre 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen, https://legilux.public.lu/eli/etat/leg/loi/2021/12/17/a927/jo#art_33.

Belgia

W Belgii przyjęto nową ustawę o telekomunikacji, która wprowadza możliwość zastosowania przez operatorów telekomunikacyjnych algorytmów do identyfikowania oraz blokowania podejrzanych wiadomości SMS[15].

Zgodnie z art. 51 § 5 Belgijski Instytut Usług Pocztowych i Telekomunikacji może żądać od operatorów sieci zablokowania dostępu do usług, gdy jest to uzasadnione z powodu oszustwa lub nadużycia, oraz nakazuje, aby w takich przypadkach operatorzy potrącali przychody z wzajemnych połączeń lub odpowiednich usług. Ponadto art. 121/8 § 1 stanowi, że bez względu na treść komunikatów operatorzy podejmują odpowiednie, proporcjonalne, zapobiegawcze środki z uwzględnieniem najnowszych możliwości technicznych w celu wykrycia oszustwa i złośliwego wykorzystania ich sieci i usług oraz w celu zapobieżenia wyrządzeniu szkody. Środki, które mają być podejmowane przez operatorów, mogą zostać określone przez Króla Belgii, przy czym Instytut jest uprawiony do wydawania wiążących instrukcji, w tym instrukcji dotyczących terminów, aby zagwarantować stosowanie tego przepisu. Przepis § 2 tego artykułu wprowadza przykładowe środki, jakimi mogą posługiwać się operatorzy usług sieciowych, aby zagwarantować wykrycie i zwalczanie oszustw. Są to m.in. środki na poziomie sieci, takie jak: blokowanie numerów, usług, adresów URL, nazw domen, adresów IP lub wszelkich innych identyfikatorów komunikacji elektronicznej, a na poziomie użytkownika końcowego środki takie jak całkowita lub częściowa dezaktywacja niektórych usług lub sprzętu[16].

Zapewnia się poszanowanie prawa do prywatności i tajemnicy komunikowania się, natomiast na zasadzie odstępstwa, aby zapewnić skuteczność art. 121/8 w celu stwierdzenia oszustwa lub złośliwego wykorzystania sieci lub usługi, lub zidentyfikowania ich autora i pochodzenia, oraz w zakresie, w jakim przetwarza je lub generuje w ramach świadczenia tej sieci lub usługi, operator może przechowywać przez 4 miesiące od daty komunikacji dane o ruchu niezbędne do powyższych celów. Takie dane mogą obejmować m.in.: identyfikator pochodzenia komunikatu, identyfikator miejsca przeznaczenia komunikacji, dokładne daty i godziny rozpoczęcia i zakończenia połączenia oraz miejsce położenia urządzeń stron biorących udział w połączeniu na początku oraz na końcu połączenia. Operator może także przez 12 miesięcy od daty połączenia, w celu zidentyfikowania inicjatora połączenia, przechowywać dane o ruchu dotyczące połączeń przychodzących w kontekście świadczenia usług komunikacji elektronicznej. Okres 4 i 12 miesięcy jest terminem instrukcyjnym, ponieważ operator może przechowywać te dane dłużej, jeżeli jest to niezbędne[17].

Z odpowiedzialności karnej dotyczącej naruszenia prawa do prywatności wyłączeni są na podstawie ustawy operatorzy, którzy podejmują działania mające na celu zwalczanie oszustw popełnianych za pomocą wiadomości wykorzystujących numery telefonów, takich jak wiadomości SMS lub MMS, przy zachowaniu następujących warunków:

a) działania pozostają ograniczone do mechanicznego badania wiadomości w celu stwierdzenia oszustwa – interwencja człowieka jest dozwolona wyłącznie w celu weryfikacji prawidłowego funkcjonowania algorytmów komputerowych,

b) działania operatorów są jasne dla użytkowników końcowych, którzy są świadomi tego, że wiadomości mogą być sprawdzane mechanicznie w kontekście zwalczania nadużyć finansowych,

c) dane te mogą być przetwarzane wyłącznie przez osoby, którym operator powierzył zadanie zwalczania nadużyć finansowych,

d) przetwarzanie danych jest ograniczone do czynności i czasu niezbędnego do zwalczania nadużyć finansowych lub do końca okresu, w którym możliwe jest wszczęcie postępowania sądowego[18].

---

[15] https://desutter.belgium.be/nl/de-nieuwe-telecomwet-van-de-sutter-staat-aan-zijde-van-klant%E2%80%AF https://commsrisk.com/belgium-to-introduce-automated-blocking-of-sms-messages/.

[16] Art. 121/8, Loi du 13 juin 2005 relative aux communications electroniques (z późn. zm), https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi.

[17] Art. 122 par. 4, Loi du 13 juin 2005 relative aux communications electroniques (z późn. zm), https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi .

[18] Art. 125 par. 1 ust. 7, Loi du 13 juin 2005 relative aux communications electroniques (z późn. zm), https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi .

Jeżeli oszustwo zostanie ujawnione, operatorzy podejmują konkretne działania w celu zwalczania oszustwa, takie jak blokowanie wiadomości lub zastępowanie w wiadomościach adresu URL odsyłającego do oszukańczej strony internetowej komunikatem ostrzegawczym lub adresem URL z ostrzeżeniem. Przed dniem 1 lutego operatorzy przekazują Instytutowi roczne sprawozdanie zawierające co najmniej środki podjęte przez nich w ciągu ostatniego roku w celu zwalczania nadużyć finansowych w komunikacji elektronicznej, ich skuteczności oraz tendencje w zakresie nadużyć finansowych[19].

Malta

Zgodnie z ustawą Maltański Urząd Komunikacji może wymagać od przedsiębiorców udostępniających publiczne sieci łączności lub świadczących usługi łączności elektronicznej, aby blokowali w poszczególnych przypadkach dostęp do numerów lub usług, jeżeli jest to uzasadnione ze względu na (potencjalne) oszustwo lub nadużycia. Ma prawo wymagać, aby w takich przypadkach dostawcy usług łączności elektronicznej potrącali przychody z tytułu połączeń wzajemnych[20].

Francja

We Francji działa numer 33700, który jest używany do walki ze spamem SMS bądź głosowym. Każdy, kto jest ofiarą oszustwa dokonanego za pomocą SMS bądź połączenia głosowego, może zgłosić ten fakt pod numer 33700[21].

Funkcjonuje także lista *Bloctel* zawierająca listę numerów konsumentów, którzy nie chcą otrzymywać telefonów handlowych od firm, z którymi nie są związani umową (SPAM).

Stany Zjednoczone Ameryki

W Stanach Zjednoczonych przedsiębiorcy zostali zobowiązani na podstawie Telephone Robocall Abuse Criminal Enforcement and Deterrence Act oraz decyzji Federal Communication Commision do stosowania rozwiązania STIR/SHAKEN, które umożliwia uwierzytelnienie informacji adresowej połączenia[22].

Zgodnie z ustawą „Truth in Caller ID Act" przepisy zabraniają komukolwiek przekazywania wprowadzających w błąd lub niedokładnych informacji o identyfikatorze dzwoniącego z zamiarem oszukania czy spowodowania szkody. Każdy, kto dopuszcza się spoofingu, może zostać ukarany karą w wysokości do 10 000 dolarów[23].

Niektóre przedsiębiorstwa telekomunikacyjne domyślnie blokują połączenia automatyczne w oparciu o analizy. Federalna Komisja Łączności (*Federal Communications Commission*) zachęca dostawców usług komunikacji, którzy blokują połączenia, aby umożliwili dzwoniącemu, którego numer jest zablokowany, skontaktowanie się z dostawcą w celu wyjaśnienia, czy numer ten powinien być blokowany czy powinien zostać usunięty z listy numerów zablokowanych[24].

Departament Bezpieczeństwa Narodowego USA nakazał także agencjom federalnym stosowanie mechanizmu uwierzytelniania poczty elektronicznej DMARC[25].

Kanada

Kanadyjska Komisja ds. Telewizji i Telekomunikacji zobowiązała dostawców usług telekomunikacyjnych do wprowadzenia nowej technologii, która ma na celu rozwiązanie problemu fałszowania identyfikatora dzwoniącego (spoofing).

---

19 Tamże.

20 Art. 45 ust. 2, Subsidiary Legislation 399.28 12th July 2011 Electronic Communications Networks and Services (General) Regulations (z późn. zm.).

21 https://www.33700.fr/identifier-et-signaler-un-spam-sms/.
https://www.33700.fr/identifier-et-signaler-un-spam-vocal/.

22 https://www.fcc.gov/document/mandating-stirshaken-combat-spoofed-robocalls-0.

23 https://www.fcc.gov/spoofing.

24 Tamże.

25 https://www.cisa.gov/sites/default/files/bod-18-01.pdf.

Technologia, która ma być wykorzystywana, to STIR/SHAKEN. Umożliwi ona operatorom weryfikację informacji o identyfikatorze rozmówcy w przypadku połączeń głosowych opartych na IP i poinformuje adresata, do którego skierowane jest połączenie, czy można zaufać tożsamości rozmówcy.

Prowadzone są także prace nad programem śledzenia, który pozwoliłby określić, skąd podchodzi uciążliwe połączenie.

Regulator wymaga od operatorów telekomunikacyjnych również wdrożenia uniwersalnego oprogramowania blokującego połączenia pochodzące z tak zwanych „nieprawidłowych numerów" (00-000-0000 lub 111-111-1111 lub te, które przekraczają 15 cyfr)[26].

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
CSIRT NASK	1	Informacja ogólnodostępna	Zespół CSIRT NASK będzie monitorował nadużycia w komunikacji elektronicznej oraz uruchomi system teleinformatyczny przekazujący wzorce wiadomości wyczerpujących znamiona smishingu. Ponadto będzie odpowiedzialny za prowadzenie listy ostrzeżeń.
Banki	542[27]	Dane UKNF[28]	Banki będą uprawnione do złożenia wniosku o wpis numeru przez nie wykorzystywanego do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Dostawcy poczty elektronicznej	brak danych[29]		Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej SPF, DKIM lub DMARC. Będą obowiązani zapewnić możliwość stosowania metod uwierzytelniania wieloskładnikowego w ramach poczty elektronicznej dla podmiotu publicznego.
Firmy inwestycyjne	66	Dane ESMA[30]	Firmy inwestycyjne będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Fundusze inwestycyjne	706	Dane UKNF[31]	Fundusze inwestycyjne będą uprawnione do złożenia wniosku o wpis swojego numeru do

[26] https://www.canada.ca/en/radio-television-telecommunications/news/2021/11/canadians-to-benefit-from-new-caller-id-technology-to-combat-spoofed-calls.html; https://www.theglobeandmail.com/business/article-crtc-calls-on-telecoms-to-adopt-new-tool-to-tackle-phone-scams/.

[27] 30 banków komercyjnych, 1 bank państwowy, 511 banków spółdzielczych.

[28] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku, str. 24; https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf - dalej zwane „Sprawozdanie KNF 2021".

[29] Na podstawie danych badania Mediapanel można założyć, że jest co najmniej 6 „platform mailowych", z usług których korzysta co najmniej 500 000 Polaków. Źródło: https://www.wirtualnemedia.pl/artykul/mail-serwisy-najlepsze-poczta-gmail. Brak danych dot. liczby dostawców poczty elektronicznej dla podmiotów publicznych.

[30] https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_upreg#.

[31] Sprawozdanie KNF 2021 str. 25.

			wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Instytucje płatnicza	40	Dane UKNF[32]	Instytucje płatnicze będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Integratorzy usług SMS A2P	co najmniej 13	Dane UKE[33]	Niektórzy z integratorów są przedsiębiorcami telekomunikacyjnymi – będą więc obowiązani blokować krótkie wiadomości tekstowe (SMS) zgodnie ze wzorcem wiadomości wyczerpującej znamiona smishingu.
Jednostki sektora finansów publicznych			Jednostki sektora finansów publicznych będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych. Podmioty publiczne w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa będą obowiązane do korzystania z poczty elektronicznej wykorzystującej mechanizmy uwierzytelniania SPF, DKIM oraz DMARC.
Kasa Krajowa SKOK	1	Informacja ogólnodostępna	Kasa Krajowa SKOK będzie uprawniona do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Komendant Centralnego Biura Zwalczania Cyberprzestępczości	1	Informacja ogólnodostępna	Obowiązek podłączenia się do systemu teleinformatycznego przekazującego wzorce wiadomości wyczerpujących znamiona smishingu.
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Minister właściwy do spraw informatyzacji będzie obowiązany zamieścić w Biuletynie Informacji Publicznej informację o uruchomieniu przez CSIRT NASK systemu teleinformatycznego przekazującego wzorce wiadomości wyczerpujących znamiona smishingu.
Oddziały instytucji kredytowej	36	Dane UKNF[34]	Oddziały instytucji kredytowych będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Prezes Urzędu Komunikacji Elektronicznej	1	Informacja ogólnodostępna	Obowiązek podłączenia się do systemu teleinformatycznego przekazującego wzorce wiadomości wyczerpujących znamiona smishingu. Prezes UKE otrzyma również kompetencję do rozpatrywania sprzeciwu:

[32] Sprawozdanie KNF 2021 str. 24.
[33] Urząd Komunikacji Elektronicznej, Rynek usług SMS A2P w Polsce, Warszawa, styczeń 2022, str. 5.
[34] Sprawozdanie KNF 2021, str. 26.

			– wobec zablokowania krótkiej wiadomości tekstowej (SMS), – wpisania domeny internetowej na listę ostrzeżeń. Prezes UKE będzie również nakładał administracyjne kary pieniężne na przedsiębiorców telekomunikacyjnych za niestosowanie się do przepisów ustawy. Uzyska możliwość zawarcia z operatorami telekomunikacyjnymi porozumienia określającego środki organizacyjne i techniczne stosowane przy przeciwdziałaniu CLI spoofing.
Przedsiębiorcy telekomunikacyjni	3881	Rejestr przedsiębiorców telekomunikacyjnych[35]	Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane ze zwalczaniem nadużyć w komunikacji elektronicznej.
Prokuratura	Prokuratura Krajowa: 1 prokuratury regionalne: 11 prokuratury okręgowe: 46 prokuratury rejonowe: 358	Mały rocznik statystyczny Polski 2022, str. 81[36]	Prowadzenie postępowań karnych w sprawach nadużyć w komunikacji elektronicznej.
Sądy powszechne	Sąd Najwyższy: 1 sądy apelacyjne: 11 sądy okręgowe: 46 sądy rejonowe: 318	Mały rocznik statystyczny Polski 2022, str. 83	Prowadzenie postępowań karnych w sprawach nadużyć w komunikacji elektronicznej. Sąd Ochrony Konkurencji i Konsumentów będzie rozpatrywał sprawy ze skarg na decyzje administracyjne Prezesa UKE o nałożeniu kary pieniężnej za niewykonanie przez przedsiębiorcę telekomunikacyjnego obowiązków w zakresie zwalczania i zapobiegania nadużyciom w komunikacji elektronicznej.
Wojewódzki Sąd Administracyjny w Warszawie Naczelny Sąd Administracyjny	2		WSA w Warszawie będzie rozpatrywał skargi na decyzje administracyjne o nałożeniu kary na dostawcę poczty elektronicznej oraz na kierownika podmiotu publicznego za niewykonanie obowiązków wynikających z ustawy.

[35] Stan na dzień 31.01.2023 r.

[36] https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/maly-rocznik-statystyczny-polski-2022,1,24.html.

			NSA będzie rozpatrywał ewentualne skargi kasacyjne.
Spółdzielcze kasy oszczędnościowo--kredytowe	23	Dane UKNF[37]	SKOK będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Towarzystwa funduszy inwestycyjnych	57	Dane UKNF[38]	Towarzystwa funduszy inwestycyjnych będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Użytkownicy internetu w Polsce	29,7 mln	Badania Mediapanel za październik 2022[39]	Użytkownicy internetu w Polsce zostaną zabezpieczeni przed domenami internetowymi, które służą do wyłudzeń danych i środków finansowych.
Użytkownicy poczty elektronicznej w Polsce	68,3% ogółu osób w wieku 16–74 lata	Mały rocznik statystyczny Polski 2022, str. 259[40]	Zmniejszenie ryzyka zetknięcia się z wiadomościami poczty elektronicznej pochodzącymi od oszustów.
Użytkownicy telefonii	2,7 mln abonentów telefonii stacjonarnej; 2,6 mln użytkowników telefonii VoIP; 56,6 mln użytkowników rynku telefonii ruchomej w Polsce	Dane UKE[41]	Zmniejszenie ryzyka zetknięcia się z CLI spoofing oraz smishingiem.
Zakład reasekuracji	1	Dane UKNF[42]	Zakłady reasekuracji będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Zakłady ubezpieczeń	55	Dane UKNF[43]	Zakłady ubezpieczeń będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.

[37] Informacja o sytuacji spółdzielczych kas oszczędnościowo-kredytowych w I kwartale 2022 r. str. 3 https://www.knf.gov.pl/knf/pl/komponenty/img/Informacja_o_sytuacji_spoldzielczych_kas_oszczednosciowo_kredytowych_w_I_kw_2022_78633.pdf.

[38] Raport dotyczący sytuacji finansowej towarzystw funduszy inwestycyjnych w 2021 r., str. 5, https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_o_sytuacji_finansowej_TFI_w_2021_roku_78397.pdf.

[39] https://www.gemius.pl/reklamodawcy-aktualnosci/wyniki-badania-mediapanel-za-pazdziernik-2022.html.

[40] https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/maly-rocznik-statystyczny-polski-2022,1,24.html.

[41] Raport o stanie rynku telekomunikacyjnego w 2021 r. str. 35, 47, 57; https://www.uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2021-r-,431.html.

[42] Sprawozdanie KNF 2021, str. 122.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach 14-dniowych konsultacji i opiniowania projekt został skierowany do zaopiniowania przez następujące podmioty:

1) American Chamber of Commerce in Poland;
2) Busines Centre Club;
3) Federacja Konsumentów;
4) Fundacja Bezpieczna Przestrzeń;
5) Fundacja im. Kazimierza Pułaskiego;
6) Fundacja im. Stefana Batorego;
7) Fundacja Instytut Mikromakro;
8) Fundacja Moje Państwo;
9) Fundacja MY Pacjenci;
10) Fundacja Nowoczesna Polska;
11) Fundacja Panoptykon;
12) Fundacja Projekt: Polska;
13) Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego UW;
14) Izba Gospodarki Elektronicznej;
15) Klaster #CyberMadeInPoland;
16) Konfederacja Lewiatan;
17) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
18) Krajowa Izba Gospodarcza;
19) Krajowa Izba Gospodarki Cyfrowej;
20) Krajowa Izba Gospodarki Morskiej;
21) Krajowa Izba Komunikacji Ethernetowej;
22) Krajowa Izba Rozliczeniowa S.A.;
23) Krajowe Stowarzyszenie Ochrony Informacji Niejawnych;
24) Naczelna Organizacja Techniczna;
25) Naczelna Rada Zrzeszeń Handlu i Usług;
26) Ogólnopolskie Porozumienie Organizacji Radioamatorskich;
27) PKP TELKOL sp. z o.o.;
28) Polska Federacja Szpitali;
29) Polska Izba Handlu;
30) Polska Izba Informatyki i Telekomunikacji;
31) Polska Izba Komunikacji Elektronicznej;
32) Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei;
33) Polska Izba Radiodyfuzji Cyfrowej;
34) Polska Organizacja Handlu i Dystrybucji;
35) Polska Organizacja Niebankowych Instytucji Płatności;
36) Polska Rada Biznesu;
37) Polska Wytwórnia Papierów Wartościowych;
38) Polski Związek Krótkofalowców;
39) Polski Związek Pracodawców Przemysłu Farmaceutycznego;
40) Polskie Centrum Badań i Certyfikacji S.A.;
41) Polskie Górnictwo Naftowe i Gazownictwo;
42) Polskie Koleje Państwowe S.A.;
43) Polskie Stowarzyszenie Marketingu SMB;
44) Polskie Towarzystwo Informatyczne;
45) Polskie Związek Przemysłu Motoryzacyjnego;
46) SABI – stowarzyszenie inspektorów ochrony danych;
47) Sieć Obywatelska Watchdog Polska;
48) Stowarzyszenie „Archiwizjoner”;
49) Stowarzyszenie Inżynierów Telekomunikacji;
50) Stowarzyszenie ISACA;
51) Towarzystwo Gospodarcze Polskie Elektrownie;
52) Związek Banków Polskich;
53) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska;
54) Związek Pracodawców Branży Internetowej IAB Polska;
55) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM;
56) Związek Pracodawców Mediów Publicznych;
57) Związek Przedsiębiorców i Pracodawców;
58) Związek Telewizji Kablowych w Polsce – Izba Gospodarcza;
59) Prezes Urzędu Komunikacji Elektronicznej;
60) Prezes Urzędu Ochrony Danych Osobowych;
61) Prezes Urzędu Ochrony Konkurencji i Konsumentów.

Z uwagi na pilną konieczność podjęcia prac legislacyjnych mających na celu wprowadzenie ram prawnych dla zwalczania nadużyć w komunikacji elektronicznej termin konsultacji publicznych został skrócony do 14 dni. Podsumowanie uwag zgłoszonych w ramach konsultacji publicznych znajduje się w raporcie z konsultacji publicznych.

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz art. 52 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Otrzymano jedno zgłoszenie lobbingowe do projektu ustawy, które zostało opublikowane w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0–10)*
Dochody ogółem	0	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,15
budżet państwa	0	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,15
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	0	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,15
budżet państwa	0	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,015	0,15
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego. Należy podkreślić, że obowiązki związane z konfiguracją poczty elektronicznej nie będą wymagały zatrudnienia nowych pracowników. Tego typu zmiana wymaga maksymalnie kilku dni roboczych osób zajmujących się administrowaniem pocztą elektroniczną.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Dochody do budżetu państwa z wpływów z administracyjnych kar pieniężnych nakładanych na podstawie niniejszej ustawy oszacowano w wysokości 15 tys. zł rocznie.

<table>
<tr><td colspan="9">7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe</td></tr>
<tr><td colspan="9">Skutki</td></tr>
<tr><td colspan="2">Czas w latach od wejścia w życie zmian</td><td>0</td><td>1</td><td>2</td><td>3</td><td>5</td><td>10</td><td>Łącznie (0–10)</td></tr>
<tr><td rowspan="3">W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)</td><td>duże przedsiębiorstwa</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>sektor mikro-, małych i średnich przedsiębiorstw</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>rodzina, obywatele oraz gospodarstwa domowe</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>W ujęciu niepieniężnym</td><td>duże przedsiębiorstwa</td><td colspan="7">Przedsiębiorcy telekomunikacyjni

Przedsiębiorcy telekomunikacyjni będą obowiązani do podejmowania proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczaniu.

Celem dostosowania do projektu ustawy przedsiębiorcy będą musieli:

– wypracować wewnętrzne procedury zapobiegania i zwalczania nadużyć w komunikacji elektronicznej,

– podłączyć się do systemu teleinformatycznego CSIRT NASK, przekazującego wzorce wiadomości wyczerpujących znamiona smishingu,

– monitorować wykaz numerów służących wyłącznie do odbierania połączeń głosowych i blokować połączenia inicjowane z tych numerów,

– blokować połączenia głosowe mające charakter CLI spoofing,

– automatycznie blokować krótkie wiadomości tekstowe zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK,

– wdrożyć środki organizacyjne i techniczne przeciwdziałające sztucznemu ruchowi, a także nieuprawnionej zmianie informacji adresowej[44].

Konsekwencją dostosowania się do obowiązków wynikających z projektu ustawy może być konieczność zmiany regulaminów świadczenia usług telekomunikacyjnych. Może zaistnieć także potrzeba dostosowania umów międzyoperatorskich – umowy te zawierają postanowienia np. dot. sztucznego ruchu czy innych nadużyć.

Wykonywanie obowiązków wynikających z niniejszego projektu ustawy przez przedsiębiorców telekomunikacyjnych zwiększy bezpieczeństwo usług komunikacji elektronicznej. Przełoży się to na zwiększenie zaufania</td></tr>
</table>

[44] W przypadku nieuprawnionej zmiany informacji adresowej będą to środki mające na celu wykonywanie obowiązków określonych w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 12 grudnia 2014 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania połączeń dla właściwego kierowania połączeń (Dz. U. z 2015 r. poz. 12), lub w rozporządzeniu, które w przyszłości zastąpi to rozporządzenie w związku z projektowanym Prawem komunikacji elektronicznej.

		użytkowników usług komunikacji elektronicznej do tych usług i szerzej do przedsiębiorców telekomunikacyjnych. Oszacowanie kosztów dostosowania się przedsiębiorców telekomunikacyjnych do nowych przepisów nie jest możliwe ze względu na to, że nie są znane rozwiązania techniczne, które już obecnie są przez nich wykorzystywane. **Dostawcy poczty elektronicznej** Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej. Wdrożenie mechanizmów SPF, DKIM oraz DMARC polega na wprowadzeniu odpowiednich rekordów DNS. Dokumentacja dot. tych mechanizmów jest dostępna bezpłatnie[45]; ponadto istnieje wiele poradników, jak poprawnie skonfigurować te mechanizmy[46]. Szacuje się, że wdrożenie tych mechanizmów zajmie kilka dni pracy administratora systemów poczty elektronicznej. **Podmioty uprawnione do złożenia wniosku o wpis numeru przez nie wykorzystywanego do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.** Wpisanie numeru podmiotu do wykazu numerów służących wyłącznie do odbierania połączeń głosowych obniży ryzyko podszywania się przez oszustów pod te podmioty. Przełoży się to na zwiększenie zaufania klientów do tych podmiotów. **Podmiot dysponujący tytułem do domeny internetowej** Domeny internetowe, których podstawowym celem działania jest wprowadzanie użytkowników internetu w błąd, będą mogły być wpisane na listę ostrzeżeń. Podmiot dysponujący tytułem do domeny będzie mógł złożyć sprzeciw do Prezesa UKE na wpisanie tej domeny na listę ostrzeżeń. Zapewniona będzie więc ścieżka odwoławcza.
	sektor mikro-, małych i średnich przedsiębiorstw	Co do zasady proponowane regulacje będą oddziaływać na wszystkich przedsiębiorców telekomunikacyjnych, bez względu na wielkość. Dotyczy to w szczególności blokowania CLI spoofing czy wiadomości o charakterze smishingu. Przemawia za tym konieczność zapewnienia jednolitych działań mających na celu zwalczanie nadużyć w komunikacji elektronicznej. Jednakże warto podkreślić, że przedsiębiorcy telekomunikacyjni będą stosowali proporcjonalne środki organizacyjne i techniczne mające na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Wybór konkretnych środków będzie więc zależny od wielkości podmiotu, posiadanej infrastruktury czy charakteru świadczonych usług. Podkreślić należy, że za naruszenie art. 3 ust. 2 (który zawiera ww. obowiązek) nie jest przewidziana sankcja w postaci administracyjnej kary pieniężnej. Prezes

[45] https://datatracker.ietf.org/doc/html/rfc7489; https://datatracker.ietf.org/doc/html/rfc6376; https://datatracker.ietf.org/doc/html/rfc7208.

[46] https://dmarc.org/resources/articles-tutorials-and-videos/; https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/configure-anti-spoofing-controls-.

		UKE będzie mógł jednak dokonać kontroli u przedsiębiorcy i w razie potrzeby wydać zalecenia pokontrolne. Warto dodać, że w przepisach o administracyjnych karach pieniężnych przewidziano fakultatywną odpowiedzialność przedsiębiorcy telekomunikacyjnego np. za niewykonywanie obowiązków związanych ze zwalczaniem smishingu i CLI spoofing, jeżeli przemawia za tym zakres lub charakter naruszenia. Takie sformułowanie pozwoli Prezesowi UKE, przed nałożeniem administracyjnej kary pieniężnej, zbadać sytuację przedsiębiorcy i przed nałożeniem kary wziąć pod uwagę także okoliczności towarzyszące naruszeniu. Do postępowania w sprawie nałożenia kar pieniężnych, o których mowa w art. 20 niniejszego projektu ustawy, będą stosowane przepisy działu IVA Administracyjne kary pieniężne Kodeksu postępowania administracyjnego[47]. Przepisy działu IVA Kodeksu postępowania administracyjnego regulują między innymi przesłanki nakładania administracyjnej kary pieniężnej, przesłanki odstąpienia od kary i skutki naruszenia prawa wywołanego działaniem siły wyższej. Z tych powodów należy uznać, że projekt ustawy uwzględnia sytuację sektora MŚP. Odnosząc się do obowiązków dostawców poczty elektronicznej, to tak, jak wyżej wspomniano, obowiązki te nie są trudne do spełnienia, dlatego nie jest to zbytnie obciążenie dla sektora MŚP.
	rodzina, obywatele oraz gospodarstwa domowe	Projekt ustawy przełoży się na zwiększenie bezpieczeństwa usług komunikacji elektronicznej świadczonych dla obywateli. Utrudni przestępcom podszywanie się pod inne osoby i oszukiwanie obywateli. Przełoży się to na zwiększenie zaufania obywateli do usług komunikacji elektronicznej. W przypadku gdy przedsiębiorca telekomunikacyjny będzie blokował SMS zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości przekazanym przez CSIRT NASK, użytkownik końcowy będzie mógł dochodzić swoich praw przez postępowanie reklamacyjne. Nadawca krótkiej wiadomości tekstowej (SMS) będzie mógł zgłosić sprzeciw wobec zablokowania tej wiadomości do Prezesa UKE. Osoba dysponująca tytułem do domeny internetowej będzie mogła złożyć sprzeciw do Prezesa UKE na wpisanie tej domeny na listę ostrzeżeń. Osoby fizyczne dokonujące, w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody, sztucznego ruchu, smishingu, CLI spoofingu oraz nieuprawnionej zmiany informacji adresowej będą podlegały odpowiedzialności karnej. Na kierującego przedsiębiorstwem telekomunikacyjnym Prezes UKE będzie mógł nałożyć administracyjną karę pieniężną, jeżeli nie zostaną wykonane obowiązki z zakresu zwalczania smishingu oraz CLI spoofing. Kierownik podmiotu publicznego będzie mógł podlegać administracyjnej karze pieniężnej, jeżeli nie zostały wdrożone mechanizmy uwierzytelniania poczty elektronicznej SPF/DKIM/DMARC.
Niemierzalne		

[47] Ustawa z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego.

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	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 popularny i obecnie jego ofiarami stają się tysiące ludzi. Jak zostało wskazane w raporcie CSIRT NASK za 2021 r. cały czas rośnie liczba tego typu ataków[48]. Sam raport opisuje również całą serię różnego rodzaju ataków z wykorzystaniem SMS-ów. 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 przyczynić się do rozwiązania bardzo poważnego problemu społecznego i ochronić kluczowe interesy obywateli. Ograniczenie rozmiarów tego zjawiska jest niemożliwe bez przetwarzania komunikatów wysyłanych przez użytkowników końcowych. 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. Projekt nakłada jedynie konieczne i niezbędne obowiązki, aby osiągnąć cele ustawy, czyli zmniejszenie liczby przypadków nadużyć w komunikacji elektronicznej oraz zwiększenie poczucia bezpieczeństwa osób korzystających z usług komunikacji elektronicznej. Projekt nie wprowadza regulacji dot. zakazu wykonywania określonej działalności gospodarczej. Z tych powodów uznaje się, że projekt jest zgodny z ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2023 r. poz. 221).

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu	
☐ nie dotyczy	
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☒ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: …	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: …
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

Ustawa nakłada na przedsiębiorców telekomunikacyjnych następujące obowiązki:

1) podejmowanie proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie;
2) podłączenie się do systemu teleinformatycznego przekazującego wzorce wiadomości wyczerpującej znamiona smishingu;
3) niezwłoczne blokowanie krótkich wiadomości tekstowych zawierających treści zawarte we wzorcu wiadomości wyczerpującej znamiona smishingu;

[48] Raport Roczny z działalności CERT Polska, str. 55-65.

4) blokowanie lub ukrycie identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia CLI spoofingu;

5) rejestracja danych o usługach telekomunikacyjnych, które nie zostały wykonane z uwagi na blokowanie krótkich wiadomości tekstowych, a także blokowanie CLI spoofing.

Prezes Urzędu Komunikacji Elektronicznej będzie:

- prowadził w BIP jawny wykaz numerów służących wyłącznie do odbierania połączeń głosowych,
- zawierał porozumienia określające środki organizacyjne i techniczne, które operatorzy świadczący usługi telekomunikacyjne dla co najmniej 50 000 abonentów będą stosowali przy realizacji obowiązków dot. zwalczania CLI spoofing,
- rozpatrywał sprzeciw:
  - wobec zablokowania krótkiej wiadomości tekstowej (SMS),
  - wpisania domeny internetowej na listę ostrzeżeń,
- wydawał decyzję nakazującą przedsiębiorcy telekomunikacyjnemu zablokowanie dostępu do numeru lub usługi w terminie 6 godzin od ogłoszenia oraz nakładającą obowiązek wstrzymania pobierania opłat za połączenia lub usługi zrealizowane po upływie tego terminu,
- obowiązany przedstawić roczne sprawozdanie z wykonania ustawy ministrowi właściwemu do spraw informatyzacji oraz sejmowej komisji właściwej w sprawach telekomunikacji,
- kontrolował przedsiębiorców telekomunikacyjnych, dostawców poczty elektronicznej, podmioty publiczne w zakresie wykonywania obowiązków wynikających z ustawy,
- nakładał administracyjne kary pieniężne za niewykonywanie obowiązków wynikających z ustawy.

Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników lub podmiotów publicznych będą obowiązani stosować mechanizmy uwierzytelnienia poczty elektronicznej.

Podmioty publiczne będą obowiązane korzystać z poczty elektronicznej wykorzystującej mechanizmy uwierzytelniania SPF, DKIM oraz DMARC.

9. Wpływ na rynek pracy

Projekt może wygenerować potrzebę zatrudnienia przez niektórych przedsiębiorców telekomunikacyjnych specjalistów do obsługi systemów wykrywania i zwalczania nadużyć w komunikacji elektronicznej.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☒ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Projekt spowoduje powstanie: – nowego systemu teleinformatycznego służącego do wymiany informacji o wzorcach wiadomości wyczerpującej znamiona smishingu, – wykazu numerów służących wyłącznie do odbierania połączeń głosowych. Ustawa wprowadza administracyjne kary za niedostosowanie się do obowiązków wynikających z jej przepisów. Skargi na decyzje administracyjne o nałożeniu kary na przedsiębiorców telekomunikacyjnych będą rozpatrywane przez Sąd Ochrony Konkurencji i Konsumentów. Trudno

	jest oszacować, ile może być nałożonych kar, a co za tym idzie, nie jest możliwe oszacowanie liczby postępowań sądowych wszczętych na podstawie skarg na te decyzje. Ustawa wprowadza nowe przepisy karne. Może to spowodować wzrost liczby postępowań karnych prowadzonych przed sądami powszechnymi.

11. Planowane wykonanie przepisów aktu prawnego

Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia. W terminie 3 miesięcy od dnia wejścia w życie ustawy zespół CSIRT NASK uruchomi system teleinformatyczny służący do przekazywania wzorców wiadomości wyczerpującej znamiona smishingu i poinformuje o tym ministra właściwego do spraw informatyzacji. Minister z kolei niezwłocznie po otrzymaniu informacji z CSIRT NASK zamieści informację o uruchomieniu tego systemu w Biuletynie Informacji Publicznej. Po opublikowaniu tej informacji Komendant Centralnego Biura Zwalczania Cyberprzestępczości, Prezes Urzędu Komunikacji Elektronicznej oraz przedsiębiorcy telekomunikacyjni będą obowiązani podłączyć się do tego systemu w terminie 3 miesięcy.

Przedsiębiorcy telekomunikacyjni będą obowiązani podjąć proporcjonalne środki organizacyjne i techniczne mające na celu zapobieganie i zwalczanie: smishingu – w terminie 6 miesięcy od dnia wejścia w życie ustawy oraz CLI spoofingu – w terminie 12 miesięcy od dnia wejścia w życie ustawy.

Prezes UKE podejmie konsultacje z przedsiębiorcami telekomunikacyjnymi w celu ustalenia konieczności zawarcia porozumienia określającego szczegółowe środki organizacyjne i techniczne służące zwalczaniu CLI spoofingu.

Podsumowując – pierwszy rok funkcjonowania przepisów ustawy będzie czasem wdrożenia przepisów, w tym wdrożenia środków organizacyjnych i technicznych przeciwdziałających nadużyciom w komunikacji elektronicznej. Pełnych efektów wdrożenia przepisów można oczekiwać w kolejnym roku funkcjonowania przepisów.

Zależnie od potrzeb rynku komunikacji elektronicznej:

- Prezes UKE będzie publikował na swojej stronie internetowej swoje stanowisko dot. stosowania przepisów ustawy[49],
- będą organizowane konferencje lub warsztaty z udziałem przedstawicieli Prezesa UKE oraz ministra właściwego do spraw informatyzacji, których celem będzie wyjaśnienie stosowania przepisów ustawy.

CSIRT NASK niezwłocznie po wejściu w życie ustawy udostępni 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/DKIM/DMARC. Stosownie do potrzeb podmiotów publicznych będzie publikował także poradniki, w jaki sposób poprawnie skonfigurować te mechanizmy.

Ponadto CSIRT NASK niezwłocznie po wejściu w życie ustawy opublikuje w BIP NASK-PIB sposób zgłaszania domen, których podstawowym celem może być wprowadzenie w błąd użytkowników internetu.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ewaluacja efektów projektu nastąpi po roku od dnia wejścia w życie ustawy. Kolejna ewaluacja zostanie przeprowadzona po kolejnym roku. Zostaną zastosowane następujące mierniki:

1) liczba numerów wpisanych do wykazu numerów służących wyłącznie do odbierania połączeń głosowych;
2) liczba wzorców wiadomości o charakterze smishingu przekazanych przez CSIRT NASK do przedsiębiorców telekomunikacyjnych;
3) liczba sprzeciwów, które wpłynęły do Prezesa UKE, wraz z informacją o sposobie ich załatwienia;

[49] Stanowiska są co pewien czas wydawane przez Prezesa UKE np. https://uke.gov.pl/akt/bez-numerow-116-w-billingach-stanowisko-prezesa-uke,448.html. Oczywiście nie mają one charakteru wiążącego dla przedsiębiorców, stanowią jednak istotną wskazówkę dla podmiotów nadzorowanych przez Prezesa UKE.

4) liczba wydanych decyzji nakazujących przedsiębiorcy telekomunikacyjnemu zablokowanie dostępu do numeru lub usługi oraz nakładających obowiązek wstrzymania pobierania opłat za połączenia lub usługi zrealizowane po upływie tego terminu;
5) liczba wszczętych postępowań w sprawie nałożenia administracyjnej kary pieniężnej za niewykonanie obowiązków wynikających z ustawy, w tym liczba wydanych decyzji;
6) liczba domen wpisanych na listę ostrzeżeń;
7) liczba postępowań karnych wszczętych w sprawach przestępstw związanych z nadużyciami w komunikacji elektronicznej.

Mierniki te dadzą odpowiedź na pytanie, czy i w jaki sposób przepisy ustawy są stosowane. Mierniki w zakresie postępowań karnych wykażą skuteczność ścigania przestępstw mających charakter nadużyć w komunikacji elektronicznej.

Zostanie też przeprowadzona analiza orzecznictwa sądów w sprawach dot. postępowań karnych oraz odpowiedzialności administracyjnej wynikającej z nowych przepisów. Analiza ta wykaże istotne kwestie w wykładni przepisów ustawy przez sądy. Będzie ona stanowiła podstawę do ustalenia, czy konieczna jest interwencja prawodawcy celem doprecyzowania przepisów ustawy.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak.

RAPORT KONSULTACJI PUBLICZNYCH I OPINIOWANIA

projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej UD402.

Niniejszy raport został sporządzony na podstawie § 51 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów[1]. Zawiera on podsumowanie konsultacji publicznych oraz opiniowania ww. projektu ustawy.

1. Omówienie wyników przeprowadzonych konsultacji publicznych

Celem konsultacji publicznych i opiniowania było zapewnienie zainteresowanym podmiotom i organizacjom, możliwości wyrażenia opinii na temat projektowanej ustawy.

Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej UD402 w dniu 15.06.2022 r. został skierowany do konsultacji publicznych i opiniowania. Projekt został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny”[2] oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji[3], w celu zapoznania się z nim przez wszystkie zainteresowane podmioty. Ponadto, projekt został przesłany niżej wymienionym instytucjom w oddzielnej korespondencji.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 58 podmiotów w terminie do 14 dni od dnia doręczenia pisma Ministra Cyfryzacji. Zaproszenie w ramach konsultacji publicznych skierowano do następujących podmiotów:

1) American Chamber of Commerce in Poland;
2) Business Centre Club;
3) Federacja Konsumentów;
4) Fundacja Bezpieczna Przestrzeń;
5) Fundacja im. Kazimierza Pułaskiego;
6) Fundacja im. Stefana Batorego;
7) Fundacja Instytut Mikromakro;
8) Fundacja Moje Państwo;
9) Fundacja MY Pacjenci;
10) Fundacja Nowoczesna Polska;
11) Fundacja Panoptykon;
12) Fundacja Projekt: Polska;
13) Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego UW;
14) Izba Gospodarki Elektronicznej;
15) Klaster #CyberMadeInPoland;
16) Konfederacja Lewiatan;
17) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
18) Krajowa Izba Gospodarcza;
19) Krajowa Izba Gospodarki Cyfrowej;
20) Krajowa Izba Gospodarki Morskiej;
21) Krajowa Izba Komunikacji Ethernetowej;

[1] M.P. z 2022 r. poz. 348.

[2] https://legislacja.rcl.gov.pl/projekt/12360854 dostęp 20.07.2022 r.

[3] https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej.html dostęp 20.07.2022 r.

22) Krajowa Izba Rozliczeniowa S.A.;
23) Krajowe Stowarzyszenie Ochrony Informacji Niejawnych;
24) Naczelna Organizacja Techniczna;
25) Naczelna Rada Zrzeszeń Handlu i Usług;
26) Ogólnopolskie Porozumienie Organizacji Radioamatorskich;
27) PKP TELKOL sp. z o.o.;
28) Polska Federacja Szpitali;
29) Polska Izba Handlu;
30) Polska Izba Informatyki i Telekomunikacji;
31) Polska Izba Komunikacji Elektronicznej;
32) Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei;
33) Polska Izba Radiodyfuzji Cyfrowej;
34) Polska Organizacja Handlu i Dystrybucji;
35) Polska Organizacja Niebankowych Instytucji Płatności;
36) Polska Rada Biznesu;
37) Polska Wytwórnia Papierów Wartościowych;
38) Polski Związek Krótkofalowców;
39) Polski Związek Pracodawców Przemysłu Farmaceutycznego;
40) Polskie Centrum Badań i Certyfikacji S.A.;
41) Polskie Górnictwo Naftowe i Gazownictwo;
42) Polskie Koleje Państwowe S.A.;
43) Polskie Stowarzyszenie Marketingu SMB;
44) Polskie Towarzystwo Informatyczne;
45) Polskie Związek Przemysłu Motoryzacyjnego;
46) SABI – stowarzyszenie inspektorów ochrony danych;
47) Sieć Obywatelska Watchdog Polska;
48) Stowarzyszenie „Archiwizjoner”;
49) Stowarzyszenie Inżynierów Telekomunikacji;
50) Stowarzyszenie ISACA;
51) Towarzystwo Gospodarcze Polskie Elektrownie;
52) Związek Banków Polskich;
53) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska;
54) Związek Pracodawców Branży Internetowej IAB Polska;
55) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM;
56) Związek Pracodawców Mediów Publicznych;
57) Związek Przedsiębiorców i Pracodawców;
58) Związek Telewizji Kablowych w Polsce – Izba Gospodarcza.

W ramach opiniowania zaproszenie skierowano do następujących podmiotów:
1) Prezes Urzędu Ochrony Danych Osobowych;
2) Prezes Urzędu Ochrony Konkurencji i Konsumentów;
3) Prezes Urzędu Komunikacji Elektronicznej.

Do projektu ustawy w ramach konsultacji publicznych uwagi zgłosiły następujące podmioty:
1) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
2) Polska Izba Informatyki i Telekomunikacji;

3) Polska Izba Komunikacji Elektronicznej;
4) Polskie Towarzystwo Informatyczne Izba Rzeczoznawców;
5) R.M. osoba fizyczna;
6) Polskie Towarzystwo Informatyczne;
7) Porozumienie Zielonogórskie;
8) Polska Wytwórnia Papierów Wartościowych;
9) Krajowa Izba Komunikacji Ethernetowej;
10) HACK&PHACK DEFENCE LTD Piotr Marcin Wierzbicki;
11) IAB Polska;
12) Związek Banków Polskich;
13) Polska Wytwórnia Papierów Wartościowych;
14) Związek Telewizji Kablowych Izba Gospodarcza;
15) Unia Metropolii Polskich;
16) Nazwa.pl sp. z o.o.

Ponadto, w trybie opiniowania, opinie przedstawiły następujące podmioty:

1) Urząd Komunikacji Elektronicznej;
2) Urząd Ochrony Konkurencji i Konsumentów;
3) Komisja Nadzoru Finansowego;
4) Urząd Ochrony Danych Osobowych.

W procedurze opiniowania i konsultacji publicznych projektu ustawy wszystkim podmiotom umożliwiono zajęcie stanowiska w sprawie projektu, a także poddano analizie przedłożone przez te podmioty uwagi.

W ramach konsultacji zgłoszono 123 uwagi, a w ramach opiniowania 41 uwag.

Omówienie ww. uwag zostało przedstawione w załącznikach do niniejszego Raportu.

Ponadto, tabele zawierające stanowisko KPRM do zgłoszonych uwag udostępnione zostało na stronie RCL, w zakładce „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach procesu konsultacji i opiniowania znaczna liczba podmiotów zwracała uwagę na potrzebę wprowadzenia obligatoryjnego wymogu blokowania stron przez przedsiębiorcę telekomunikacyjnego, a nie jedynie uprawnienia do takiego działania. Zwrócono również uwagę na konieczność doprecyzowania przepisów wprowadzających sankcje tj. karę administracyjną oraz sankcję karną. Proponowano także zmiany w zakresie tworzenia oraz publikacji wzorca wiadomości stanowiących nadużycie w komunikacji elektronicznej.

W uwagach zgłoszonych podczas konsultacji publicznych pojawił się postulat ujednolicenia przepisów, które mogłyby kolidować bądź dublować przepisy z innych projektów ustaw m.in. projektu ustawy – Prawo komunikacji elektronicznej. Zgłoszono ponadto uwagi w zakresie definiowania pojęć zawartych w projekcie ustawy, zarówno pod względem wprowadzenia zmian, nowych pojęć bądź rezygnacji z definiowania pojęć zawartych dotychczas w projekcie ustawy. Szczególna uwaga została poświęcona propozycjom zmian dotyczących definicji kluczowych dla projektu ustawy – tj. smishing, CLI spoofing, sztuczny ruch.

Ważną kwestią, wielokrotnie podnoszoną podczas konsultacji publicznych, był postulat dookreślenia procesu monitorowania nadużyć w komunikacji elektronicznej przez CSIRT NASK, a także poszerzenia katalogu podmiotów nadzorowanych przez KNF. Ponadto zgłoszono uwagi

co do publicznego rejestru wzorców wiadomości argumentując to podatnością na wykorzystywanie jawnego rejestru przez oszustów.

2. Przedstawienie wyników konsultacji projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Projekt ustawy nie wymagał przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

3. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa

Zgodnie z przepisami ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej. W toku prac nad projektem wpłynęło jedno zgłoszenie lobbingowe do projektu ustawy, które zostało opublikowane w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Podmiot zgłaszający zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa – HACK&PHACK DEFENCE LTD Piotr Marcin Wierzbic.

Tabela uwag zgłoszonych w ramach opiniowania projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej.

Lp.	Instytucja	Jednostka redakcyjna	Treść uwagi	Odniesienie
1.	UKE	Uwaga ogólna	Uwaga ogólna -projektowana ustawa nakłada na UKE całkowicie nowe zadania, które wymagają wiedzy specjalistycznej, co wiąże się z koniecznością zatrudnienia albo co najmniej przeszkolenia pracowników. Niezbędne jest zatem zapewnienie środków dla Urzędu na realizację ww. zadań.	**Uwaga nieuwzględniona** Nowe zadania są ściśle powiązane z dotychczasowymi zadaniami UKE, w związku z czym urząd posiada już niezbędne kadry. W związku z tym możliwa jest realizacja nowych zadań w ramach posiadanych środków.
2.	UOKIK	Uwaga ogólna	Należy podkreślić, że projekt oraz zaprojektowane w nim rozwiązania należy co do zasady ocenić pozytywnie, szczególnie uwzględniając rosnącą liczbę stwierdzonych przypadków tzw. smishingu oraz spoofingu. Tego typu działania są sprzeczne z prawem i bezpośrednio prowadzą do znacznych strat finansowych po stronie konsumentów. Prezes Urzędu Ochrony Konkurencji i Konsumentów (dalej jako „Prezes UOKiK") otrzymuje zgłoszenia od osób, które były celem tego typu ataków. Rozwiązania prowadzące do zwiększenia ochrony konsumentów przed tego typu działaniami powinno się zatem uznać za pożądane. Jednocześnie wskazać należy, że projekt wymaga dopracowania w niektórych jego aspektach. W szczególności dotyczy to zagadnienia tzw. „sztucznego ruchu", które zostało zdefiniowane w tekście projektowanej ustawy, jednak nie zostało w jakikolwiek sposób rozwinięte w jej treści. Sztuczny ruch został wyszczególniony w art. 3 jako nadużycie w komunikacji elektronicznej, brakuje jednak w projekcie przepisów szczegółowych, których celem byłoby przeciwdziałanie lub zwalczanie do tego typu aktywności, analogicznie do przepisów dotyczących smishingu oraz spoofingu. Projekt wyraźnie koncentruje się na wspomnianych dwóch zjawiskach. Niezbędne jest przy tym wskazanie, że Prezes UOKiK w swojej praktyce spotkał się z przypadkami, w których wykonujący dużo połączeń konsumenci (zwykle korzystający z taryf „bez limitu")	**Uwaga nieuwzględniona** Do zjawiska sztucznego ruchu będzie miał zastosowanie ogólny przepis nakładający obowiązek stosowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Problemy wskazane w uwadze mogą zostać przezwyciężone w drodze postępowania reklamacyjnego, czy postępowań ADR prowadzonych przez Prezesa UKE. Nie jest uzasadnione wprowadzanie szczególnej regulacji, np. obowiązku informacyjnego, tylko i wyłącznie w związku z zapobieganiem i zwalczaniem zjawiska sztucznego ruchu.

			stawali się (niezamierzonym) celem mechanizmów lub działań ze strony operatorów telekomunikacyjnych, mających na celu przeciwdziałanie sztucznemu ruchowi. W stosowanych przez przedsiębiorców telekomunikacyjnych wzorcach umownych zdarzają się bardzo wysokie z perspektywy konsumenta kary za nadużycia telekomunikacyjne (np. w wysokości 5000 zł), które uznawane były za klauzule abuzywne m.in. ze względu na zbyt ogólne sformułowanie przesłanek określających, czy doszło do nadużycia. Tego typu sytuację należałoby ocenić jako niekorzystną dla konsumentów. W związku z powyższym wydaje się, że byłoby uzasadnione przyjęcie szczegółowych rozwiązań dopasowanych do zwalczania sztucznego ruchu, przewidujących jednocześnie możliwość ochrony konsumentów przed nieproporcjonalnym lub omyłkowym działaniem przedsiębiorców telekomunikacyjnych, np. przez udzielenie im odpowiednich informacji o podstawie podjęcia działań przez operatora oraz umożliwienie powtórnej weryfikacji sytuacji.	
3.	DC UKNF	Art. 2 pkt 4	Definicja nadużycia w komunikacji elektronicznej odnosi się do użytkownika końcowego, którym zgodnie z art. 2 pkt 50 ustawy Prawo telekomunikacyjne jest podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi, dla zaspokojenia własnych potrzeb. W praktyce można spotkać się zaś z przypadkami, w których atak cyberprzestępców dokonywany jest na osobę fizyczną, np. pracownika instytucji państwowej lub podmiotu gospodarczego, w celu wyrządzenia szkody tej instytucji bądź podmiotowi gospodarczemu. Dotyczy to zarówno sytuacji, gdy ofiara ataku korzysta z urządzenia służbowego oraz usługi telekomunikacyjnej, której abonentem jest pracodawca, jak i przypadku, w którym atak nakierowany jest na prywatne urządzenia użytkownika i wykorzystywane przez niego prywatne usługi telekomunikacyjne. Użycie w ramach omawianego przepisu terminu „użytkownik końcowy” może powodować konieczność	**Uwaga wyjaśniona w zakresie pojęcia użytkownika końcowego** W pierwszym opisanym przypadku nadużycie w komunikacji elektronicznej jest kierowane przeciwko instytucji państwowej, która jest użytkownikiem końcowym. W drugim przypadku nadużycie jest wobec pracownika tej instytucji, przy wykorzystaniu jego prywatnych urządzeń – pracownik też jest użytkownikiem końcowym.

			doprecyzowania jego treści tak, aby objęte nim były również rodzaje przypadków zasygnalizowane powyżej. Jednocześnie omawiana definicja posługuje się sformułowaniem „osiągnięcie nienależnych korzyści". Zasadna jest w ocenie UKNF zmiana omawianego sformułowania na „osiągnięcie nienależnych korzyści dla siebie lub kogo innego" (wyrażeniem takim posłużono się np. w art. 297 k.k.) lub „osiągnięcie nienależnych korzyści dla siebie lub innej osoby". Mogą bowiem wystąpić sytuacje, w których celem lub skutkiem działania osoby dopuszczającej się nadużycia w komunikacji elektronicznej nie jest osiągnięcie korzyści dla siebie – sytuacja taka może wystąpić w szczególności, gdy osoba taka działa z polecenia innej osoby i nie osiąga korzyści z samego nadużycia w komunikacji elektronicznej, natomiast osiąga je osoba „zlecająca" tego rodzaju działanie. W kontekście art. 16 projektu ustawy omawiana zmiana nie jest przy tym w ocenie UKNF wymagana z uwagi na definicję korzyści majątkowej lub osobistej, którą zawiera art. 115 § 4 k.k., a która odnosi się do korzyści zarówno dla siebie, jak i dla kogo innego. Wątpliwe byłoby jednak zastosowanie omawianej definicji do art. 2 pkt 4 projektu ustawy, gdyż nie ma on charakter przepisu prawnokarnego, a także z uwagi na zasadę zakazu rozszerzającej wykładni norm o charakterze represywnym.	**Uwaga uwzględniona w pozostałym zakresie –** osiągnięcie nienależnych korzyści zostanie zamienione na „osiągnięcie nienależnych korzyści dla siebie lub innej osoby"
4.	UOKIK	Art. 2 pkt 4	Art. 2 pkt 4 W projekcie pojawia się definicja nadużycia w komunikacji elektronicznej, rozumianego jako świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści. W art. 2 pkt 12 projektu zdefiniowano także usługę komunikacji interpersonalnej, a w art. 2 pkt 13 z kolei usługę komunikacji interpersonalnej niewykorzystującą numerów.	**Uwaga nieuwzględniona** Szersza definicja w ustawie jest niezbędna z powodu wprowadzenia przepisów dotyczących poczty elektronicznej. Z uwagi na wykorzystywanie w komunikacji elektronicznej również szyfrowania end-to-end, które sprawia, że wykrywanie części nadużyć byłoby niemożliwe, a także kwestie prywatności w

			Niezbędne jest wskazanie, że zgodnie z art. 2 pkt 48 ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 501), usługę telekomunikacyjną określa się jako usługę polegającą głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej. Tym samym definicja nadużycia w komunikacji elektronicznej odnosi się wyłącznie do wąskiej definicji usługi telekomunikacyjnej i pomija definicje usługi komunikacji interpersonalnej i komunikacji interpersonalnej niewykorzystującej numerów. Wydaje się, że tego typu wąskie zakreślenie zakresu przedmiotowego art. 2 pkt 4 projektu nie jest wskazane i być może rozważyć należałoby jego rozszerzenie o dodatkowe definicje.	komunikacji, nie proponuje się objęcia tej komunikacji szczególnymi rozwiązaniami w projekcie ustawy.
5.	DC UKNF	Art. 3 ust. 1 pkt 2	Zakaz sformułowany w art. 3 ust. 1 pkt 2 projektu ustawy obejmuje wiadomości SMS, jednak poza jego zakresem pozostają wiadomości EMS i MMS. Jeżeli technicznie możliwe jest wykorzystanie wiadomości EMS lub MMS w celach wskazanych w w/w przepisie, a także blokowanie tego rodzaju wiadomości przez przedsiębiorców telekomunikacyjnych, to zasadnym wydaje się rozszerzenie zakresu omawianego zakazu również na wiadomości EMS i MMS. Postulat ten uzasadniony jest również doświadczeniami UKNF w zakresie monitorowania negatywnych zjawisk na rynku finansowym oraz im przeciwdziałania. Znane są bowiem przypadki wykorzystywania wiadomości MMS w celu podszycia się przez nadawcę pod inny podmiot, aby nakłonić odbiorcę takiej wiadomości do określonego działania (w szczególności przekazania danych osobowych czy rozporządzenia majątkiem). W przypadku uwzględnienia niniejszej uwagi, uzasadnione będą także zmiany dostosowujące w: art. 1 pkt 2, art. 4 ust. 1-3 oraz 5-6, art. 5 ust. 1 i 2, art. 6 ust. 1 pkt 2, art. 7, art. 14 ust. 2 oraz ust. 3 pkt 1, oraz art. 16 ust. 1 pkt 2.	**Uwaga częściowo uwzględniona** Ustawa będzie odnosić się do wiadomości MMS, w kontekście uprawnienia przedsiębiorcy telekomunikacyjnego do blokowania MMS, które będą zawierające treści wyczerpujące znamiona smishingu, a także w kontekście penalizowania wysyłki takich wiadomości.
6.	DC UKNF	Art. 3 ust. 1 pkt 2 oraz art. 16 ust. 1 pkt 2	Omawiany zakaz odnosi się do wysyłania SMS, w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy od określonego działania, m.in. nieświadomego rozporządzenia	**Uwaga nieuwzględniona** Zawarte w ustawie brzmienie lepiej oddaje istotę nadużyć w

			majątkiem. Omawiany katalog działań, do których nakłaniać może nadawca, ma co prawda charakter otwarty, jednak sugerujemy rozważenie zastąpienia terminu „nieświadomego” (w ramach w/w sformułowania) terminem „niekorzystnego” rozporządzenia majątkiem. Nieświadomy oznacza bowiem niezdający sobie z czegoś sprawy, powstały bez udziału świadomości. Zmiana ta pozwoli uniknąć wątpliwości, że zakaz rozciąga się również na nakłanianie, poprzez podszywanie się pod inny podmiot, do rozporządzenia majątkiem, które jest świadome ale niekorzystne dla ofiary ataku. Sama czynność rozporządzenia majątkiem będzie zazwyczaj dokonywana pod wpływem błędu, który wywołał sprawca. Również znamiona przestępstwa oszustwa (art. 286 k.k.) nie wymagają braku „świadomości” działania pokrzywdzonego, a odnoszą się one do niekorzystnego rozporządzenia mieniem. Omawiana uwaga odnosi się również do art. 16 ust. 1 pkt 2 projektu ustawy.	telekomunikacji elektronicznej. Istotą smishingu jest podszycie pod inny podmiot i doprowadzenie użytkownika do dokonania czynności, której konsekwencji nie jest świadom. W ramach normalnego obrotu gospodarczego dochodzi z kolei do wielu transakcji gdzie można mówić o niekorzystnym rozporządzeniu majątkiem, ale jeśli osoba dokonująca danej czynności jest świadoma jej konsekwencji to nie mamy do czynienia z przestępstwem. Z powyższych względów pozostawiono dotychczasowe brzmienie przepisu.
7.	DC UKNF	Art. 3 ust. 1 pkt 3	W zakresie użytego w tym przepisie terminu „nieświadomego rozporządzenia majątkiem” postulujemy rozważenie zastąpienia go terminem „niekorzystnego rozporządzenia majątkiem”, z tożsamych przyczyn jak wskazane w w/w uwadze do art. 3 ust. 1 pkt 2 projektu ustawy.	**Uwaga nieuwzględniona** Zawarte w ustawie brzmienie lepiej oddaje istotę nadużyć w telekomunikacji elektronicznej. Istotą smishingu jest podszycie pod inny podmiot i doprowadzenie użytkownika do dokonania czynności, której konsekwencji nie jest świadom. W ramach normalnego obrotu gospodarczego dochodzi z kolei do wielu transakcji gdzie można mówić o niekorzystnym rozporządzeniu majątkiem, ale

				jeśli osoba dokonująca danej czynności jest świadoma jej konsekwencji to nie mamy do czynienia z przestępstwem. Z powyższych względów pozostawiono dotychczasowe brzmienie przepisu.
8.	UOKIK	Art. 4 ust. 2	**4 ust. 2** Prezes UOKiK popiera ogólny kierunek wprowadzonych rozwiązań legislacyjnych, a także wspiera zmiany regulacyjne, które pozwolą na skuteczną walkę ze zjawiskiem smishingu. Jednocześnie należy wskazać, że według założeń omawianego przepisu, CSIRT NASK będzie posiadać bardzo dużą uznaniowość odnośnie do tworzenia wzorca wiadomości wyczerpującej znamiona smishingu. Wzorzec ten posłużyć ma w następnej kolejności do rozpoczęcia przez przedsiębiorców telekomunikacyjnych niezwłocznego blokowania krótkich wiadomości tekstowych (SMS) zawierających treści zawarte we wzorcu wiadomości. Prezes UOKiK stale otrzymuje różnorodne sygnały ze strony konsumentów oraz przedsiębiorców, dotyczące bardzo szerokiego spektrum praktyk rynkowych i zagadnień, wliczając w to liczne zgłoszenia dotyczące sfery telekomunikacji i e-commerce. Prezes UOKiK jest podmiotem, który regularnie styka się zatem z przejawami nadużyć w komunikacji elektronicznej, zarówno noszącymi znamiona smishingu i spoofingu, jak i innymi. W związku z powyższym istnieje możliwość, że Prezes UOKiK wejdzie w posiadanie informacji na temat praktyki lub zjawiska w telekomunikacji niezgodnego z prawem, zgłoszenie którego do CSIRT NASK może być uzasadnione, w tym na przykład identyfikacji wiadomości noszącej znamiona smishingu. Wydaje się zatem zasadne, aby CSIRT NASK zobowiązany	**Uwaga nieuwzględniona** Nie jest w ocenie projektodawcy zasadne tak dokładne ukształtowanie zasad współpracy pomiędzy różnymi podmiotami administracji publicznej. Każdy podmiot posiadający informacje o występujących przypadkach smishingu może poinformować o tym CSIRT NASK. Takie działania mieszczą się w ramach normalnego funkcjonowania podmiotów publicznych i nie wymagają uściślenia w ustawie. Należy również zauważyć, że każdy będzie mógł zapoznać się ze wzorcem wiadomości wyczerpującej znamiona smishingu po jego udostępnieniu na stronie internetowej, a nadawca zablokowanej wiadomości SMS, będzie mógł wnieść sprzeciw do Prezesa UKE.

			był do udzielenia pisemnej odpowiedzi Prezesowi UOKiK w przypadku uznania, że dana wiadomość nie stanowi smishingu. Uzasadnienie odmownej decyzji pozwoliłoby to Prezesowi UOKiK na zdobycie informacji z zakresu nadużyć telekomunikacyjnych, a tym samym lepsze wykonywanie jego funkcji i potencjalne zwiększenie poziomu ochrony konsumentów w Polsce.	W związku z powyższym proces tworzenia i publikacji wzorców smishingowych został kompleksowo uregulowany i nie wymaga zmian, o których mowa w uwadze.
9.	DC UKNF	Art. 4 ust. 4	Przepis przewiduje udostępnianie na stronie internetowej CSIRT NASK wzorców wiadomości wyczerpujących znamiona smishingu. Udostępnianie tego rodzaju wzorców wiąże się w ocenie UKNF z ryzykiem wykorzystania tych informacji przez przestępców do przygotowywania wiadomości, które będą odróżniały się od opublikowanych wzorców, w celu ominięcia zabezpieczeń. Sugerujemy rozważenie usunięcia omawianego przepisu i pozostawienie sposobu przekazywania informacji o wzorcach tego typu wiadomości w sposób przewidziany w projektowanym art. 4 ust. 3, podmiotom w nim wskazanym, pozostawiając wzorce poza możliwością publicznego do nich dostępu.	**Uwaga nieuwzględniona** Jawność wzorca wiadomości smishingowej jest niezbędna dla zapewnienia przejrzystości procesu blokowania wiadomości a także jest niezbędna dla zagwarantowania praw użytkowników i możliwości skorzystania z instytucji sprzeciwu przez nadawcę wiadomości, która została zablokowana jako wpisująca się we wzorzec.
10.	UOKIK	Art. 4 ust. 4	Art. 4 ust. 4 Przepis wskazuje, że wzorzec wiadomości wyczerpującej znamiona smishingu, CSIRT NASK udostępnia na swojej stronie internetowej, w terminie 14 dni nie później jednak niż w terminie 21 dni od dnia jego przekazania przedsiębiorcy telekomunikacyjnemu. Z perspektywy Prezesa UOKiK, powyższe terminy są relatywnie długie, jeśli chodzi o kwestie cyberbezpieczeństwa i ochrony konsumentów. Należy także zauważyć, że mimo obowiązku niezwłocznego blokowania tego typu wiadomości przez przedsiębiorcę (art. 4 ust. 6), istnieje ryzyko modyfikacji treści wiadomości przez jej autora i dalszego jej wysyłania, przy zachowaniu zbliżonej treści lub sposobu jej sformułowania. Tym samym jak najwcześniejsza możliwość zapoznania się ze wzorcem takiej	**Uwaga wyjaśniona** Opisany mechanizm dotyczy publikacji wzorca dla wszystkich odbiorców, a nie jego przekazania do przedsiębiorców telekomunikacyjnych. Przekazanie wzorca do przedsiębiorcy następuje niezwłocznie po jego zidentyfikowaniu przez CSIRT NASK. W związku z tym ochrona konsumentów będzie następować w najszybszym możliwym

			wiadomości może być korzystna z punktu widzenia ochrony jej potencjalnych odbiorców. Dzięki temu możliwe byłoby także przekazanie informacji na temat danego przypadku i stosowanej metody smishingu do publicznej wiadomości. Warto zatem rozważyć skrócenie wskazanych w projekcie terminów udostępnienia wzorca wiadomości przez CSIRT NASK na jego stronie internetowej. Można także zauważyć, że uzasadnienie projektu nie odnosi się w jakikolwiek sposób do wskazanych terminów i trudno ocenić, na jakiej podstawie zostały określone, a także czy ich długość jest uzasadniona ograniczeniami technologicznymi.	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.
11.	UKE	Art. 4 ust. 5	Art. 4 ust. 5 – proponuje się doprecyzować pojęcie „niecelowości” (blokowania SMS). Jest to o tyle istotne, że w art. 4 ust. 6 pkt 2 ponownie użyte jest to pojęcie w kontekście obowiązku ciążącego na przedsiębiorcy telekomunikacyjnym, za którego niewykonanie przewidziano karę pieniężną w art. 15 ust. 2 pkt 1 projektu. W omawianym przepisie należy również skreślić wyraz „uzna”, który jest zbędny, a nadto sugeruje arbitralność decyzji CSIRT NASK.	**Uwaga częściowo uwzględniona w zakresie pojęcia niecelowości.** Pojęcie niecelowości zostanie wyjaśnione w uzasadnieniu. Niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS), jeżeli pomimo wzorca: smishing dociera do użytkowników i wzorzec musi być poprawiony lub wzorzec jest zbyt szeroki i blokuje także sms nie mające charakteru smishingu, a także gdy oszuści już nie korzystają z wcześniejszych metod w smishingu, np. nie używają sformułowań związanych ze szczepieniem. Wzorzec może być wycofany. **Uwaga nieuwzględniona w pozostałym zakresie**

				Nie ma konieczności usunięcia wyrazu „uzna” – CSIRT NASK dokonuje subsumpcji i kwalifikuje sms jako zawierający treści o charakterze smishingu w oparciu o przepisy prawa.
12.	UKE	Art. 4 ust. 6 pkt 1	Art. 4 ust. 6 pkt 1 – wyraz „niezwłocznego” należy przenieść do wprowadzenia do wyliczenia w ust. 6 tak, aby dotyczył on obu punktów.	**Uwaga uwzględniona**
13.	UKE	Art. 5 ust. 2	Art. 5 ust. 2 – wydaje się, że sprzeciw powinien zawierać przede wszystkim treść krótkiej wiadomości tekstowej (SMS), gdyż to ona decyduje o wystąpieniu smishingu.	**Uwaga uwzględniona**
14.	UKE	Art. 6 ust. 1	Art. 6 ust. 1 – celowe jest doprecyzowanie przepisu poprzez jednoznaczne przesądzenie, że do sprzeciwu nie stosuje się przepisów Kodeksu postępowania administracyjnego. Poza tym w przepisie brak jest obowiązku Prezesa UKE w zakresie powiadomienia CSIRT NASK o uwzględnieniu sprzeciwu.	**Uwaga uwzględniona** Zostanie dodane wyłączenie stosowania KPA, a także obowiązek Prezesa UKE o poinformowaniu CSIRT NASK o uwzględnieniu sprzeciwu.
15.	UOKIK	Art. 7	Art. 7 Zgodnie z treścią tego przepisu, przedsiębiorca telekomunikacyjny może blokować krótkie wiadomości tekstowe (SMS) zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości CSIRT NASK. W ocenie Prezesa UOKiK istnieją określone zagrożenia związane z uznaniowym charakterem uprawnienia, w jakie wyposażeni zostają przedsiębiorcy w omawianym zakresie. Nie istnieją żadne reguły dotyczące blokowania wiadomości SMS przez przedsiębiorców na podstawie tego przepisu. Istnieje zatem ryzyko stosowania przez nich arbitralnych kryteriów oceny danej wiadomości, stanowiących podstawę podjęcia decyzji o blokowaniu krótkiej wiadomości tekstowej.	**Uwaga nieuwzględniona** Przedsiębiorcy telekomunikacyjni będą podlegali odpowiedzialności kontraktowej za niewykonanie usługi. Kwestie te powinny zostać rozstrzygnięte w ramach postępowania reklamacyjnego, prowadzonego przez Prezesa UKE postępowania ADR, czy w związku z postanowieniami umownymi.

			Prezes UOKiK w swojej działalności obserwuje różnego rodzaju nieprawidłowości, których dopuszczają się nie tylko podmioty trzecie względem dostawców usług telekomunikacyjnych (niepowiązane z nimi), lecz także kontrahenci przedsiębiorców telekomunikacyjnych świadczący np. usługi rozliczane w modelu direct billing (doliczania do rachunku) lub usługi premium, w ramach których część korzyści ze świadczenia usługi czerpie również przedsiębiorca telekomunikacyjny. W przeszłości zdarzały się przypadki braku stosownej reakcji na sygnalizowane przez konsumentów nieprawidłowości związane z różnego rodzaju kampaniami SMS-owymi prowadzonymi przez kontrahentów przedsiębiorców telekomunikacyjnych1. Ustalenie zasad blokowania wiadomości jednolitych dla różnego rodzaju nadużyć mogłoby być zasadne, z uwagi na potrzebę zapewnienia równych standardów traktowania dla wszystkich uczestników rynku. Wskazane byłoby także udzielenie informacji konsumentowi na temat zablokowania danej wiadomości i wskazanie, z jakich przyczyn została zablokowana. Adresat miałby dzięki temu świadomość, że została do niego skierowana wiadomość, która jednak w ocenie przedsiębiorcy nosiła znamiona smishingu. Jednocześnie mógłby dzięki temu zakwestionować decyzję operatora, jeśli jego zdaniem została zaklasyfikowania jako smishing błędnie i powinna zostać dostarczona, co ograniczyłoby negatywne skutki ewentualnych błędów przy realizacji ww. obowiązków. Uwzględniając, że art. 7 daje przedsiębiorcy możliwość uznaniowego, arbitralnego klasyfikowania wiadomości SMS, tego typu sytuacje mogą mieć miejsce. Dlatego wydaje się, że wprowadzenie obowiązku informowania konsumenta przez przedsiębiorcę byłoby uzasadnione.	
16.	UKE	Art. 8	Art. 8 – rekomenduje się użycie w tym przepisie zwrotu „eliminacja prezentacji identyfikacji numeru wywołującego”, by w największym możliwym stopniu zapewnić zgodność terminologiczną projektowanego przepisu z art. 171 Prawa telekomunikacyjnego. Poza tym omawiany przepis nie określa dostatecznie jasno zakresu	**Uwaga częściowo uwzględniona** Zamiast „informacji adresowej” zostanie użyte sformułowanie „ukrycie informacji numeru wywołującego”.

			stosowania ustanowionej w nim normy. Z dosłownego jego brzmienia odnieść można wrażenie, że przedsiębiorca telekomunikacyjny zawsze ma blokować połączenie głosowe albo ukrywać identyfikację numeru wywołującego dla użytkownika końcowego. Dlatego poddaje się pod rozwagę, aby treść przepisu rozpoczynała się np. od wyrazów: „W przypadku uzasadnionego podejrzenia CLI spoofingu (...)”	Należy zauważyć, że art. 8 ustanawia ogólny obowiązek blokowania połączeń głosowych w ramach zwalczania i przeciwdziałanie spoofingowi. Użyte sformułowanie jest najbardziej ogólne tak aby objąć całość działalności przedsiębiorców telekomunikacyjnych w tym zakresie. Przepis ten musi również być odczytywany w kontekście całej ustawy, a zwłaszcza przepisów mówiących o porozumieniu między przedsiębiorcami telekomunikacyjnymi a Prezesem UKE. W związku z tym opisywane w tym przepisie działanie będzie wynikało z wprowadzonych środków technicznych i organizacyjnych służących przeciwdziałaniu nadużyciom w telekomunikacji elektronicznej. W związku z powyższym nie jest konieczne doprecyzowanie tego przepisu.
17.	UOKIK	Art. 8	Art. 8 W opinii Prezesa UOKiK, wskazany przepis budzi wątpliwości interpretacyjne w odniesieniu do sformułowania „ukrywa identyfikację numeru wywołującego dla użytkownika końcowego”. Wskazane byłoby wyjaśnienie, jak należy rozumieć to stwierdzenie. Czy chodzi tu o ukrycie numeru przez operatora w taki sposób, że	**Uwaga wyjaśniona** Tak, chodzi o ukrycie numeru przez operatora w taki sposób, że numer telefonu udający numer innego podmiotu miałby nie być pokazywany na wyświetlaczu

			numer telefonu udający numer innego podmiotu miałby nie być pokazywany na wyświetlaczu odbiorcy? Opisane sformułowanie może być interpretowane na różne sposoby, a w takiej sytuacji jego doprecyzowanie może pozwolić na zwiększenie przejrzystości omawianego przepisu. W ramach propozycji, można zasugerować zmianę sformułowania na „ukrywa nieprawdziwą identyfikację numeru wywołującego dla użytkownika końcowego”.	odbiorcy (per analogiam jak działa usługa CLIR). Ukrycie prezentacji identyfikacji linii wywołującej oznacza w praktyce, że odbiorcy wyświetli się, że dzwoni do niego nieznany numer a nie np. informacja, ze dzwoni osoba bliska, której numer jest wpisany na liście kontaktów. Pozwoli to zapobiec takim atakom jak np. podszycie się pod byłego szefa CBA Pawła Wojtunika.
18.	UKE	Art. 9 ust. 1	Art. 9 ust. 1 - proponuje się wykorzystanie do prowadzenia wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych systemu teleinformatycznego, o którym mowa w art. 29b ust. 2 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, po dokonaniu jego rozbudowy o wymaganą do tego funkcjonalność. Proponowane rozwiązanie zapewni udostępnienie pełnego wykazu do pobrania (w odpowiednim formacie) wyłącznie zweryfikowanym i podłączonym do tego systemu przedsiębiorcom telekomunikacyjnym, na potrzeby implementacji rozwiązań służących zapobieganiu i zwalczaniu CLI spoofingu. Z kolei podmiotom innym niż przedsiębiorcy telekomunikacyjni, w szczególności abonentom wnioskującym o wpis wykorzystywanego przez siebie numeru do wykazu, o którym mowa w art. 9 ust. 1 projektu, powinna być jedynie zapewniona możliwość wglądu do tego wykazu i to tylko w zakresie obejmującym wpisane numery (tzn. bez danych podmiotów, które te numery wykorzystują). Powyższe mogłoby nastąpić np. poprzez udostępnienie zanonimizowanych danych z wykazu, o którym mowa w art. 9 ust. 1 projektu, w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa UKE.	**Uwaga uwzględniona w zakresie wykreślenia wyrazu „telefonów”** **W pozostałym zakresie uwaga nieuwzględniona** W ocenie projektodawcy, nie jest zasadne wskazywanie konkretnego systemu teleinformatycznego w tym przepisie, a zapewnić możliwość jak najłatwiejszej i jak najmniej obciążającej zarówno Urząd jak i przedsiębiorców telekomunikacyjnych integracji w celu wykonania postanowień ustawy.

			Niezależnie od powyższego z ust. 1 należy wykreślić wyraz „telefonów", by zapewnić spójność terminologiczną z Prawem telekomunikacyjnym.	
19.	DC UKNF	Art. 9 ust. 2	Katalog podmiotów uprawnionych do złożenia wniosku o wpis do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych obejmuje obecnie jednostki sektora finansów publicznych oraz banki. Zagrożenie związane ze spoofingiem dotyczy zaś szerszej kategorii podmiotów rynku finansowego. Podwyższone ryzyko „podszywania się" z wykorzystaniem spoofingu dotyczy przede wszystkim tych podmiotów, które prowadzą rachunki (bankowe, płatnicze lub papierów wartościowych), świadczą usługi płatnicze, bądź prowadzą działalność inwestycyjną (lokują środki pieniężne zebrane w drodze proponowania nabycia jednostek uczestnictwa albo certyfikatów inwestycyjnych w określone w ustawie papiery wartościowe, instrumenty rynku pieniężnego i inne prawa majątkowe) ale może również obejmować podmioty z sektora ubezpieczeniowego. W związku z powyższym sugerujemy rozważenie poszerzenia omawianego katalogu o możliwość złożenia wniosku przez inne podmioty sektora finansowego szczególnie narażone na spoofing. Dotyczy to przede wszystkim następujących podmiotów, podlegających nadzorowi KNF lub nadzorowi państwa macierzystego (jak w przypadku oddziałów instytucji kredytowych): spółdzielczej kasy oszczędnościowo-kredytowej lub Krajowej Kasy Oszczędnościowo-Kredytowej, instytucji płatniczej, firmy inwestycyjnej, funduszu inwestycyjnego lub towarzystwa funduszy inwestycyjnych, zakładu ubezpieczeń lub zakładu reasekuracji, oddziału instytucji kredytowej. Jednocześnie, ze względu na istotną rolę na rynku finansowym niektórych podmiotów pozostających poza nadzorem KNF, a także	**Uwaga częściowo uwzględniona** Dodane zostaną kategorie podmiotów, które są nadzorowane przez KNF. **Uwaga nieuwzględniona w zakresie podmiotów uprawnionych do złożenia ww. wniosku do rozporządzenia Prezesa RM** Takie rozwiązanie nie wydaje się adekwatne, biorąc pod uwagę, że adresaci uprawnień i obowiązków, to co do zasady, powinny zostać określeni w przepisach rangi ustawowej.

			podwyższone ryzyko „podszycia się" pod takie podmioty w ramach ataku z użyciem spoofingu, sugerujemy rozważenie dodania do omawianego katalogu również tego rodzaju podmiotów (zastrzegając jednocześnie, że np. w przypadku podmiotów prowadzących systemy płatności istotna może być opinia Prezesa Narodowego Banku Polskiego sprawującego nadzór systemowy nad systemem płatniczym). Dotyczy to w szczególności następujących kategorii podmiotów: bankowej izby gospodarczej, podmiotu prowadzącego system płatności, instytucji utworzonej na mocy art. 105 ust. 4 ustawy z dnia z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2021 r. poz. 2439 z późn. zm.). Poddajemy pod rozwagę delegowanie katalogu podmiotów uprawnionych do złożenia w/w wniosku do Rozporządzenia Prezesa RM, co w opinii Urzędu KNF usprawni proces zarządzania katalogiem uprawnionych podmiotów w przypadku konieczności jego aktualizacji.	
20.	DC UKNF	Art. 9 ust. 4	Wniosek o wpis numeru do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych ma zawierać jedynie oznaczenie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych. Brak jest natomiast przewidzianego środka weryfikacji, czy zgłaszany numer w rzeczywistości należy do wnioskodawcy. Można rozważyć w tym zakresie wymóg załączenia aktualnej umowy na usługi telekomunikacyjne dotyczące omawianego numeru bądź weryfikację przez Prezesa UKE u przedsiębiorcy telekomunikacyjnego prowadzącego numer (wtedy należałoby przewidzieć wymóg wskazywania takiej informacji we wniosku). Brak wprowadzenia środka weryfikacji uprawnienia wnioskodawcy do zgłaszanego przez niego numeru telefonu może bowiem kreować ryzyko złośliwego/nieuprawnionego zablokowania możliwości wykonywania	**Uwaga uwzględniona** Zostanie dodany w przepisie wymóg udowodnienia we wniosku korzystania z numeru. **Uwaga wyjaśniona** Wykaz będzie jawny, więc będzie możliwość wycofania wniosku przez kolejny podmiot korzystający z numeracji.

			połączeń z numerów telefonów podmiotów, o których mowa w projektowanym art. 9 ust. 2 ustawy. Jednocześnie zwracamy uwagę, że Projekt nie obejmuje sytuacji, w której podmiot uprawniony przestaje korzystać ze zgłoszonej przez niego puli numeracyjnej (i nie informuje o tym fakcje Prezesa UKE). Pomimo zmiany abonenta pula numerów nadal jest blokowana. Może to doprowadzić do sytuacji pozyskania i dalszego wykorzystania przez podmiot nieuprawniony puli numeracyjnej z której korzystał uprzednio podmiot uprawniony, a która pozostaje wpisana w wykazie.	
21.	UKE	Art. 9 ust. 6	Art. 9 ust. 6 - zasadnym jest doprecyzować ten przepis, aby zakreślony dla Prezesa UKE 5-dniowy termin na wpis do wykazu dotyczył kompletnego wniosku.	**Uwaga uwzględniona**
22.	UKE	Art. 9 ust. 8	Art. 9 ust. 8 - sugeruje się rezygnację z formy decyzji administracyjnej dla odmowy dokonania wpisu do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych. Wniosek niezgodny z art. 9 ust. 2 i 3 projektu powinien być pozostawiony przez organ bez rozpoznania, co uprości i odformalizuje procedurę odmowy dokonania wpisu do wykazu. Poza tym należy zauważyć, że przepis ust. 8 jest wadliwie skonstruowany, ponieważ wynika z niego, że przesłanką odmowy wpisu jest to, że numer jest niewykorzystywany przez podmiot nieuprawniony.	**Uwaga częściowo uwzględniona** Usunięty zostanie wymóg decyzji administracyjnej dla odmowy dokonania wpisu do wykazu numerów. Ust. 8 zostanie poprawiony. **Uwaga nieuwzględniona w pozostałym zakresie** W zakresie numeru niewykorzystywanego należy zauważyć, że ust. 8 musi być czytany w kontekście całego art. 9. Na etapie składania wniosku, wnioskodawca musi przedstawić dowód, że numer wskazany we wniosku należy do niego. Na tym etapie jest to badane jedynie pod kątem formalnym. Sformułowanie o „niewykorzystywanym numerze” w ust. 8 jest za to

				podstawą do organu do zbadania pod kątem materialnym, czy rzeczywiście numer ten jest użytkowany przez dany podmiot. Z tego względu przepis w tym brzmieniu jest potrzebny.
23.	UKE	Art. 9 ust. 9	Art. 9 ust. 9 -wyraz „złożenia” należy zastąpić wyrazem „otrzymania” (wniosku) by zapewnić jednolitość brzmienia tego ustępu z ust. 6.	**Uwaga uwzględniona**
24.	UKE	Art. 10 ust. 1	Art. 10 ust. 1 – proponuje się zawężenie kręgu podmiotów, które mogą zawrzeć z Prezesem UKE porozumienie, jedynie do operatorów zapewniających świadczenie usług dla co najmniej 50 000 abonentów. Zapewnienie wszystkim operatorom możliwości podpisania porozumienia z Prezesem UKE będzie dla Prezesa UKE bardzo trudne do realizacji z uwagi na znaczną liczbę tych podmiotów i spowoduje zagrożenie dla sprawnej realizacji innych zadań organu. Przyjęcie progu 50 000 abonentów pozwoli na zawarcie porozumienia z kluczowymi podmiotami (ok. 15) świadczącymi usługę telefonii stacjonarnej i mobilnej (obsługującymi 99,68% użytkowników sieci ruchomych i 90,81% użytkowników sieci stacjonarnych w Polsce), które ze względu na posiadany potencjał techniczny i ludzki będą w stanie aktywnie uczestniczyć w implementacji i dalszym rozwoju rozwiązań przeciwdziałających CLI spoofingowi. Dla pozostałych przedsiębiorców telekomunikacyjnych Prezes UKE powinien natomiast wydawać rekomendacje dotyczące środków organizacyjnych i technicznych, służących realizacji obowiązku, o którym mowa w art. 8 projektu. Skutkiem prawidłowego wykonywania rekomendacji powinno być zaś to, że przedsiębiorca telekomunikacyjny nie będzie ponosił odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będącej skutkiem wprowadzonych środków technicznych i organizacyjnych, o których mowa w tych rekomendacjach (analogicznie jak w przypadku porozumienia – por. art. 10 ust. 3 projektu). Realizowanie przez pozostałych przedsiębiorców	**Uwaga uwzględniona**

			telekomunikacyjnych rekomendacji wydawanych przez Prezesa UKE zapewni spójność ze środkami organizacyjnymi i technicznymi określonymi w porozumieniu, o którym mowa w art. 10 ust. 1 projektu.	
25.	UOKIK	Art. 10 ust. 1	Art. 10 ust. 1 Art. 10 wskazuje jako jego adresatów operatorów, którzy mogą zawrzeć z Prezesem UKE porozumienie z zakresu realizacji obowiązków, o których mowa w art. 8. Art. 8 posługuje się wyłącznie terminem „przedsiębiorca telekomunikacyjny", na którego nakłada obowiązek blokowania połączenia głosowego albo ukrywania identyfikacji numeru wywołującego dla użytkownika końcowego. Termin operator i przedsiębiorca telekomunikacyjny zostały zdefiniowane w art. 2 odmiennie i jako odrębne od siebie - art. 2 pkt 5) (operator) oraz art. 2 pkt 7 (przedsiębiorca telekomunikacyjny). Powstaje zatem nieścisłość terminologiczna między powiązanymi ze sobą przepisami. Powstaje zatem pytanie, czy jest to zabieg celowy i jak powinien być rozumiany. Niezbędne jest odniesienie się do tej kwestii.	**Uwaga częściowo uwzględniona** **Przepis zostanie przeredagowany zgodnie z propozycją Prezesa UKE** Porozumienie będzie mogło być zawarte z operatorami zapewniającymi świadczenie usług dla co najmniej 50 000 abonentów. Dla pozostałych przedsiębiorców telekomunikacyjnych Prezes UKE powinien natomiast wydawać rekomendacje dotyczące środków organizacyjnych i technicznych, służących realizacji obowiązku, o którym mowa w art. 8 projektu.
26.	UKE	Art. 10 ust. 2	Art. 10 ust. 2 – przepis powinien dotyczyć operatorów będących stroną porozumienia, a nie stron porozumienia, ponieważ jedną ze stron będzie Prezes UKE.	**Uwaga uwzględniona**
27.	UOKIK	Art. 10 ust. 3	Art. 10 ust. 3 Zgodnie z treścią tego przepisu, operator prawidłowo wykonujący porozumienie nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będącej skutkiem wprowadzonych środków technicznych i organizacyjnych, które będzie stosował przy realizacji obowiązków, o których mowa w art. 8. Konieczne jest podkreślenie, że termin „zwolnienie z odpowiedzialności" ma bardzo szerokie i nieokreślone znaczenie, może też podlegać swobodnej interpretacji przez przedsiębiorców. Wskazane byłoby doprecyzowanie, nawet jeżeli wyłącznie w uzasadnieniu projektu, że chodzi o odpowiedzialność konkretnie	**Uwaga uwzględniona**

			związaną z wykonywaniem czynności, o których mowa w art. 8, tj. odpowiedzialności za blokowanie połączeń głosowych albo ukrywanie identyfikacji numeru wywołującego dla użytkownika końcowego.	
28.	UKE	Art. 10 ust. 4	Art. 10 ust. 4 – w związku z brzmieniem tego przepisu postuluje się wprowadzenie do projektu kary pieniężnej za nieprawidłowe stosowanie środków organizacyjnych i technicznych określonych w zawartym przez operatora porozumieniu, o którym mowa w ust. 1. Niezależnie od powyższego, odesłanie zamieszczone w tym przepisie powinno następować nie do przepisów Prawa telekomunikacyjnego dotyczących kontroli, lecz do rozdziału 2 w dziale X Prawa telekomunikacyjnego, zatytułowanego „Kontrola i postępowanie pokontrolne". Umożliwi to Prezesowi UKE wydawanie zaleceń pokontrolnych.	**Uwagi uwzględnione**
29.	UOKIK	Art. 11	**Art. 11** Co do zasady należy pozytywnie ocenić ideę prowadzenia jawnej listy ostrzeżeń dotyczącej stron internetowych, opisanej w art. 11 projektu. Wątpliwości może jednak przy tym budzić wyłącznie uznaniowe blokowanie witryn przez przedsiębiorców telekomunikacyjnych. Jak wynika z brzmienia art. 11 ust. 6, przedsiębiorca telekomunikacyjny „może" uniemożliwić użytkownikom Internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę. Jego działanie ma zatem charakter wyłącznie fakultatywny i podejmuje on arbitralną decyzję o zastosowaniu blokady. Lista prowadzona przez CSIRT NASK ma zatem jedynie wymiar informacyjny. Wydaje się, że z uwagi na to, że omawiane witryny znajdujące się na liście stanowią poważne zagrożenie dla użytkowników Internetu, podszywając się m.in. pod strony banków lub instytucji płatniczych, zasadne byłoby wprowadzenie obowiązku ich blokowania lub w inny sposób doprecyzowanie sytuacji, w której powinno dojść do zablokowania takiej strony. Nawet jeśli generalną praktyką przedsiębiorców byłoby stosowanie blokady, to trudno znaleźć uzasadnienie dla pozostawienia tego typu decyzji wyłącznie	**Uwaga uwzględniona poprzez dodanie obligatoryjnego wymogu blokowania stron**

			w gestii przedsiębiorców, którzy mogą kierować się w jej podjęciu np. kosztami z tym związanymi. Dodatkowo, analogicznie do uwagi dotyczącej art. 4 ust. 2 projektu, wydaje się, że zasadne byłoby każdorazowe pisemne uzasadnianie przez CSIRT NASK odmowy wpisania strony internetowej listę, jeśli zgłoszenie pochodziło od Prezesa UOKiK. Liczne postępowania Prezesa UOKiK dotyczą działań opisanych w art. 11, posiada on też wiedzę na temat rynku telekomunikacyjnego i e-commerce, sytuacji i zwyczajów konsumentów oraz funkcjonowania podmiotów inicjujących aktywności takie jak CLI spoofing. Aktualna pozostaje przy tym argumentacja podniesiona w uwadze do art. 4 ust. 2 projektu.	
30.	DC UKNF	Art. 11 ust. 1, 4 i 6	Zgodnie z art. 11 ust. 6 projektu ustawy, przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom Internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1. Przepis ten sformułowany jest w formie uprawnienia, a nie obowiązku blokowania stron wpisanych na listę ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników Internetu. Uwzględniając skalę wykorzystywania omawianych stron do wyłudzeń oraz negatywne skutki, jakie wiąże się z ich funkcjonowaniem dla obywateli RP i podmiotów gospodarczych (w tym ich straty finansowe mogące sięgać dziesiątków milionów złotych) w ocenie UKNF zasadne jest nałożenie na przedsiębiorców telekomunikacyjnych obowiązku blokowania dostępu do omawianych stron. W związku z powyższym sugerujemy rozważenie zmiany treści art. 11 ust. 6 projektu ustawy i zastąpienie sformułowania „może uniemożliwić” terminem „uniemożliwia”. Dodatkowo, projektowany art. 11 ust. 1 odnosi się do możliwości zawarcia porozumienia w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, o których mowa powyżej. Ustęp 4 wymienionego przepisu wskazuje przy tym,	**Uwaga uwzględniona poprzez dodanie obligatoryjnego wymogu blokowania stron** **Uwaga nieuwzględniona w zakresie nałożenia obowiązku przystąpienia do porozumienia** W ocenie projektodawcy należy pozostawić przedsiębiorcom telekomunikacyjnym swobodę wyboru sposobu realizacji obowiązków związanych z przeciwdziałaniem nadużyć telekomunikacyjnych. Będą oni mogli wybrać inny sposób realizacji nałożonych na nich obowiązków, ale będzie się to wiązało z brakiem domniemania, że obowiązki są prawidłowo realizowane.

			że stronami takiego porozumienia są m.in. „przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni". W kontekście omawianego sformułowania powstaje wątpliwość, czy zawarcie porozumienia pozostaje dla przedsiębiorców telekomunikacyjnych dobrowolne, czy też obowiązkowe. W ocenie UKNF zasadne jest doprecyzowanie omawianego przepisu, aby z jego treści wynikał obowiązek zawarcia omawianego porozumienia przez przedsiębiorców telekomunikacyjnych. Obligatoryjny charakter przystąpienia do omawianego porozumienia pozytywnie przyczyniłby się do skuteczności projektowanych w niniejszym przepisie rozwiązań. Przedmiotowe porozumienie reguluje bowiem m.in. zasady zgłaszania domen internetowych, a zasadnym jest udział w tym procesie również przedsiębiorców telekomunikacyjnych – dzięki porozumieniu i ustalonym w nim wiążącym zasadom współpracy mógłby on być zaś bardziej efektywny.	
31.	DC UKNF	Art. 11 ust. 1	W celu zapewnienia, że ochronie podlegać będą również przypadki, w których rozporządzenia dokonuje np. pracownik przedsiębiorcy dysponujący jego majątkiem (przykładowo atak na księgowego spółki metodą „podszycia się" pod członka zarządu) sugerujemy usunięcie ze sformułowania „doprowadzającymi użytkowników Internetu do niekorzystnego rozporządzenia ich majątkiem" słowa „ich". Jednocześnie, dla zachowania spójności ze zdaniem pierwszym (które odnosi się do majątku), sugerujemy rozważenie zastąpienia w zdaniu drugim omawianego przepisu terminu „środków finansowych" terminem „majątku" – jest to pojęcie szersze i mogą zdarzyć się ataki, w których wyłudzeniu podlegać będzie towar czy wykonanie usługi, a nie środki finansowe. Proponowane zmiany pozostają również zgodne z zaproponowaną w projekcie definicją CLI spoofing.	**Uwaga nieuwzględniona** Mechanizm proponowany w ustawie funkcjonuje obecnie – jest nim lista ostrzeżeń przed niebezpiecznymi stronami prowadzona przez NASK-PIB[1].
32.	UKE	Art. 11 ust. 2	Art. 11 ust. 2 – przepis wymaga przeredagowania, ponieważ przy obecnym brzmieniu niezrozumiały jest fragment „oraz uniemożliwienia dostępu do tych stron".	**Uwaga wyjaśniona w związku z uwzględnieniem uwagi** Polskiego Towarzystwa Informatycznego

[1] https://cert.pl/posts/2020/03/ostrzezenia_phishing/

				Izba Rzeczoznawców usunięty został przepis, którego uwaga dotyczy.
33.	UKE	Art. 11 ust. 6	Art. 11 ust. 6 – w związku z treścią tego ustępu proponuje się dodać do projektu przepis stanowiący, że zawarcie przez przedsiębiorcę telekomunikacyjnego porozumienia, o którym mowa w art. 11 ust. 1, rodzi obowiązek uniemożliwienia użytkownikom internetu dostępu do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę ostrzeżeń dotyczących domen internetowych.	**Uwaga uwzględniona poprzez dodanie obligatoryjnego wymogu blokowania stron**
34.	UKE	Art. 13	Art. 13 – proponuje się rozważyć wprowadzenie do projektowanej ustawy kary pieniężnej za naruszenie tego przepisu, co powinno przyczynić się do zapewnienia przestrzegania obowiązków, o których w nim mowa. Ponadto w ust. 2 nie wskazano terminu początkowego przechowywania danych o usługach telekomunikacyjnych, które nie zostały przez przedsiębiorcę telekomunikacyjnego wykonane w związku z blokowaniem smishingu (powinno się go liczyć od dnia, w którym usługa miała być wykonana).	**Uwaga uwzględniona w zakresie wskazania dnia, od którego liczony jest okres 12-miesięczny** **Uwaga nieuwzględniona w zakresie kary** Wprowadzenie kary pieniężnej za naruszenie przepisu art. 13 byłoby nieproporcjonalne względem obowiązków nałożonych na przedsiębiorcę. Analogicznie do przepisów Prawa telekomunikacyjnego, zgodnie z którymi obowiązek rejestracji danych o wykonanych usługach telekomunikacyjnych, wyrażony w art. 168 PT nie podlega karze pieniężnej, przedsiębiorca musi zapewnić rozliczalność przed organami i abonentem. W przypadku projektowanej ustawy

				odnosi się to do sytuacji składania reklamacji względem niedostarczonej usługi. Ponadto, należy wskazać, że przetwarzanie bez podstawy prawnej danych, o których mowa w art. 13, stanowiących dane osobowe, będzie podlegało sankcjom przewidzianym w RODO.
35.	UODO	Art. 13 ust. 2	Wątpliwości organu właściwego w sprawie ochrony danych osobowych dyspozycja art. 13 ust. 2 projektu. Komentowany przepis obliguje przedsiębiorcę telekomunikacyjnego do przechowywania (rejestracji) danych o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązków i uprawnień ustawowych2, przez okres co najmniej 12 miesięcy. Tym samym przepis ten, w zaproponowanym brzmieniu, nie określa w sposób jednoznaczny po jakim maksymalnym czasie przedsiębiorca telekomunikacyjny jest obowiązany usunąć zarejestrowane dane o niewykonanych usługach telekomunikacyjnych. Co za tym idzie dane te mogłyby być przechowywane przez przedsiębiorcę telekomunikacyjnego przez okres dłuższy niż jest to niezbędne do celów, dla realizacji których dane te zostały zebrane. Tak więc przyjęte w projekcie brzmienie art. 13 ust. 2 może naruszać zasadę ograniczenia przechowywania statuowaną w art. 5 ust. 1 lit. e 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	**Uwaga uwzględniona** Proponuje się zmianę wyrażenia „co najmniej przez okres 12 miesięcy” na „przez okres 12 miesięcy”

[2] Wskazanych w art. 4 ust. 6 i art. 7 projektu.

			95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1, z późn. zm.)3, powoływanego dalej z zastosowaniem skrótu „rozporządzenie 2016/679”.	
36.	UKE	Art. 14 ust. 3 pkt 2	Art. 14 ust. 3 pkt 2 – w przepisie tym brakuje odesłania do art. 8.	**Uwaga uwzględniona**
37.	UODO	Art. 14 ust. 4	Rozważenia wymaga także konstrukcja prawna zaproponowana w art. 14 ust. 4 projektu. O ile bowiem nie budzi wątpliwości uprawnienie Projektodawcy do ograniczenia – przewidzianych w art. 14 i art. 15 rozporządzenia 2016/679 – praw osoby, której dane dotyczą, ze względu na konieczność identyfikacji, zapobiegania i zwalczania przestępstw, to nie można pominąć, iż art. 23 ust. 1 lit. c i d rozporządzenia 2016/679 dopuszcza jedynie ograniczenie4 – ze względu na bezpieczeństwo publiczne i zapobieganie przestępczości – praw przewidzianych w art. 12–22 rozporządzenia 2016/679, nie zaś ich całkowite wyłączenie.	**Uwaga uwzględniona** Proponuje się rozszerzenie uzasadnienia, odnosząc się do relewantnych postanowień wskazanych w art. 23 ust. 2 RODO. Projekt ustawy zakłada ograniczenie stosowania art. 15 wyłącznie w zakresie, jaki jest niezbędny dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego (po zmianie przepisu w wyniku uwzględnienia uwag rynku – w celu identyfikacji, zapobiegania oraz zwalczania nadużyć). Wyłączenie art. 14 RODO zostało usunięte – w zamian przedsiębiorca telekomunikacyjny będzie mógł podać informacje wymagane przez art. 14 rozporządzenia na swojej stronie internetowej lub przez

[3] W myśl art. 5 ust. 1 lit. e rozporządzenia 2016/679 „Dane osobowe muszą być […] przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane…

[4] O ile nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym.

				umieszczenie stosownych informacji w miejscach widocznych w siedzibie lub miejscu działania administratora danych osobowych, w zakresie w jakim dotyczy to danych osobowych pozyskanych w ramach identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.
38.	UKE	Art. 15 ust. 4	Art. 15 ust. 4 – odesłanie do przepisów Prawa telekomunikacyjnego trzeba rozszerzyć o ust. 1^1 w art. 209.	**Uwaga wyjaśniona:** Zmieniono brzmienie ust. 4 i obecnie nie zawiera on odesłania do przepisów PT. Przepis otrzymał brzmienie: 4. Kara, o której mowa w ust. 1-3, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.
39.	UKE	Art. 15 ust. 5	Art. 15 ust. 5 – po pierwsze, wskazać należy, że kara pieniężna w wysokości do jednokrotności przeciętnego wynagrodzenia wydaje się karą niską, która może nie spełnić funkcji prewencyjnej i represyjnej kary. Po drugie, w ust. 5 występuje błędne odesłanie do art. 11 ust. 2.	**Uwaga częściowo uwzględniona** Zmieniona została wysokość kary, jaka może zostać nałożona przez Prezesa UKE na kierującego przedsiębiorstwem – do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.

				Zmieniona została także sama konstrukcja przepisu, który otrzymał brzmienie: 5. Niezależnie od kar pieniężnych, o których mowa w ust. 1 i 2, Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.
40.	DC UKNF	Art. 16 ust. 1	Przepis posługuje się pojęciem korzyści majątkowej, podczas gdy nie można wykluczyć działania sprawców tego rodzaju przestępstw w celu osiągnięcia korzyści osobistej. Może mieć to w szczególności znaczenie przy atakach z wykorzystaniem spoofingu na instytucje publiczne. Kategoria korzyści osobistych znana jest przy tym w prawie karnym i odnosi się do niej np. art. 228 k.k. Sugerujemy rozważenie zmiany omawianego przepisu poprzez posłużenie się zwrotem, „Art. 16. 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody dopuszcza się: (…)”	**Uwaga uwzględniona** Przepis zostanie poprawiony zgodnie z propozycją.
41.	UKE	Art. 20	Art. 20 – z literalnego brzmienia tego przepisu intertemporalnego wynika, że chodzi w nim wyłącznie o moment wydania decyzji o nałożeniu kary. Przepis ten wymaga przeredagowania ponieważ	**Uwaga wyjaśniona** Intencja projektodawcy zostanie uwypuklona w uzasadnieniu.

			wydaje się, że intencją projektodawcy jest nienakładanie kar za naruszenia dokonane we wskazanych w tym przepisie okresach.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (UD402)

Lp.	Instytucja	Jednostka redakcyjna	Treść uwagi	Odniesienie
1.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Uwaga ogólna	I. [UWAGA OGÓLNA] (1.) Izba od wielu lat konsekwentnie popiera wszelkie słuszne inicjatywy mające na celu zwalczanie nadużyć na rynku telekomunikacyjnym (w tym zakresie zostały przedstawione przynajmniej dwukrotnie rozwiązania legislacyjne służące zwalczaniu nadużyć). (2.) Aby jednak takie działania były efektywne, konsekwentnie wnosimy o precyzyjne uregulowanie obowiązków na tym polu. Wszelkie obowiązki powinny być określone w sposób maksymalnie precyzyjny i wyczerpujący.	**Uwaga wyjaśniona** Przepisy projektu ustawy są adekwatne do obecnej sytuacji.
2.	Unia Metropolii Polskich	Uwaga ogólna	Nieprawidłowo ustalony zakres projektu w stosunku do jego tytułu oraz przeznaczenia. Jeżeli projekt ma dotyczyć zwalczania nadużyć powinien nakładać obowiązki na podmioty dokonujące takich nadużyć lub zakazywać ich im dokonywania takich czynności. Obowiązku dotyczące podmiotów publicznych, które mogą stanowić „ochronę” przed nadużyciami powinny być zamieszczone w przepisach stanowiących podstawę dla działalności jst w zakresie informatyzacji lub cyberbezpieczeństwa np. w ustawie o informatyzacji ale najlepiej w ustawie KSC. Nie należy dążyć do dalszego rozchwiania systemu i tworzenia obowiązków dla podmiotów publicznych w różnych ustawach szczegółowych, które *de facto* dotyczą ochrony bezpieczeństwa informacyjnego.	**Uwaga wyjaśniona** Projektowany akt prawny znajduje się na styku dziedziny prawa telekomunikacyjnego i wyodrębniającego się materialnego prawa administracyjnego z zakresu cyberbezpieczeństwa. Z tego względu, a także ze względu na doniosłość materii regulowanej, zasadne jest aby przepisy te znalazły się w odrębnym akcie prawnym. Odpowiednie przepisy dotyczące nadużyć telekomunikacyjnych zostaną usunięte (lub przeniesione) z ustawy - Prawo komunikacji elektronicznej na kolejnym etapie prac legislacyjnych (zgodnie z projektem z 5 maja 2022 r. przepisem do usunięcia jest m.in. art. 173 PKE). Art. 97 ust. 2 Europejskiego Kodeksu Łączności Elektronicznej odnosi się do obowiązku zapewnienia przez państwo członkowskie, aby

				właściwy (właściwe organ (organy) mógł (mogły) wymagać od przedsiębiorców komunikacji elektronicznej zablokowania incydentalnego dostępu do numerów lub usług, gdy jest to związane z oszustwem lub nadużyciem. Wdrożenie rzeczonego przepisu EKŁE stanowi projektowany art. 343 PKE, który również zostanie przeniesiony do projektowanej ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, w zakresie w jakim kompetencje Prezesa Urzędu Komunikacji Elektronicznej są wykonywane w „uzasadnione ochroną użytkowników końcowych przed nadużyciami telekomunikacyjnymi”.
3.	Unia Metropolii Polskich	Uwaga ogólna	Ustawa nakłada pewne zadania na przedsiębiorców telekomunikacyjnych i w przypadku CLI spoofing i jest zrozumiałe. Są też określone obowiązki nakładane na operatorów poczty e-mail. Jednakże projektodawca pozostawia poza zakresem regulacji niezagospodarowany obszar komunikacji elektronicznej w postaci różnego rodzaju komunikatorów. Jest to tym bardziej dziwne, że w projekcie zastosowano szeroką definicja „usług komunikacji interpersonalnej” a jednocześnie w dalszej części nie ma słowa o komunikatorach i formach świadczących te usługi. Młode pokolenie nie korzysta z SMSów. Tymi kanałami też posługują się coraz częściej różne instytucje.	**Uwaga wyjaśniona** Ustawa posługuje się szerokim pojęciem usług komunikacji interpersonalnej, gdyż zawiera zarówno przepisy odnoszące się do zwalczania nadużyć w telekomunikacji, jak i te dotyczące poczty internetowej (usługi komunikacji elektronicznej). Projektowana ustawa w szczególności zawiera szereg obowiązków i uprawnień po stronie przedsiębiorców telekomunikacyjnych. Z tej perspektywy wskazane przez zgłaszającego uwagę rozwiązania wiązałoby się z koniecznością analizowania treści komunikatów oraz zestawiania ich z innymi informacjami. Ponadto część komunikacji elektronicznej wykorzystuje szyfrowania end-to-end, więc ich wykrywanie jest niemożliwe.

			Należy zadać pytanie, dlaczego ww. regulacja nie dotyczy tego obszaru.	
4.	Polska Izba Informatyki i Telekomunikacji	Uwaga ogólna	Obecnie obowiązujące przepisy prawa, które jako zasadę przyjmują obowiązek zestawiania połączeń a możliwość ich blokowania traktują jako wyjątki dopuszczalne wyłącznie w przypadkach wskazanych w ustawie, wręcz utrudniają przedsiębiorcom telekomunikacyjnym zwalczanie nadużyć telekomunikacyjnych, zmuszając do dokonywania wyborów pomiędzy walką z nadużyciami telekomunikacyjnymi a bezpieczeństwem regulacyjnym. Pomimo ograniczeń regulacyjnych wynikających z obowiązujących przepisów prawa przedsiębiorcy telekomunikacyjni stanowią pierwszą (i najczęściej niestety ostatnią) linię obrony przed przeróżnymi działaniami przestępczymi przyjmującymi postać nadużyć telekomunikacyjnych. Jednym z podstawowych celów przedsiębiorców telekomunikacyjnych w zakresie zwalczania nadużyć jest ochrona klientów. Przedsiębiorcy telekomunikacyjni podejmowali i podejmują szereg proporcjonalnych działań (zarówno technicznych i organizacyjnych) mających na celu przeciwdziałanie nadużyciom oraz zapewnienie w jak największym stopniu bezpieczeństwa usług świadczonych abonentom. Zgromadzone przez przedsiębiorców telekomunikacyjnych doświadczenia pozwalają stwierdzić, że projektowana ustawa wymaga dalszych prac i zmian zgodnych z postulatami wyrażonymi w niniejszym stanowisku, gdyż w obecnym kształcie projektowane przepisy nie do końca prawidłowo rozkładają ciężar odpowiedzialności za walkę z nadużyciami.	**Uwaga wyjaśniona** W projekcie zostały wprowadzone przepisy karne. Poprzez nałożenie obowiązków z zakresu przeciwdziałania i zwalczania nadużyć w komunikacji elektronicznej przedsiębiorcy telekomunikacyjni uzyskają również niezbędne kompetencje do podejmowania działań w tym zakresie.

			Nadużycia z wykorzystaniem sieci i usług telekomunikacyjnych bez wątpienia są zjawiskiem na tyle społecznie szkodliwym, że wymagają kompleksowych i przemyślanych przepisów, które wyposażałyby przede wszystkim organy, instytucje i służby państwa w narzędzia niezbędne do zwalczania tego zjawiska, gdyż to państwo, a nie przedsiębiorcy, jest odpowiedzialne za walkę z przestępczością, a tym w wielu przypadkach są nadużycia z wykorzystaniem sieci i usług telekomunikacyjnych. Jednoczenie takie przepisy powinny umożliwiać przedsiębiorcom telekomunikacyjnym (operatorom i dostawcom usług) podejmowanie działań mających na celu zwalczanie nadużyć, w ramach obsługi ruchu i świadczenia usług telekomunikacyjnych. Przedsiębiorcy telekomunikacyjni mogą wspierać Państwo w walce z tym procederem, w ramach dostępnych możliwości technicznych uwzględniających obecny etap rozwoju sieci i usług telekomunikacyjnych, ale nie mogą Państwa w tym zakresie zastąpić. Natomiast projektowana ustawa składa ciężar ochrony obywateli przed nadużyciami na barki przedsiębiorców telekomunikacyjnych. Nie można również zapominać o tym, że implementacja rozwiązań proponowanych w projektowanej ustawie będzie stanowiła dla przedsiębiorców telekomunikacyjnych kolejne, znaczące koszty oraz wysiłek organizacyjny, kumulujący się z kosztami i nakładem pracy, jaki przedsiębiorcy telekomunikacyjni będą zmuszeni włożyć we wdrożenie wymagań wynikających z projektu ustawy – Prawo komunikacji elektronicznej (oraz ustawy ją wprowadzającej) oraz projektowanej ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Nie sposób nie zauważyć, że w chwili obecnej Minister	

			Cyfryzacji prowadzi prace legislacyjne nad projektami trzech ustaw, z których każda będzie miała istotny wpływ na funkcjonowanie rynku telekomunikacyjnego i każda będzie oznaczać dla przedsiębiorców telekomunikacyjnych nowe obowiązki oraz znaczne koszty zarówno dostosowawcze jak i utrzymaniowe. Operatorzy budują sieci i świadczą usługi telekomunikacyjne na podstawie standardów, norm, wytycznych i zasad, które są ustalane oraz koordynowane na poziomie międzynarodowym – ITU, ETSI, 3GPP. Stosując powszechnie uznane, międzynarodowe standardy techniczne dochowujemy najwyższej możliwej staranności, zapewniając naszym klientom interoperacyjne, niezawodne i bezpieczne usługi telekomunikacyjne o zasięgu globalnym. Istniejące standardy techniczne dla sieci telekomunikacyjnych nie przewidują gotowych rozwiązań i narzędzi, które można by wykorzystać do identyfikowania połączeń telekomunikacyjnych, które są zestawiane zgodnie z przyjętymi normami technicznymi, a które są inicjowane przez przestępców dla osiągnięcia niezgodnych z prawem celów. Fakt, że przestępcy wykorzystują sieci i usługi telekomunikacyjne do popełniania przestępstw można porównać do sytuacji popełnienia przestępstwa z użyciem noża – nie jest winą ani odpowiedzialnością producenta i sprzedawcy noża, że przestępca wykorzystał nóż do złamania prawa. Procesy zwalczania nadużyć muszą być kształtowane przede wszystkim z myślą o efektywnym ściganiu i karaniu przestępców przez powołane do tego służby i organy Państwa, jednocześnie dając przedsiębiorcom telekomunikacyjnym możliwość	

			podejmowania działań anty-fraudowych, mieszczących się w zakresie posiadanych przez przedsiębiorców możliwości technicznych i organizacyjnych. Wysiłki przedsiębiorców telekomunikacyjnych na rzecz ograniczenia zjawiska nadużyć w komunikacji elektronicznej nie przyniosą oczekiwanych rezultatów tak długo, jak długo sprawcy tych naruszeń będą pozostawali nieustaleni i bezkarni. Proceder nadużyć kwitnie, gdyż jest postrzegany przez przestępców jako bezpieczne źródło nielegalnego zarobku, gdyż możliwość zagarnięcia znacznych pieniędzy idzie w parze ze znikomym ryzykiem wykrycia i ukarania. Podsumowując tę część pragniemy podkreślić, że: 1. zwalczanie nadużyć telekomunikacyjnych, przynajmniej tych, które są przestępstwami w rozumienia prawa karnego, jest i powinno być obowiązkiem i odpowiedzialnością powołanych do ścigania przestępstw służb i organów Państwa; 2. sprawcy, którzy dopuszczają się nadużyć, powinni być wykrywani przez powołane do tego służby i organy, a następnie stawiani przed wymiarem sprawiedliwości; 3. przedsiębiorcy telekomunikacyjni powinni mieć prawo do podejmowania proporcjonalnych działań mających na celu identyfikowanie, zapobieganie i zwalczanie nadużyć telekomunikacyjnych, wspierając w ten sposób wysiłki służb i organów Państwa na rzecz ograniczenia zjawiska nadużyć w komunikacji elektronicznej.	
5.	Polska Izba Informatyki i Telekomunikacji	Uwaga ogólna	II. Prawa, obowiązki i kary Zasadą na gruncie projektowanej ustawy powinno być uprawnienie dla przedsiębiorców telekomunikacyjnych	**Uwaga nieuwzględniona** Aby skutecznie walczyć z nadużyciami w komunikacji elektronicznej powinien zostać

			do zwalczania nadużyć w komunikacji elektronicznej. Wyjątki od tej zasady powinny dotyczyć tylko tych przypadków, w których można precyzyjnie określić zakres czynności, jakie mają być powinnością przedsiębiorcy telekomunikacyjnego – w tych przypadkach w grę może wchodzić obowiązek, ale bez konieczności obwarowywania jego wykonania ryzykiem kary pieniężnej. Każdy większy przedsiębiorca telekomunikacyjny posiada w swoich strukturach komórki anty-fraudowe, zatrudnia ekspertów od zwalczania nadużyć, utrzymuje i rozwija procedury i narzędzia IT wspierające ekspertów w detekcji i zwalczaniu nadużyć telekomunikacyjnych. Utrzymywanie i rozwijanie zasobów kadrowych i technicznych to wymierny koszt, który każdy operator traktuje jako koszt konieczny, bez którego straty ponoszone przez przedsiębiorców telekomunikacyjnych i abonentów byłby jeszcze większe. Straty ponoszone przez przedsiębiorców telekomunikacyjnych mają charakter zarówno wizerunkowy jak i majątkowy, gdyż wiele ze scenariuszy nadużyciowych jest wprost wymierzonych w przedsiębiorców telekomunikacyjnych albo szkodzi przedsiębiorcom telekomunikacyjnym niejako w ramach efektów ubocznych działań przestępców. Zresztą jest to odzwierciedlone w samej definicji „nadużycia w komunikacji elektronicznej”, gdzie jedną z przesłanek jest szkoda przedsiębiorcy telekomunikacyjnego. Na poziomie hurtowego rynku telekomunikacyjnego operatorzy rozliczają się wzajemnie za terminowany ruch, co oznacza, że operator abonenta inicjującego połączenie albo wysyłającego wiadomość SMS płaci określoną stawkę hurtową operatorowi abonenta odbierającego połączenie albo SMS.	nałożony obowiązek prawny (obowiązki) na przedsiębiorców telekomunikacyjnych. W przypadku przyznania uprawnienia przedsiębiorca telekomunikacyjny mógłby, ale nie musiałby podejmować działań mających na celu zwalczanie nadużyć.

			Dodatkowy poziom hurtowych rozliczeń międzyoperatorskich pojawia się przy połączeniach międzynarodowych i realizowanych w roamingu międzynarodowym. Konieczność płacenia za zakańczanie połączeń w relacjach hurtowych oznacza, że nadużycia telekomunikacyjne, generujące istotne ilości ruchu, dla operatorów oznaczają niechciane i nieuzasadnione koszty, które są liczone w setkach tysięcy złotych miesięcznie. Jednocześnie na poziomie detalicznym operatorzy muszą i chcą walczyć z nadużyciami telekomunikacyjnymi w trosce o bezpieczeństwo swoich klientów, gdyż niezwykle konkurencyjny, polski rynek telekomunikacyjny nie pozostawia miejsca do działania dla dostawców usług, którzy nie są gotowi zapewnić swoim abonentom najwyższych możliwych standardów bezpieczeństwa. Wszystko to powoduje, że zwalczanie nadużyć w komunikacji elektronicznej jest w interesie zarówno przedsiębiorców telekomunikacyjnych jak i abonentów korzystających z tych usług. Z tego też względu przedsiębiorcy telekomunikacyjni nie potrzebują dodatkowej motywacji do walki z nadużyciami, w szczególności w postaci obowiązków pod groźbą kary, potrzebują natomiast wsparcia ze strony organów Państwa i regulatora rynku, w szczególności w postaci przepisów prawa, które zamiast krępować ręce dadzą przedsiębiorcom telekomunikacyjnym uprawienia (nie obowiązki) niezbędne do skutecznej walki z nadużyciami. Podsumowując wątek dotyczący uprawnień, obowiązków i kar: 1. sprawcy nadużyć w komunikacji elektronicznej powinni ponosić odpowiedzialność za swoje nielegalne działania, w związku z czym konieczne jest utrzymanie w	

			projekcie ustawy przepisów, które przewidują odpowiedzialność karną za naruszenie zakazu nadużyć (art. 16 projektu ustawy) oraz dają Prezesowi UKE możliwość nałożenia kary pieniężnej na sprawcę naruszenia (art. 15 ust. 1 projektu ustawy); 2. projektowana ustawa jako zasadę powinna przewidywać uprawnienie dla przedsiębiorców telekomunikacyjnych do zwalczania nadużyć telekomunikacyjnych; 3. reżim obowiązku dla przedsiębiorców telekomunikacyjnych można sobie wyobrazić jako wyjątek od zasady (jaką powinno być uprawienie) tylko dla tych przypadków, w których da się precyzyjnie opisać zakres czynności, które w interesie publicznym powinni wykonać przedsiębiorcy telekomunikacyjni; przykładowo obowiązek może dotyczyć: a. blokowania SMS wpisujących się we wzorzec przekazany przez NASK (art. 4 ust. 6 projektu ustawy); b. blokowania połączeń głosowych inicjowanych z wykorzystaniem numeru wpisanego do wykazu numerów służących wyłącznie do odbierania połączeń głosowych, prowadzonego przez Prezesa UKE (art. 9 ust. 12 projektu ustawy); 4. nie jest konieczne wprowadzanie ryzyka kar pieniężnych za naruszenie obowiązków, które mają ciążyć na przedsiębiorcach telekomunikacyjnych; 5. jeśli jednak w ocenie Projektodawcy takie kary są niezbędne, to powinny one dotyczyć tylko obowiązków wymienionych w punkcie 3 powyżej i powinny mieć	

			charakter fakultatywny (tak jak obecnie w art. 15 ust. 2 projektu ustawy); 6. jeśli Projektodawca chce objąć obowiązkiem i ryzykiem kar obszary inne niż wymienione w punkcie 3 powyżej (np. CLI spoofing – art. 8 w zw. z art. 15 ust. 2 pkt 2) projektu ustawy), to dla każdego takiego obszaru konieczne jest wyznaczenie organu państwa, który będzie identyfikował konkretny ruch będący nadużyciem i przekazywał taką informację przedsiębiorcom telekomunikacyjnym celem zablokowania tego konkretnego ruchu (analogicznie do zaprojektowanego mechanizmu identyfikowania smishingowych wiadomości SMS przez NASK); tak zidentyfikowany przez organ państwa ruch przedsiębiorcy telekomunikacyjni mogą blokować w reżimie obowiązku; Realizacja powyższych postulatów będzie wymagała przeredagowania szeregu przepisów projektowanej ustawy, które obecnie mówią o obowiązku przedsiębiorcy telekomunikacyjnego, tak, aby obowiązek zastąpić uprawnieniem (możliwością). W szczególności: • art. 3 ust. 2 projektu ustawy powinien uzyskać następujące brzmienie: Przedsiębiorca telekomunikacyjny może podejmować proporcjonalne działania mające na celu zapobieganie nadużyciom komunikacji elektronicznej i ich zwalczanie. • art. 8 projektu ustawy powinien uzyskać następujące brzmienie: W przypadku uzasadnionego podejrzenia wystąpienia CLI spoofingu przedsiębiorca telekomunikacyjny może	

			zablokować takie połączenie albo wyeliminować prezentację identyfikacji numeru wywołującego.	
6.	Polska Izba Informatyki i Telekomunikacji	Uwaga ogólna	**Relacja projektowanej ustawy do przepisów o nadużyciach telekomunikacyjnych w projekcie ustawy – Prawo komunikacji elektronicznej** Nie sposób nie zauważyć, że zarówno konstrukcja jak i brzmienie niektórych przepisów projektowanej ustawy jest wzorowana albo jest powtórzeniem przepisów o nadużyciach telekomunikacyjnych, obecnych w projektowanej ustawie – Prawo komunikacji elektronicznej. Zakładamy, że Projektodawca przedkładając projektowaną ustawę *o zwalczaniu nadużyć w komunikacji elektronicznej* chciał, aby problematyka ta miała dedykowaną ustawę, w związku z czym konieczne jest usunięcie przepisów dotyczących nadużyć telekomunikacyjnych z projektu ustawy – Prawo komunikacji elektronicznej, tak, aby uniknąć konfliktu pomiędzy przepisami obu tych ustaw. Z projektu ustawy – Prawo komunikacji elektronicznej usunąć należy następujące przepisy: • art. 2 pkt 26) projektu PKE (definicja nadużyć telekomunikacyjnych); • art. 173 projektu PKE (określający prawa i obowiązki w zakresie zwalczania nadużyć telekomunikacyjnych); • art. 343 ust. 1 projektu PKE (w zakresie, w jakim przepis ten dotyczy wydawania przez Prezesa UKE decyzji dotyczących nadużyć telekomunikacyjnych);	**Uwaga częściowo uwzględniona** w zakresie projektowanych przepisów ustawy - Prawo komunikacji elektronicznej: - art. 173 zostanie usunięty; - art. 343 w zakresie w jakim dotyczy kompetencji Prezesa Urzędu Komunikacji Elektronicznej związanych z ochroną użytkowników końcowych przed nadużyciami telekomunikacyjnymi (a nie innymi nadużyciami związanymi z wykorzystaniem sieci), zostanie przeniesiony do projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej; - w zakresie art. 171 i art. 211, użyte tam określenie nadużyć telekomunikacyjnych należy odczytywać uwzględniając przepisy ustawy o nadużyciach w komunikacji elektronicznej. Projekt ustawy - Prawo komunikacji elektronicznej jest właściwym miejscem jako ustawa holistycznie odnosząca się do zagadnień umowy o połączeniu sieci oraz obowiązków regulacyjnych sensu stricto.

			• art. 441 ust. 2 pkt 4) i 5) projektu PKE (przepisy przewidujące możliwość nałożenia kary w kontekście nadużyć telekomunikacyjnych). Jednocześnie dalszych analiz wymaga to, czy z uwagi na relację obu ustaw usunięcia albo zmian wymagają następujące przepisy projektu ustawy – Prawo komunikacji elektronicznej: • art. 171 ust. 1 pkt 9) projektu PKE (przepis stanowiący, że jednym z elementów umowy o dostępie w zakresie połączenia sieci ma być opis działań podejmowanych w związku z przypadkami nadużycia telekomunikacyjnego); • art. 211 ust. 4 projektu PKE (odnoszący się do nadużyć telekomunikacyjnych w kontekście decyzji SMP).	
7.	Polska Izba Komunikacji Elektronicznej	Uwaga ogólna	**Uwagi ogólne** Szczegółowa analiza projektu ustawy, nie tylko pod względem legislacyjnym, ale również pod względem skuteczności proponowanych rozwiązań w zapobieganiu i zwalczaniu nadużyciom w komunikacji elektronicznej, doprowadziła zrzeszonych w Izbie przedsiębiorców do szeregu wątpliwości. Zdaniem Izby **ustawa w obecnym kształcie nie sprosta rynkowym oczekiwaniom, przede wszystkim ze względu na fakt niedostosowania regulacji do obecnie używanych i ciągle rozwijających się technologii i zabezpieczeń.** Wydaje się, że proponowane rozwiązania nie podążają za realiami rynku, a tym samym nie będą wystarczające do tego, aby wypełnić swoje funkcje. Regulacja nie uwzględnia szeregu nowych i często stosowanych obecnie rozwiązań, przez co pozostaje **niepełna i nieprecyzyjna**. Słowem przykładu	**Uwaga wyjaśniona** Momentem na ewentualne doprecyzowanie, czy uzupełnienie regulacji jest właśnie rządowy proces legislacyjny, w tym m.in. przeprowadzone konsultacje publiczne, w których Izba wzięła udział. Szczegółowe odniesienie są zawarte przy konkretnych uwagach.

			można wskazać na kwestie nieuwzględnienia w przepisach dot. CLI spoofing zjawisk związanych z podmianą numeru abonenta (m.in. fraudów na rozliczeniach międzyoperatorskich). W dalszej mierze należy wskazać, że wątpliwości Izby potęgują **liczne błędy legislacyjne w przepisach projektu**. W szczególności należałoby podkreślić wśród nich szereg przepisów o niskiej precyzji, które dla swojej skuteczności wymagają dopracowania (np. art. 3 ust. 1 pkt 3 i zawarte w nim pojęcie CLI spoofing, błędne pojęcie „nieświadomego rozporządzenia majątkiem", czy zawężające zastosowanie „podszywania się" pod inny podmiot). Ponadto w niektórych przepisach pojawiają się sprzeczności przyjętej siatki pojęciowej (np. zamienne korzystanie z pojęcia „nadawcy" i „osoby inicjującej"). Jak wspomniano powyżej, ustawa tego rodzaju – wprowadzająca przepisy związane z wysoce technicznymi kwestiami i pojęciami, a także przepisy przewidujące odpowiedzialność karną i administracyjną, powinna być **całkowicie dopracowana** również pod względem legislacyjnym i redakcyjnym. Stąd też, Izba postuluje, aby projekt ustawy został ponownie szczegółowo przepracowany, a następnie uzupełniony i doprecyzowany. Ustawa w obecnym brzmieniu z dużym prawdopodobieństwem nie będzie właściwie stosowana. Wywoła natomiast szereg nieporozumień i sporów.	

8.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Uwaga ogólna	Uwaga ogólna W USTAWIE z dnia 7 października 1999 r. o języku polskim (Dz. U. z 2021 r. poz. 672) w **Art. 4. Język polski jest językiem urzędowym: 1) konstytucyjnych organów państwa;** oraz w **Art. 5. 1. Podmioty wykonujące zadania publiczne na terytorium Rzeczypospolitej Polskiej dokonują wszelkich czynności urzędowych oraz składają oświadczenia woli w języku polskim, chyba że przepisy szczególne stanowią inaczej.** Oznacza to, że również teksty uchwalanych ustaw powinny być w języku polskim, z zastrzeżeniem **Art. 11. Przepisy art. 5–10 nie dotyczą: 5) zwyczajowo stosowanej terminologii naukowej i technicznej;** Powyższe zastrzeżenie może być skuteczne jedynie, gdy konieczne do wskazania w treści terminy nie mają odpowiedników w języku polskim. W przypadku treści projektu ustawy (RD402) proponujemy na terminy: • SMS – krótka wiadomość tekstowa, która w języku polskim, zamiast skrótu SMS, może być opisana terminem **esemes** wraz z możliwością jego odmiany (taki termin występuje w słowniku PWN), • smishing – szalbierczy esemes • CLI spoofing – szalbierczy numer dzwoniącego Proponując wprowadzenie terminu **szalbierczy** jednoznacznie wskazujemy na negatywny odbiór takiego esemesa oraz rozmowy z podszywającego się numeru dzwoniącego. Termin ten można też używać przypadku phishingu – szalbierczej strony oraz szalbierczego mejla.	**Uwaga nieuwzględniona** Określenie „szalbierczy” potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, że jest to archaizm. Wyraz ten jest rzadko używany w codziennych dyskursach. Z tego powodu proponuje się pozostawienie pojęcia „smishing”, które jest powszechnie znane i wykorzystywane. Słownik języka polskiego PWN dopuszcza także skrótowiec SMS[1].

[1] https://sjp.pwn.pl/slowniki/SMS.html

			Tekst tej ustawy może przy tej okazji również wprowadzić polską jednoznacznie zrozumiałą terminologię ostrzegania przed nadużyciami w komunikacji elektronicznej.	
9.	R.M. osoba fizyczna	Uwaga ogólna	W ramach ogłoszonego projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402), w ramach konsultacji publicznych, chciałbym zgłosić swoje stanowisko jako osoba fizyczna. Projekt nie przewiduje niezbędnego dla zapewnienia bezpieczeństwa obywateli wprowadzenia rejestru "Do not call". Rejestr ten pozwoliłby na dodanie przez obywateli swojego numeru telefonu do ogólnopolskiej bazy (prowadzonej według mnie przez UKE), a realizujący połączenia telefoniczne z usługami niezamawianymi (co mogłoby też obejmować instytucje chcące wyłudzić dane) musieliby pod groźbą kary weryfikować czy mogą wykonać połączenie z tym numerem. Wśród zapisów Prawa Telekomunikacyjnego (Dz.U.2019.2460 t.j.) znajduje się zapis zabraniający używania urządzeń końcowych i automatycznych systemów wywołujących do celu marketingu bezpośredniego (Art. 172). Niestety, zapis ten nie jest wciąż respektowany przez wiele firm, które realizują szeroko zakrojone kampanie telefoniczne, także z wykorzystaniem automatycznych systemów wywołujących. Często dzieje się to bez udziału człowieka, czasem zaś w sposób mieszany: przełączenie do sprzedawcy następuje po odsłuchaniu automatycznego komunikatu i wciśnięciu konkretnej cyfry na telefonie. Firmy te nieraz odmawiają podania danych rejestrowych, podają fałszywe dane lub w sposób ordynarny kończą rozmowę, jeśli nie przebiega ona po ich myśli (np. odbiorca rozmowy dopytuje się o źródło posiadania numeru telefonu). W Stanach Zjednoczonych oraz innych	**Uwaga wyjaśniona** Zgodnie z obecnie obowiązującymi przepisami Prawa telekomunikacyjnego przedsiębiorcy mają zakaz używania telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego bez zgody abonenta lub użytkownika końcowego. Za naruszenie tego zakazu, zgodnie z ogólną zasadą, grozi administracyjna kara pieniężna w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Ustawa wprowadziła więc generalny zakaz prowadzenia takiej formy marketingu, chyba że zostanie wyrażona zgoda. Rejestr Do Not Call działałby na odwrotnej zasadzie – abonent musiałby wyraźnie stwierdzić, że nie chce otrzymywać takich informacji i wpisać się do rejestru.

			krajach (np. Australia, Nowa Zelandia, Wielka Brytania) stworzono rejestry nazywane ogólnie "Do not call register" (np. dla USA: https://www.donotcall.gov/). Użytkownik końcowy (osoba fizyczna) może zgłosić fakt, że nie życzy sobie telefonów, zaś firmy muszą się pod groźbą dużych kar do tego życzenia dostosować. W Polsce można by użyć do tego ePUAP. Proponuję rozszerzenie w/w projektu ustawy o taką usługę także zmniejszającą ryzyko phishingu.	
10.	Polskie Towarzystwo Informatyczne	**Art. 1 pkt 2)**	**ad Art. 1 pkt 2)** zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej; Propozycja PTI Przyjąć, w całym tekście ustawy, dopuszczony przez słownik PWN termin **esemes** (wraz z jego odmianą rzeczownikową) zamiast angielskiego skrótu SMS (patrz „Uwaga ogólna").	**Uwaga nieuwzględniona** Słownik języka polskiego PWN dopuszcza także skrótowiec SMS[2].
11.	Porozumienie Zielonogórskie	Uwaga ogólna	Ustawa powinna w miarę możliwości obejmować również zwalczanie działań wykonywanych spoza kraju.	**Uwaga wyjaśniona** Ustawa zakłada zwalczanie nadużyć w komunikacji elektronicznej niezależnie od kraju nadawcy.
12.	Polska Wytwórnia Papierów Wartościowych	Uwaga ogólna	**Uwaga ogólna do projektu ustawy** W projekcie ustawy zostały użyte określenia i skróty nieznane powszechnie oraz nieostre, takie jak: „standard SMTP (Simple Mail Transfer Protocol)", „POP3 (Post Office Protocol)", „IMAP4 (Internet Message Access Protocol)", „SPF (Sender Policy Framework)", „DMARC (Domain-based Message Authentication Reporting and Conformance)", „DKIM (DomainKeys Identified Mail)". W związku z powyższym proponujemy rozważenie	**Uwaga wyjaśniona** Określenia te zostały wyjaśnione w uzasadnieniu projektu ustawy.

[2] https://sjp.pwn.pl/slowniki/SMS.html

			umieszczenie ww. skrótów (wraz z ich rozwinięciem i objaśnieniem) w art. 2 projektu ustawy.	
13.	ZTKIG	Uwaga ogólna	**Uwagi ogólne do projektu** Każde działanie dotyczące obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego należy oceniać jako pozytywne. Bezpieczeństwo jest największą wartością człowieka tuż po zapewnieniu potrzeb biologicznych (fizjologicznych) takich jak sen, pożywienie, picie, warunki bytowe, itp. Dlatego przepisy określające prawa i obowiązki związane z bezpieczeństwem powinny stanowić jednoznaczne normy nie pozwalające na ich dowolną interpretację oraz powinny być łatwe do lokalizacji. Aktualnie obowiązuje kilkanaście ustaw określających obowiązki i prawa przedsiębiorców telekomunikacyjnych z zakresu bezpieczeństwa i obronności. Podstawowym aktem prawnym regulującym działalność telekomunikacyjną, jest ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn. Dz. U. z 2021 r. poz. 576 z późn. zm.), zwana dalej prawem telekomunikacyjnym, i tam powinny być określane wszelkie prawa i obowiązki podmiotów wykonujących działalność telekomunikacyjną. W myśl § 2 załącznika do rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. z 2016 r. poz. 283), zwanego dalej rozporządzeniem w sprawie techniki prawodawczej, ustawa powinna wyczerpująco regulować daną dziedzinę spraw, nie pozostawiając poza zakresem swego unormowania istotnych fragmentów tej dziedziny. Niestety niektóre zakresy regulacji objęte projektem ustawy o zwalczaniu nadużyć w komunikacji elektronicznej są zbieżne z obszarami już regulowanymi	**Uwaga wyjaśniona w zakresie zasadności objęcia zagadnień nadużyć w komunikacji elektronicznej w odrębnym akcie prawnym** Ze względu na doniosłość materii nadużyć w komunikacji elektronicznej zasadne jest uregulowanie tych zagadnień w odrębnej ustawie. Znaczna część projektowanych przepisów nie ma swojego odpowiednika w projektowanej ustawie Prawo komunikacji elektronicznej, która jest na zaawansowanym etapie rządowego procesu legislacyjnego. **Uwaga nieuwzględniona w zakresie postulatu finansowania niektórych obowiązków realizowanych przez przedsiębiorców telekomunikacyjnych ze środków budżetu państwa** Opisywany ogólnie obowiązek jest częścią prowadzenia działalności telekomunikacyjnej, która jest działalnością regulowaną.

			w obowiązujących ustawach, co potwierdzają poniżej przytoczone przykłady: a/ art. 178 ust. 1 pkt 2 prawa telekomunikacyjnego uprawnia Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej Prezesem UKE, do nakładania w drodze decyzji administracyjnej na przedsiębiorcę telekomunikacyjnego obowiązku ograniczenia niektórych, publicznie dostępnych usług telekomunikacyjnych. b/ art. 175 c prawa telekomunikacyjnego zobowiązuje przedsiębiorcę telekomunikacyjnego do podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym: 1) eliminację przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług; 2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług. Ponadto, ustawy określające prawa i obowiązki uprawnionych podmiotów, o których mowa w art. 179 ust. 3 pkt 1 lit. a prawa telekomunikacyjnego określają uprawnienia tych podmiotów do zarządzenia zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. [np. art. 18 c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jedn. Dz. U. z 2021 r. poz. 1882 z późn. zm.), zwanej dalej ustawą o Policji].	

			Mając powyższe przepisy na względzie wydaje się zatem uzasadnione oczekiwanie rozszerzenia regulacji już istniejącej i obowiązującej zamiast projektowania i wydawania kolejnej ustawy regulującej kolejne obowiązki z zakresu bezpieczeństwa i obronności nakładane na przedsiębiorcę telekomunikacyjnego. Projekt omawianej ustawy powstał i jest procedowany w czasie, gdy na bardzo zawansowanym etapie są prace legislacyjne nad projektem ustawy Prawo komunikacji elektronicznej i nad przepisami wprowadzającymi prawo komunikacji elektronicznej oraz procedowany jest projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, w których określono obowiązki przedsiębiorców telekomunikacyjnych zbieżne z zakresem objętym projektem. Zasadnym zatem będzie uwzględnienie przedmiotu regulacji objętego projektem w projektowanym Prawie Komunikacji Elektronicznej, gdyż pozytywnym skutkiem takiego działania będzie to, że przepisy będą bardziej czytelne oraz nie będzie dochodziło do różnych definicji lub powieleń definicji tych samych określeń. Z kolei prawa i obowiązki dostawcy poczty elektronicznej w zakresie objętym projektem, można określić w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn. Dz. U. z 2020 r. poz. 344), zwanej dalej ustawą o świadczeniu usług drogą elektroniczną, która to ustawa przecież reguluje także instytucję poczty elektronicznej. Jak pokazuje powyższa analiza różne ustawy nakładają na przedsiębiorcę telekomunikacyjnego obowiązek podjęcie określonych działań organizacyjnych i technicznych	

			związanych z realizacją zadań na rzecz obronności i bezpieczeństwa, co wiąże się z ponoszeniem kosztów. Część tych zadań ma na celu zabezpieczenie infrastruktury, usług, danych lub przekazów telekomunikacyjnych znajdujących się we władaniu przedsiębiorcy telekomunikacyjnego- te zadania są i powinny być realizowane na koszt przedsiębiorcy telekomunikacyjnego. Są jednak i inne zadania z tego zakresu realizowane na rzecz organów administracji publicznej odpowiedzialnych za obronność i bezpieczeństwo, przykładowo tylko wskazując do takich zadań należą: - zapewnienie podmiotom właściwym w sprawach bezpieczeństwa warunków technicznych i organizacyjnych dostępu do przekazów i danych telekomunikacyjnych oraz ich utrwalanie (art. 179 ust 3 prawa telekomunikacyjnego), - zatrzymywanie, przechowywanie, zabezpieczenie niektórych danych telekomunikacyjnych oraz ich udostępniania podmiotom właściwym w sprawach bezpieczeństwa, (art. 180 a prawa telekomunikacyjnego, art. 180 c prawa telekomunikacyjnego, art. 180 d prawa telekomunikacyjnego). Również obowiązki określone w projekcie realizowane będą na rzecz bezpieczeństwa państwa oraz bezpieczeństwa wewnętrznego i porządku publicznego. Obowiązki te powinny być w dalszym ciągu realizowanie przez przedsiębiorców telekomunikacyjnych jako zadanie niezwykle istotne dla obronności i bezpieczeństwa, natomiast finansowanie ich winno następować z budżetu państwa. Rekomendujemy zatem podjęcie działań legislacyjnych dotyczących finasowania niektórych obowiązków	

			realizowanych przez przedsiębiorców telekomunikacyjnych ze środków budżetu państwa.	
14.	ZTKIG	Tytuł ustawy	**Tytuł ustawy o zwalczaniu nadużyć w komunikacji elektronicznej** Wskazane by było wprowadzenie zmiany tytułu ustawy na: *„ ustawa z dnia ……. o zwalczaniu nadużyć w telekomunikacji*" lub też pozostawić tytuł w zaproponowanym brzmieniu przy jednoczesnym zdefiniowaniu w słowniczku projektu definicji legalnej pojęcia „*komunikacji elektronicznej*". Dotychczas bowiem nie zdefiniowano pojęcia „*komunikacja elektroniczna*", gdy tymczasem pojęcie to pojawiło się i jest zdefiniowane w projekcie ustawy Prawo komunikacji elektronicznej.	**Uwaga nieuwzględniona** Zasadność wprowadzenia legalnej definicji komunikacji elektronicznej powinna zostać ewentualnie rozważana na gruncie projektowanej ustawy - Prawo komunikacji elektronicznej.
15.	ZTKIG	Art. 1 ust. 1 pkt 3	**Art. 1 ust. 1 pkt 3** Proponujemy obowiązki dostawcy poczty elektronicznej określić w ustawie o świadczeniu usług drogą elektroniczną, gdyż jest to właściwe miejsce do zawarcia tego rodzaju regulacji, czego nie można powiedzieć o opiniowanym projekcie.	**Uwaga wyjaśniona** Obowiązki dostawcy poczty elektronicznej mają na celu przeciwdziałanie spoofowaniu poczty elektronicznej, dlatego zasadne jest umieszczenie tych przepisów w projekcie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej.
16.	Porozumienie Zielonogórskie	Art. 2 pkt 2	W art. 2. Rozszerzyć definicję dostawcy poczty elektronicznej o spółki cywilne oraz m.in. jawne. Te spółki nie mają osobowości prawnej ani nie są osobami fizycznymi więc nie spełniają kryteriów z definicji	**Uwaga wyjaśniona** Definicja dostawcy poczty elektronicznej obejmuje jednostki organizacyjne nieposiadające osobowości prawnej, a więc również wszystkie spółki osobowe wskazane w Kodeksie spółek handlowych. Ponadto spółka cywilna jest jednostką organizacyjną, także definicja również obejmuje tę spółkę.

17.	ZTKIG	Art. 2 pkt 3	**Art. 2 ust. 1 pkt 3** Definicję legalną pojęcia „komunikatu elektronicznego" należałoby zaczerpnąć z projektu ustawy Prawo komunikacji elektronicznej (Projekt z dnia 5 maja 2022 r.). Definicję komunikatu elektronicznego w projekcie w porównaniu do definicji zawartej w art. 1 pkt 19 projektu PKE rozszerzono o frazę: *„… lub usług komunikacji interpersonalnej niewykorzystujących numerów*;" **Jest to argument przemawiający za tym, aby regulacje objęte projektem umieścić w prawie telekomunikacyjnym lub w projektowanej ustawie PKE.**	**Uwaga uwzględniona** Definicja komunikatu elektronicznego zostanie uspójniona z projektem ustawy - Prawo komunikacji elektronicznej.
18.	ZTKIG	Art. 2 pkt 9	**Art. 2 ust. 1 pkt 9** Definicja o takiej treści znajduje się już w projekcie ustawy Prawo komunikacji elektronicznej (art. 2 pkt 35 projektu PKE). **Jest to kolejny argument przemawiający za tym, aby regulacje objęte projektem umieścić w prawie telekomunikacyjnym lub w projektowanej ustawie PKE.**	**Uwaga wyjaśniona** Ustawa posługuje się siatką pojęciową niezbędną dla uregulowania materii nadużyć w komunikacji elektronicznej.
19.	ZTKIG	**Art. 2 pkt 12**	Definicja zawarta w art. 2 pkt 12 i 13 są podobne do definicji znajdującej się w art. 2 pkt 79 projektu PKE. Definicje te nieco różnią się między sobą. Jest to również argument przemawiający za tym, aby regulacje objęte Ustawą umieścić w ustawie z 16 lipca 2004 r. Prawo telekomunikacyjne lub w projektowanej ustawie PKE.	**Uwaga wyjaśniona** Ustawa posługuje się siatką pojęciową niezbędną dla uregulowania materii nadużyć w komunikacji elektronicznej.
20.	Krajowa Izba Komunikacji Ethernetowej	Art. 2, art. 3	Definicje pojęć w projekcie ustawy	**Uwaga częściowo uwzględniona w zakresie uzupełnienia regulacji o MMS**

			Analiza definicji terminów oraz definicji nadużyć w komunikacji elektronicznej wskazuje, że terminologia w projekcie ustawy wymaga dokładnej analizy oraz korekty. Sam termin „nadużycie w komunikacji elektronicznej" z art. 2 pkt 4 projektu ustawy jest niejasny i konieczne jest jego przepracowanie. Nie jest wiadome czym jest *„przeznaczenie usług telekomunikacyjnych i urządzeń telekomunikacyjnych*", ani czym są nienależne korzyści. W dodatku projekt ustawy w tej definicji (oraz w innych definicjach) posługuje się zwrotami i sposobem myślenia z przepisów prawa karnego, tj. do określenia działania jako nadużycia wymaga również celu lub skutku działania polegającego najczęściej na wyrządzeniu szkody lub osiągnięciu „nienależnych korzyści". Taka filozofia jest prawidłowa przy ocenie przez organy ścigania i wymiaru sprawiedliwości zamiaru sprawcy przy określaniu karalności czynu. W przedmiotowym projekcie ustawy jest to wadliwa regulacja, gdyż wymaga od podmiotów gospodarczych oceny celu działania ich użytkownika lub partnera handlowego, do czego przedsiębiorcy z sektora ICT nie są ani uprawnieni, ani przygotowani. Przedsiębiorca telekomunikacyjny nie jest w stanie określić czy przesyłane do jego sieci SMS mają na celu spowodowanie nieświadomego rozporządzenia majątkiem użytkownika końcowego lub mają na celu wyrządzenie mu krzywdy. Co więcej poszczególne definicje nadużyć w komunikacji elektronicznej są niejasne oraz niespójne z przepisami projektu ustawy, w tym z samą definicją nadużycia w komunikacji elektronicznej. Definicja nadużycia w komunikacji elektronicznej wymaga celu lub skutku	Ustawa będzie odnosić się do wiadomości MMS, w kontekście uprawnienia przedsiębiorcy telekomunikacyjnego do blokowania MMS, które będą zawierające treści wyczerpujące znamiona smishingu, a także w kontekście penalizowania wysyłki takich wiadomości. **Uwaga nieuwzględniona w pozostałym zakresie** Nie jest konieczne definiowanie każdego wyrazu wykorzystywanego w przepisach. Pojęcia takie jak przeznaczenie usług i urządzeń telekomunikacyjnych są zrozumiałe, a ich definiowanie mogłoby jedynie wprowadzić niepotrzebne wątpliwości. Ponadto, „odbiorcą", wobec którego jest skierowane nadużycie, często będzie „abonent" w przypadku usług świadczonych na rynku detalicznym. Równocześnie nie wydaje się właściwe stworzenie definicji spoofingu czy smishingu nie wskazując na konkretny cel jaki przyświeca sprawcy. Zgodnie z informacjami przedstawionymi przez przedsiębiorców telekomunikacyjnych oraz uwzględniając projektowane rozwiązania, możliwe będzie rozpoznawanie występowania nadużyć telekomunikacyjnych. Nie można też zgodzić się z zarzutem niespójności. Wszystkie definicje odnoszą się do celu działań sprawcy. Należy też podkreślić, że nie jest intencją

			działania w postaci wyrządzenia szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści. Tymczasem żadna z szczegółowych form nadużyć nie ma odwołania do skutku a jedynie do celu. Co więcej cele działania przy smishingu jak i przy spoofingu są znacznie szersze niż wyrządzenie szkody lub osiągnięcie korzyści. Wskazujemy, że przykładowo wymienione cele smishingu przekierowanie na stronę internetową, żądanie kontaktu telefonicznego lub instalacji oprogramowania nie muszą prowadzić do szkody. KIKE zwraca uwagę, że: - przepisy projektu ustawy zostały tak sformułowane, że zakazuje się świadczenia usług telekomunikacyjnych w sposób, którego skutkiem może być osiągnięcie nienależnych korzyści. Sformułowanie to jest skrajnie szerokie i KIKE wyraża wątpliwość czy projektodawca rozważył konsekwencje tej regulacji z punktu widzenia choćby regulacji telekomunikacji. Przykładowo KIKE nie ma wątpliwości, że pobieranie przez operatorów mobilnych nadmiernych opłat za zakańczanie SMSów A2P będzie stanowiło nienależne korzyści. Oznacza to, że działania operatorów mobilnych w tym zakresie naruszają przepisy prawa i tym samym nie podlegają jego ochronie. Analogicznie ocenić należy fakt korzystania z urządzeń uzyskiwania przez OPL nieuzasadnionych korzyści związanych choćby z tranzytem wewnętrznym do sieci mobilnej. - niezrozumiałe jest także w jaki sposób możliwe jest świadczenie usług telekomunikacyjnych niezgodnie z ich przeznaczeniem. Czy było objęte intencją prawodawcy, by każde świadczenie usług telekomunikacyjnych niezgodnie z przepisami prawa będzie stanowiło	projektodawcy objęcie zakresem niniejszej ustawy „zwykłej” działalności związanej z prowadzeniem marketingu bez zgody użytkownika. Wskazane przez zgłaszającego uwagę rozwiązania, w kontekście rozszerzenia obowiązków po stronie przedsiębiorców telekomunikacyjnych wiązałoby się z koniecznością analizowania treści komunikatów oraz zestawiania ich z innymi informacjami. Ponadto część komunikacji elektronicznej wykorzystuje szyfrowania end-to-end, więc wykrywanie ich byłoby niemożliwe. Problem smishingu jest nadal aktualny istnieje, zgodnie z danymi CSIRT NASK przekazanymi przez odbiorców wiadomości: - Łączna liczba podejrzanych SMS-ów – IV-XII 2021: 16 724; - Łączna liczba podejrzanych SMS-ów – 1. półrocze 2022: 66 385; - Liczba SMS-ów zawierających niebezpieczny link – IV-XII 2021: 7 313; - Liczba SMS-ów zawierających niebezpieczny link – 1. półrocze 2022: 27 217.

			nadużycie w komunikacji elektronicznej, którego skutkiem będzie np. osiągnięcie nienależnych korzyści? Przykład w tym zakresie stanowić może zawarcie w treści umowy o świadczenie usług komunikacji elektronicznej niedozwolonej klauzuli umownej. Czy w każdym takim wypadku inni przedsiębiorcy będą zobowiązani (zgodnie z treścią art. 3 ust. 2 projektu) do zapobiegania takim nadużyciom i ich zwalczania, choćby przez blokowanie ruchu przychodzącego od przedsiębiorcy naruszającego przepisy prawa? - wątpliwości Izby budzi także zamknięty katalog podmiotów, które mogą być poszkodowane nadużyciem w komunikacji elektronicznej. W szczególności – nie obejmuje abonentów. Nie obejmuje też podmiotów trzecich, na których szkodę niekiedy podmioty dopuszczają się nadużyć w komunikacji elektronicznej. - przepis obejmuje w zakresie swoje dyspozycji osiągnięcie nienależnych korzyści w sytuacji, w której nie zostanie wyrządzona szkoda. Czy intencją było objęcie jego zakresem „zwykłej" działalności związanej z prowadzeniem marketingu bez zgody użytkownika? Co kluczowe także zapis art. 16 odbiega od hipotezy art. 3 projektu (np. właśnie poprzez poszerzenie zakresu podmiotowego o podmioty inne niż wskazane w art. 3 ust. 1 pkt 1). Innymi słowy – kary przewidziane są w przypadkach, które nie są objęte zakazem opisanym w art. 3 ust. 1-3. KIKE wyraża także zastrzeżenia wobec zakresu przedmiotowego regulacji. W szczególności niezrozumiałe jest zdefiniowanie nadużyć jako dokonywanych w komunikacji elektronicznej, mających za przedmiot komunikaty elektroniczne, podczas gdy podmiotem regulacji są wyłącznie przedsiębiorcy	

			telekomunikacyjni, tj. podmioty inne niż podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów, w szczególności dostawcy poczty elektronicznej. Niezrozumiałe jest także, dlaczego przedmiot regulacji obejmują wyłącznie wiadomości SMS, nie zaś wiadomości MMS czy RCS, nie wspominając o innych formach komunikatów niepowiązanych z sieciami.	
21.	HACK&PHACK DEFENCE LTD Piotr Marcin Wierzbicki	art. 2, art. 3	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Opierając się na doświadczeniu wynikającym z praktyki wnoszę o uwzględnienie moich poniższych uwag do projektu UD402: z art. 2 ustęp 4 usunięcie słów: „celem lub skutkiem„ a w ich miejsce wpisanie słów ”skutkiem wynikającym z celowego działania”, bo znając zasadę rozliczeń między operatorskich IC/CW mogą się często zdarzać sytuacje gdy np. pracownicy jakiej bądź firmy lub nawet osoby prywatne korzystając ze swojego numeru telefonu będą w większości wykonywać połączenia wychodzące do innych sieci (np. kontakt z klientami albo starszą osobą która nie potrafi zbytnio korzystać z telefonu i ogranicza jego użytkowanie do odbierania połączeń do Niej przychodzących) a mając abonament typu No Limit przy określonych dyrektywą UE stawkach MTR/FTR - zostanie to uznane za działanie na szkodę przedsiębiorcy telekomunikacyjnego i będzie podlegać odpowiedzialności wynikającej z niniejszego projektu ustawy. Do tego słowa „osiągnięcie nienależytych korzyści” art. 2 ustęp 4 w w/w przypadkach można przypisać operatorowi telekomunikacyjnemu do którego sieci byłyby takie połączenia kierowane i także pociągnąć do	**Uwaga nieuwzględniona** Nie jest jasne dlaczego wykonywanie połączeń do klientów w sposób wskazany w uwadze miałoby mieć charakter nadużycia w komunikacji elektronicznej. Nie jest jasne proponowane pojęcie *ultrakrótkich* połączeń głosowych. Procedura uruchamiania punktu styku sieci operatorów telekomunikacyjnych polegająca na kalibracji systemów rozliczeniowych tych operatorów nie będzie karana, jeżeli nie będzie wypełniała znamion przestępstwa. Sytuacje te uwzględniają postanowienia umów międzyoperatorskich.

			odpowiedzialności z mocy niniejszej ustawy dlatego wnoszę o skreślenie słów ”lub osiągnięcie nienależytych korzyści”. Dlatego wnoszę o wycofanie się z penalizacji i wszelkich innych form karania za – jak sam Ustawodawca podnosi - otwartą definicję nadużycia w komunikacji elektronicznej przez skreślenie z projektu UD402 zapisów artykułu 3 ustęp 1 pkt 1 - lub dodanie w nim w treści „**ultrakrótkich** połączeń głosowych” zamiast „połączeń głosowych”, w przypadku niezmodyfikowania tego artykułu wnoszę o jego skreślenie. Ponadto wnoszę o skreślenie art. 16 ustęp 1 pkt 1, bo penalizuje standardową procedurę uruchamiania punktu styku sieci operatorów telekomunikacyjnych polegającą na kalibracji systemów rozliczeniowych tych operatorów. Należy zwrócić uwagę, że istniejące przepisy Kodeksu Karnego skutecznie chronią interes prawny poszkodowanych, w tym przedsiębiorców telekomunikacyjnych oraz abonentów końcowych. Natomiast skupiłbym się na artykułach dotyczących CLI SPOOFING oraz SMISHING bo nie wzbudzają one większych kontrowersji poza oczywistym faktem , że np. zapoznanie się (nawet automatyczne) z treścią np. SMS wysyłanego przez adwokata narusza tajemnicę adwokacką (art 14 ustęp 2 projektu UD402 oraz art 14 ustęp 3 pkt 1 tego projektu).	
22.	IAB Polska	5	**UWAGA:** Zdaniem IAB Polska definicja nadużycia w komunikacji elektronicznej jest niepełna, ponieważ nie uwzględnia sytuacji, gdy nie tylko świadczenie usługi telekomunikacyjnej może stanowić nadużycie w komunikacji elektronicznej, ale również korzystanie z usług telekomunikacyjnym może takie nadużycie	**Uwaga uwzględniona** Definicja nadużycia w komunikacji elektronicznej zostanie uzupełniona o aspekt „korzystania”.

			stanowić, zwłaszcza że definicja nadużycia telekomunikacyjnego (art. 2 pkt 26) PKE) wskazuje, że nadużyciem jest „*świadczenie lub korzystanie z usługi telekomunikacyjnej*”. **PROPOZYCJA:** IAB Polska proponuje następującą zmianę definicji nadużycia w komunikacji elektronicznej: *4) nadużycie w komunikacji elektronicznej – świadczenie **lub korzystanie z** usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;*	
23.	Polska Izba Informatyki i Telekomunikacji	Art. 2 ust. 4	**Definicja nadużycia w komunikacji elektronicznej** (art. 2 pkt 4 projektu ustawy) Uzupełnienia o aspekt „korzystania” z usług telekomunikacyjnych wymaga projektowana definicja „nadużycia w komunikacji elektronicznej” (art. 2 pkt 4) projektowanej ustawy). Bez wątpienia projektowana definicja jest wzorowana na definicji „nadużycia telekomunikacyjnego”, zwartej w art. 2 pkt 26) projektu ustawy – Prawo komunikacji elektronicznej (dalej „projekt PKE”), jednak z powodów których nie znamy definicja tego pojęcia na gruncie projektu ustawy pomija element „korzystania” z usług telekomunikacyjnych jako działanie składające się na nadużycie. W naszej ocenie zawarta w projektowanej ustawie definicja „nadużycia w	**Uwaga uwzględniona** Definicja nadużycia w komunikacji elektronicznej zostanie uzupełniona o aspekt „korzystania”.

			komunikacji elektronicznej" powinna, na wzór projektu PKE, uzyskać następujące brzmienie: *nadużycie w komunikacji elektronicznej - świadczenie <u>lub korzystanie</u> z usługi telekomunikacyjnej lub urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;* Pominięcie „korzystania" z usług telekomunikacyjnych na poziomie definicji oznaczałaby diametralne zawężenie przypadków kwalifikujących się jako „nadużycie w komunikacji elektronicznej" w rozumieniu projektowanej ustawy, gdyż wiele nadużyć polega na korzystaniu z usług telekomunikacyjnych w sposób niezgodny z przepisami prawa i ich przeznaczeniem. Jedynie tytułem przykładu smishing (SMS) czy sztuczny ruch – a więc zjawiska wprost wskazane w projekcie ustawy jako nazwane postacie nadużyć w komunikacji elektronicznej (art. 3 ust. 1 projektu ustawy) - to przypadki korzystania z usług telekomunikacyjnych w sposób niezgodny z przepisami prawa i ich przeznaczeniem. Zatem należy powrócić do pierwotnego brzmienia definicji.	
24.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 2 pkt 4	**IX. [DEFINICJA NADUŻYCIA W KOMUNIKACJI ELEKTRONICZNEJ – ART. 2 PKT 4)]** **(33.)** W naszej ocenie pojęcie „*niezgodnego z ich przeznaczeniem*" wykorzystywania usługi jest zbyt nieostre, by mogło stanowić podstawę do jakichkolwiek sankcji.	**Uwaga nieuwzględniona** Nadużycia w komunikacji elektronicznej mają zgoła różny i często skomplikowany charakter dlatego celowo definicja jest ogólna. Świadczenie usługi telekomunikacyjnej niezgodnie z jej przeznaczeniem również powinno być uznane za nadużycie w

			(34.) Jeszcze raz pragniemy odnieść się do Prezentacji, gdzie podkreślono, że *„definicja posługuje się nieostrymi pojęciami, brak jest wyraźnie stypizowanych i konkretnych zachowań kwalifikujących je jako nadużycie telekomunikacyjne (może z wyjątkiem „nieuprawnionej" modyfikacji informacji adresowej o numerze)*". **(35.)** Wnosimy zatem o usunięcie z definicji [art. 2 pkt 4)] passusu „*z ich przeznaczeniem lub*". W konsekwencji art. 2 pkt 4) Projektu powinien otrzymać następujące brzmienie: *„nadużycie w komunikacji elektronicznej – świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;"*	komunikacji elektronicznej (por. art. 5 Kodeksu cywilnego).
25.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 2 pkt 8	**ad Art. 2 pkt 8)** poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie komunikatu elektronicznego z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol); <u>Propozycja PTI</u> Powyższą definicję skrócić do postaci: *poczta elektroniczna – usługa przekazywania komunikatu elektronicznego z wykorzystaniem protokołu SMTP bądź protokołów będących jego rozszerzeniem.* <u>Komentarz PTI</u> W treści ustawy nie należy umieszczać nazw produktów/protokołów, które mogą się z czasem technicznie zmieniać i występować pod innymi nazwami	**Uwaga nieuwzględniona** Poczta e-mail jest usługą komunikacji interpersonalnej niewykorzystującą numerów. Wskazanie wyłącznie standardu SMTP w nieuzasadniony sposób utrudni właściwą subsumpcję normy prawnej.

			– wystarczy podać jedynie charakterystyczny protokół SMTP z ogólnym dopuszczeniem protokołów go rozszerzających. Fraza *...komunikacji interpersonalnej niewykorzystującą numerów, …* jest niepotrzebna.	
26.	Unia Metropolii Polskich	Art. 2 pkt 8	Definicja poczty elektronicznej jest zbyt wąska i kazuistyczna. Nie obejmuje m.in. protokołów np. Exchange ActiveSync Microsoftu. Definicję należy zmienić na bardziej opisową .	**Uwaga uwzględniona** Poprzez dodanie „lub innego standardu zapewniającego te same funkcje”.
27.	IAB Polska	Art. 2 pkt 12	**UWAGA:** Przez wzgląd na rosnącą jakością obsługi konsumenta coraz powszechniejsze staje się udostępnianie na stronach internetowych świadczących różnego rodzaju usługi (sklepy internetowe, platformy handlu elektronicznego, platformy gier internetowych czy inne) dedykowanych kanałów ułatwiających komunikację konsumenta korzystającego z usług elektronicznych ze sprzedającym bądź z innymi użytkownikami danej strony. Przykładem takich narzędzi do komunikacji interpersonalnej niewykorzystującej numerów stanowią chatboty czy dedykowane kanały komunikacji. Usługa ta pozostaje podrzędna i dodatkowa względem usługi głównej, tj. przykładowo, sprzedaży przez stronę internetową bądź pośrednictwa w sprzedaży na platformie. Wyłączenie zawarte w art. 2 pkt 12 projektowanej ustawy ujęte zostało w sposób bardzo ogólny. Biorąc pod uwagę, iż zakres wyłączenia nie został doprecyzowany ani określony w uzasadnieniu do projektu ustawy, zakres podmiotowy projektowanej ustawy pozostaje niepewny, co w naszej ocenie może rodzić wątpliwości interpretacyjne kiedy regulacja wejdzie już w życie. Sankcyjny charakter projektowanej regulacji w	**Uwaga nieuwzględniona** Projekt ustawy nie reguluje obowiązków operatorów platform handlu elektronicznego czy portali udostepniających gry internetowe. Uwaga jest to poza zakresem projektowanej ustawy.

			połączeniu z terminologiczną niepewnością ma duży potencjał wywołania tzw. *chilling effect* wśród legalnie i prawidłowo działających podmiotów, a ponadto w takiej formule wywołuje uzasadnione zastrzeżenia odnośnie konstytucyjności takiej formuły zakazu i zgodności z prawidłową techniką prawodawczą. **PROPOZYCJA:** Nałożenie określonych w projektowanej ustawie obowiązków na przedsiębiorców prowadzących sklepy internetowe, będących operatorem platformy handlu elektronicznego czy portali udostępniających gry internetowe, którzy udostępniają kanały komunikacji stanowiącę usługę komunikacji interpersonalnej niewykorzystującej numerów byłoby nieproporcjonalne do świadczonych przez nich usług. W związku z powyższym proponujemy dodanie zdania drugiego do obecnego brzmienia art. 2 pkt 12 w następujący sposób "(...) *Funkcję podrzędną względem usługi podstawowej stanowi w szczególności usługa komunikacji interpersonalnej udostępniona w sklepach internetowych, na platformach handlu elektronicznego czy w grach internetowych.*", bądź dodanie do uzasadnienia projektu ustawy powyższego zdania.	
28.	Związek Banków Polskich	Art. 2 pkt 17 i 18	**17) bank – podmiot, o którym mowa w art. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.),** **18) spółdzielcza kasa oszczędnościowo-kredytowa – podmiot, o którym mowa w art. 2 ustawy z dnia 5**	**Uwaga częściowo uwzględniona** Odwołania do definicji ustawowych banku i SKOK znajdą się w przepisach dotyczących listy numerów wykorzystywanych wyłącznie do odbierania połączeń.

			listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. 2022 r. poz. 924). Proponujemy wprowadzenie definicji pojęć użytych w projekcie ustawy.	
29.	Polska Wytwórnia Papierów Wartościowych	Art. 3 ust. 1	W art. 3 ust. 1 projektu ustawy ujęto opisowo rodzaje nadużyć spotykanych w komunikacji elektronicznej, każdorazowo opatrując dane zachowanie nawiasem wraz z używaną nazwą, takich jak „sztuczny ruch", „smishing" czy „CLI spoofing". W związku z tym, że te pojęcia nie są powszechnie znane proponujemy rozważenie umieszczenia definicji w art. 2 projektu ustawy.	**Uwaga nieuwzględniona** Celowo wyodrębniono konkretne nadużycia w komunikacji elektronicznej. Zgodnie z zasadą zwięzłości tekstu prawnego przyjęte w projekcie rozwiązanie jest bardziej adekwatne.
30.	Krajowa Izba Komunikacji Ethernetowej	Art. 3 ust. 1 pkt 1	Sztuczne generowanie ruchu *„inicjowanie wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej , lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch)"* Izba potwierdza, że to nadużycie było wcześniej problemem związanym z wysokimi stawkami rozliczeniowymi między przedsiębiorcami telekomunikacyjnymi. Obecnie z powodu zmniejszenia w rozporządzeniu unijnym stawek FTR i MTR problem ten ma znacznie mniejszą skalę i szkody. W dodatku projekt ustawy oprócz zdefiniowania tego zjawiska (nieprecyzyjnego i niejasnego) nie wprowadza żadnych regulacji związanych z tym nadużyciem. Jednocześnie Izba wskazuje, że przedsiębiorcy telekomunikacyjni (przy współpracy Prezesa UKE) pozwierali umowy międzyoperatorskie identyfikujące i zwalczające to nadużycie. Wprowadzenie tej regulacji w	**Uwaga nieuwzględniona** Nadużycie związane ze sztucznym ruchem powinno być wprost zakazane na podstawie przepisów ustawy. W przypadku zagadnień mogących budzić jakąkolwiek wątpliwość (jak np. połączenia testowe), są przesądzone na gruncie umów zawieranych pomiędzy przedsiębiorcami.

			ustawie spowoduje konieczność zmiany tych umów międzyoperatorskich i kolejną dyskusję na temat legalności określonych rodzajów połączeń. Przykładowo Izba wskazuje, że istotą sztucznego ruchu jest wygenerowanie określonych „połączeń" w systemach billingowych. Nie jest celem sztucznego ruchu wyłącznie zarejestrowanie się na punktach styku sieci, gdzie rejestrowane są połączenia odebrane jak i nie odebrane (tylko te pierwsze generują przychody z rozliczeń międzyoperatorskich). Co więcej, proponowana definicja sztucznego ruchu obejmie połączenia testowe wykorzystywane przez przedsiębiorców telekomunikacyjnych do wykrywania spoofingu (operator generuje połączenia z danego kierunku co do którego ma podejrzenia podmieniania numeracji, po czym weryfikuje z jakim numerem to połączenie wróciło do jego sieci). W opinii Izby w chwili obecnej nie ma powodu do ustawowej regulacji sztucznego ruchu, tym bardziej że głównymi podmiotami dokonującymi takich działań są podmioty zagraniczne, których projekt ustawy nie obejmuje.	
31.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 3 ust. 1 pkt 1	**ad Art. 3. ust. 1. pkt 1)** inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch); <u>Propozycja PTI</u> Usunąć frazę *...lub odbierania….*	**Uwaga nieuwzględniona** Ruch ten może być wprowadzany do sieci telekomunikacyjnej, niekoniecznie „inicjowany", aby działanie takie stanowiło nadużycie polegające na sztucznym ruchu.

			Komentarz PTI Wpisanie frazy *...lub odbierania….* nie ma uzasadnienia, gdyż odbiorca takich komunikatów elektronicznych nie ma wpływu (oprócz całkowitej blokady dostępu do wszystkich komunikatów) na ich odbieranie. Jedynie po rozpoznaniu, mając odpowiednią wiedzę lub doświadczenie, może je zakończyć lub usunąć. W żadnym stopniu nie może odpowiadać za ich rozpowszechnianie, jeżeli ich dalej nie rozsyła, pod warunkiem że ma wiedzę, że są one komunikatami szalbierskimi.	
32.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 3 ust 1 pkt 1	**Art. 3 ust. 1 pkt 1** Pomysł, aby działalność w zakresie tzw. sztucznego ruchu traktować jako nadużycie należy ocenić pozytywnie. Natomiast wydaje się bardzo trudne (jeśli w ogóle możliwe) do wykazania, że dane zdarzenie ma znamiona nadużycia. Argumentem przemawiającym za stwierdzeniem, że określone działanie jest nadużyciem, jest cel tego działania, nawet w przypadku, gdy to działanie nie wywoła jakichkolwiek skutków. Celem bowiem przepisów projektu jest stworzenie narzędzi do zapobiegania nadużyciom w komunikacji elektronicznej zanim wywołają skutki. W projekcie nie określono sposobu zapobiegania nadużyciom w komunikacji elektronicznej zdefiniowanych w art. 3 ust. 1 pkt 1 projektu, ani też nie wskazano podmiotów i ich obowiązków w tym zakresie. Ponadto brak jest definicji pojęć: „*punkt połączenia sieci telekomunikacyjnych*”, „*systemy rozliczeniowe*”. Również prawo telekomunikacyjne nie definiuje takich pojąć. **Postulować by zatem wypadało umieszczenie w słowniczku ustawowym pojęć: „*punkt połączenia sieci***	**Uwaga wyjaśniona** Pod pojęciem systemów rozliczeniowych należy rozumieć każdy system używany przez przedsiębiorcę telekomunikacyjnego do obsługi rozliczeń za usługi telekomunikacyjne. Punkt styku sieci, czy punkt połączenia sieci telekomunikacyjnych należy intepretować zgodnie z przepisami ustawy Prawo telekomunikacyjne. W przypadku innych wyrażeń i wątpliwości – ze słownictwem używanym w dziedzinie telekomunikacji.

			***telekomunikacyjnych*", „*systemy rozliczeniowe*" oraz określenie ich definicji legalnych.**	
33.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 3 ust. 1 pkt 2	**ad Art. 3 ust. 1. pkt 2)** wysyłania krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę internetową, żądania kontaktu telefonicznego lub instalacji oprogramowania (smishing); Propozycja PTI W danym przepisie i w całym tekście ustawy używanie terminu **esemes** (zamiast SMS) oraz nazwanie tych komunikatów terminem **esemesy szalbierskie**. Komentarz PTI Rozwinięcie jest zawarte w uwadze ogólnej.	**Uwaga nieuwzględniona** Określenie „szalbierczy" potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, iż jest to archaizm. Wyraz ten jest rzadko używany w codziennych dyskursach. Z tego powodu proponuje się pozostawienie pojęcia „smishing", które jest powszechnie znane i wykorzystywane.
34.	Krajowa Izba Komunikacji Ethernetowej	Art. 3 ust. 1 pkt 3	Spoofing *„nieuprawnione posłużenie się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing)".* Izba całkowicie zgadza się z Panem Ministrem w konieczności bezprawnej podmiany numeru wywołującego połączenie telefoniczne. Niemniej wskazujemy, że definicja tego zjawiska w projekcie ustawy jest niejasna oraz niepełna. Nie obejmuje ona	**Wyjaśnienie** Kwestia oszustw na rozliczeniach międzyoperatorskich została uwzględniona w definicji sztucznego ruchu. Z kolei kwestia wyłudzania danych bankowych jest uwzględniona w obecnej definicji spoofingu. W związku z tym, że wprowadzone zostało nadużycie w telekomunikacji polegające na nieuprawnionej modyfikacji informacji adresowej w postaci numeru telefonu lub identyfikatora użytkownika wysyłającego komunikat elektroniczny albo wywołującego połączenie głosowe. Tym samym ukrywanie numeru przed służbami również będzie ujęte w tej ustawie.

			wiele niekorzystnych zjawisk związanych z podmianą numeru abonenta (fraudy na rozliczeniach międzyoperatorskich, ukrywanie przez służbami numeru, z którego wykonywane są fałszywe alarmy bombowe). Do regulacji wymaga ona podszywania się pod inny podmiot oraz określonego celu działania oszusta, który nie musi być wiadomy przedsiębiorcy telekomunikacyjnemu. Definicja nie obejmuje m.in. podmiany numeru A w zakresie zmiany rozliczeń za zakańczanie połączeń czy w celu wyłudzenia danych bankowych.	
35.	Polska Izba Informatyki i Telekomunikacji	Art. 3 ust. 1 pkt 3	**Definicja CLI spoofingu** (art. 3 ust. 1 pkt 3) projektu ustawy) Przedstawiona w projekcie ustawy definicja zakłada, że CLI spoofing ma miejsce w przypadku, gdy nieuprawnionego posłużenia się informacją adresową dopuszcza się „użytkownik" wywołujący połączenie głosowe. I faktycznie tak skonstruowana definicja obejmie swoim zakresem zdecydowaną większość przypadków CLI spoofingu. Niemniej jednak pogłębione analizy wykazały, że historycznie zdarzały się (nieliczne, ale jednak) przypadki, w których podmiotem w sposób nieuprawniony posługującym się informacją adresową podczas inicjowania połączenia był nieuczciwy przedsiębiorca telekomunikacyjny (a nie użytkownik). Biorąc pod uwagę, że pojęcie „użytkownika" jest zdefiniowane w ustawie – Prawo telekomunikacyjne (i oznacza podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi – art. 2 pkt 49) ustawy – Prawo telekomunikacyjne) tak skonstruowana definicja CLI spoofingu będzie pomijała przypadki, w których to nieuczciwy przedsiębiorca telekomunikacyjny jest	**Uwaga uwzględniona częściowo** W definicji CLI spoofing zostanie dodane, że może się go dopuścić również przedsiębiorca telekomunikacyjny. W definicji zostanie uwzględniona również intencja w postaci wywołania strachu u innej osoby. **W pozostałym zakresie uwaga nieuwzględniona** Nie można zgodzić się z usunięciem z definicji CLI spoofingu intencji sprawcy. Celem ustawy jest przeciwdziałanie konkretnym przestępstwem i działanie w tym zakresie muszą odnosić się do tych działań.

			podmiotem, który inicjuje połączenie w sposób nieuprawniony posługując się informacją adresową. Ponadto, zwracamy uwagę, że przedsiębiorcy telekomunikacyjni nie dysponują i nie będą dysponowali rozwiązaniami, które pozwolą ustalić jaki cel ma osoba albo podmiot wykonujący spoofowane połączenie głosowe. Z perspektywy organów ścigania tak skonstruowana definicja będzie oznaczała konieczność udowodnienia, że sprawca działał w celu nakłonienia odbiorcy połączenia do określonego działania, co dowodowo może być trudne do osiągnięcia. Nie można również zapominać, że w niektórych przypadkach, znanych publicznie i opisywanych w mediach, celem sprawców nie było nakłonienie ofiary do określonego działania, a sprawcom chodziło najprawdopodobniej o wywołanie strachu, poczucia zagrożenia u odbiorcy spoofowanego połączenia (przypadki osób publicznych i polityków otrzymujących połączenia informujące o śmierci osób najbliższych). Z tej perspektywy warto się zastanowić nad usunięciem z definicji słów „… służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania …”. W związku z powyższym, aby definicja CLI spoofingu obejmowała wszystkie znane scenariusze działań nadużyciowych w tym zakresie, postulujemy nadanie jej następującego brzmienia (zmiany w stosunku do obecnego brzmienia przepisu widoczne są jako przekreślenia i podkreślenia):	

			nieuprawnionego posłużenia się przez ~~użytkownika~~ wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ~~ten użytkownik~~ <u>podmiot wywołujący</u>~~, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania~~ (CLI spoofing). Definicja w kształcie zaproponowanym powyżej powinna objąć swoim zakresem wszystkie znane przypadki CLI spoofingu, a zaproponowane brzmienie usuwa potencjalne problemy jakie wiążą się z niemożnością ustalenia przez przedsiębiorcę telekomunikacyjnego zamiaru / celu / intencji spoofera, ułatwiając organom ścigania pociągniecie sprawców do odpowiedzialności, zwalniając je z konieczności udowodnienia działania w konkretnym celu. Jednocześnie definicja w zaproponowanym brzmieniu zachowuje podstawowe przesłanki uznania określonego działania za CLI spoofing, mianowicie nieuprawnione posłużenie się informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż podmiot wywołujący połączenie głosowe. W przypadku uwzględnienia powyższych zmian definicyjnych odpowiednich zmian wymagać będzie również brzmienie art. 16 ust. 1 pkt 3) projektu ustawy.	
36.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 3 ust. 1 pkt 3	**ad Art. 3 ust. 1 pkt 3)** nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu	**Uwaga nieuwzględniona** Określenie „szalbierczy” potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, iż jest to archaizm. Wyraz ten jest

			się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing). <u>Propozycja PTI</u> Wprowadzenie zamiast określenia „(CLI spoofing)" terminu: ***szalbierczy numer dzwoniącego*** <u>Komentarz PTI</u> Termin CLI spoofing jest mało zrozumiały. Już lepszy byłby termin Caller ID spoofing, gdyby nie był angielski, dlatego proponujemy używanie terminu - **szalbierczy numer dzwoniącego,** jednoznacznie wskazujący na szkodliwy identyfikator dzwoniącego.	rzadko używany w codziennych dyskursach. Z tego powodu proponuje się pozostawienie pojęcia „smishing", które jest powszechnie znane i wykorzystywane.
37.	Polska Izba Komunikacji Elektronicznej	Art. 3 ust. 1 pkt 3	**Pojęcie „CLI spoofing"** ***(art. 3 ust. 1 pkt 3)*** Art. 3 ustawy wprowadza katalog otwarty nadużyć w komunikacji elektronicznej. Jednocześnie wskazuje na trzy typowe naruszenia, stanowiące największe zagrożenia. PIKE szczególnie zwraca uwagę na proponowane w art. 3 ust. 1 pkt 3) pojęcie CLI spoofing. Proponuje się, aby przepis przyjął następujące brzmienie: **Art. 3.** 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności dotyczące: (…) 3) nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania	**Uwaga częściowo uwzględniona** W projekcie zostanie dodana nowa postać nadużycia w komunikacji elektronicznej, uwzględniające podmianę numeru abonenta.

			danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing). Otóż zawarte w projekcie pojęcie CLI spoofing nie zostało dostatecznie doprecyzowane. Nie uwzględnia ono szeregu stosowanych obecnie technologii i występujących zjawisk, a także odmiennych niż wskazane w przepisie działań użytkownika. Za przykład może posłużyć wskazane już wcześniej zjawisko podmiany numeru abonenta, z którego dokonywane jest połączenie. Co więcej, wskazuje się, że jest to działanie służące podszyciu się pod inny podmiot, a zatem skoro użytkownik podawałby się za podmiot nieistniejący, to nie wkraczałoby to w zakres zastosowania przepisu (błąd legislacyjny). Zastosowanie przepisu zostało w ten sposób znacznie zawężone. Egzekwowanie regulacji i objęcie nią możliwie wielu odmian spoofingu wymaga przygotowania pojęcia udoskonalonego, precyzyjnego i uwzględniającego szeroki wachlarz stosowanych technologii i działań. **Izba postuluje zatem o podjęcie próby zaprojektowania definicji od początku.**	
38.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 3 ust. 1 pkt 3	**Art. 3 ust. 1 pkt 3** Pojęcie „informacja adresowa” jest niejednoznaczne. **Proponujemy zatem zawarcie definicji legalnej tego pojęcia w słowniczku projektu.**	**Uwaga nieuwzględniona** Pojęcie to nie jest definiowane również w Prawie telekomunikacyjnym oraz w projektowanym Prawie komunikacji elektronicznej, podobnie jak inne zwroty dotyczące kwestii identyfikacji użytkownika. Przepisy powinny być przyszłościowe, a samo pojęcie informacji adresowej jest bardzo pojemne - obejmuje numery i identyfikator użytkownika. Identyfikatorem mogą być znaki identyfikujące abonenta (z art. 130 Pt np. adresy elektroniczne, nazwy, kody,

				radioamatorskie znaki identyfikujące stację) oraz też adresy IP. W powyższym zakresie zostało uzupełnione uzasadnienie.
39.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 3 ust. 1	II. [OTWARTOŚĆ KATALOGU NADUŻYĆ – ART. 3 UST. 1] **(3.)** Zwracamy uwagę, że **określenie otwartego katalogu** zachowań wyczerpujących znamiona nadużyć w komunikacji elektronicznej **nie jest zasadne**. **(4.)** Wskazujemy, że penalizowane są jedynie nadużycia enumeratywnie określone w art. 3 ust. 1 pkt 1-3. **(5.)** Zatem z praktycznego punktu widzenia **ogólny zakaz nadużyć w komunikacji elektronicznej okaże się nieskuteczny**. **(6.)** W tym zakresie zwracamy uwagę, że w 2018 r. ówczesne MC wskazało (w odpowiedzi na uwagi zgłaszane przez PIIT i KIGEiT w ramach tzw. Okrągłego Stołu ds. FTR w prezentacji zatytułowanej „*NADUŻYCIA TELEKOMUNIKACYJNE – PROPOZYCJE IZB*"; prezentacja została przesłana w dniu 10 września 2018 r., zwana dalej „***Prezentacją***"), że „*wydaje się, że tego rodzaju działania powinny być precyzyjnie wskazane, zwłaszcza że podlegać mają sankcjonowaniu przez organ regulacyjny*" (Prezentacja s. 3). Zdaniem Izby powyższe wątpliwości są aktualne. **(7.)** Naszym zdaniem należy **rozważyć rozszerzenie katalogu zachowań wyczerpujących znamiona nadużyć w komunikacji elektronicznej oraz jego zamknięcie**. Zatem **w art. 3 ust 1 wnosimy o usunięcie zwrotu „w szczególności"**.	**Uwagi nieuwzględnione** Problem nadużyć nie ogranicza się wyłącznie do zjawisk sztucznego ruchu, smishingu, CLI spoofingu i podszywania się w komunikacji z wykorzystaniem poczty elektronicznej. Nie należy również zakładać, że nie jest zmienny w czasie. Dlatego zasadne jest odzwierciedlenie stanu faktycznego poprzez otwarcie katalogu. Nie mniej, ze względu na fakt, ze pozostałe nadużycia są „nienazwanymi" w świetle projektu ustawy, obowiązek przeciwdziałaniu nim nie jest obwarowany sankcjami. Równocześnie jednak przedsiębiorcy telekomunikacyjni powinni podejmować działania mające przeciwdziałać nowym metodom działania przestępców.

40.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 3 ust. 1	**[ROZSZERZENIE NAZWANYCH PRZYPADKÓW NADUŻYĆ W KOMUNIKACJI ELEKTRONICZNEJ – ART. 3 UST. 1]** **(8.)** Izba od wielu lat wskazuje, że **genezą większości nadużyć jest podmiana numeru A (czego emanacją jest również CLI spoofing) oraz korzystanie z usług detalicznych w celu realizacji usług hurtowych**. **(9.)** Istotą nadużycia w zakresie podmiany numeru jest to, że (z uwagi na asymetrię rozliczeń EOG/non-EOG) połączenia kierowane z obszaru non-EOG są opisywane numerami ze strefy EOG (w tym numerami krajowymi). Celowa modyfikacja przez nieuczciwych przedsiębiorców numeru międzynarodowego na numer krajowy w systemach bilingowych, prowadzi do stosowania w rozliczeniach międzyoperatorskich niższej stawki. Dodatkowo należy podkreślić, iż propozycje regulacji dotyczące niezmienności numeru będą miały na względzie zapewnienie bezpieczeństwa i porządku publicznego, co sprzyjać będzie prawidłowemu wykonywaniu obowiązków przez organy powołane m.in. do niesienia pomocy (lokalizacja). **(10.) Wnosimy stąd o uzupełnienie zachowań wyczerpujących znamiona nadużyć w komunikacji elektronicznej o przypadki, o których mowa w pkt (11-12.)**. **(11.)** W stanowisku z dnia 15 października 2018 r. sformułowaliśmy następującą redakcję przepisu: *„1. Zakazane jest nieuprawnione wykorzystanie usług telekomunikacyjnych, w połączonych sieciach lub innych sieciach telekomunikacyjnych, przy zastosowaniu środków niezgodnych z prawem, polegające na:*	**Uwaga częściowo uwzględniona w zakresie modyfikacji numeru międzynarodowego na numer krajowy** W projekcie zostanie dodana nowa postać nadużycia w komunikacji elektronicznej, uwzględniające podmianę numeru abonenta. Informacja adresowa o numerze abonenta wywołującego powinna być zasadniczo niezmienna na całej drodze połączeniowej, o czym stanowi obecne brzmienie § 1 załącznika pn. „Szczegółowe wymagania dotyczące zasad adresowania dla właściwego kierowania połączeń” do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 12 grudnia 2014 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania połączeń dla właściwego kierowania połączeń. Dodany do projektu ustawy nowy rodzaj nadużycia polega na niedozwolonym oddziaływaniu na urządzenia telekomunikacyjne i zmianę danych rejestrowych np. połączenia międzynarodowego wywołującego (numeru A) oraz takim kierowaniu ruchu telekomunikacyjnego z/do innych sieci telekomunikacyjnych lub za pośrednictwem sieci operatorów, aby zgubić źródło ruchu i zakończyć połączenie po stawkach krajowych. Zasadniczym celem podmiany numeru jest wprowadzenie w błąd (co do źródła ruchu) systemów operatora do którego powinien trafić ruch. W wyniku powyżej opisanej działalności operatorzy telekomunikacyjni nie są w stanie przedstawić prawdziwych i

			a) nieuprawnionej modyfikacji lub zmianie numeru inicjującego połączenie (numeru A), z zastrzeżeniem ust. 2, *b) przesyłaniu sygnalizacji niezwiązanej ze świadczeniem usług,* *c) świadczeniu hurtowych usług międzysieciowych z wykorzystaniem usług abonenckich, w tym z wykorzystaniem urządzeń FCT, simboxing,* *d) wykorzystaniu jakichkolwiek numerów bądź zakresów numeracji niezgodnie z ich przeznaczeniem określonym w PNK lub decyzji o przydziale numeracji.* *2. Nie stanowi zmiany, o której mowa w ust. 1 modyfikacja numeru, która wynika z realizacji zasad adresowania dla właściwego kierowania połączeń ustalonych na podstawie art. 126 ust. 13".* Powyższe zachowania są aktualne obecnie. **(12.)** Ingerencji ustawowej wymagają również inne przypadki nadużyć telekomunikacyjnych, takie jak celowe przesyłanie sygnalizacji niezwiązanej ze świadczeniem usług, świadczenie hurtowych usług międzysieciowych z wykorzystaniem usług abonenckich, w tym z wykorzystaniem urządzeń FCT, simboxing oraz wykorzystanie jakichkolwiek numerów bądź zakresów numeracji niezgodnie z ich przeznaczeniem określonym w PNK lub decyzji o przydziale numeracji. **(13.)** Przedstawione rozwiązanie bazuje na wypracowanych na rynku telekomunikacyjnym postanowieniach umownych związanych z regulacją stawek MTR i FTR.	kompletnych informacji o tym, kto faktycznie dzwonił na podany numer. **W pozostałym zakresie uwaga nieuwzględniona** W zakresie rozliczeń między operatorami należy zauważyć, że sztuczny ruch został już uwzględniony w projekcie ustawy. Pozostałe propozycje mogą się mieścić w otwartym katalogu nadużyć w komunikacji elektronicznej.

			(14.) W ocenie Izby **niezbędne jest wprowadzenie sankcji w postaci pieniężnej kary administracyjnej, która będzie dodatkowo odstraszać przed stosowaniem nieuczciwych praktyk, o których mowa powyżej**. Na szczególną uwagę zasługuje kwestia niezmienności numeru A na całej drodze połączenia. **Obecnie takiego typu zachowania nie są penalizowane, a ogólny obowiązek niezmienności adresacji na całej drodze połączenia wynika z rozporządzenia, a nie ustawy**.	
41.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 3 ust. 2	**V. [OBOWIĄZEK PODEJMOWANIA PROPORCJONALNYCH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH MAJĄCYCH NA CELU ZAPOBIEGANIE NADUŻYCIOM W KOMUNIKACJI ELEKTRONICZNEJ I ICH ZWALCZANIE – ART. 3 UST. 2]** **(24.)** Taki ogólny obowiązek pojawił się w niektórych propozycjach Rynku dotyczących rozwiązań legislacyjnych w zakresie zwalczania nadużyć. **(25.)** W tym jednak zakresie należy wskazać, że **taki ogólny obowiązek nie został przez MC zaaprobowany**. Zwracano uwagę na następujące wątpliwości: 1) *„co dzieje się w praktyce, w przypadku gdy Prezes UKE uzna, że zastosowane środki są nieproporcjonalne lub nie służą realizacji celów przepisu? Co jeśli przedsiębiorca się odwoła od decyzji Prezesa? Jak dalej wygląda postępowanie?*”; 2) *„jakie są przesłanki do dokonania oceny, czy zastosowane środki są proporcjonalne i służą realizacji celu?*”;	**Uwaga wyjaśniona** Nadużycia w komunikacji elektronicznej mają zgoła różny i często skomplikowany charakter, a co za tym idzie przeciwdziałanie i zwalczanie ich wymaga podejmowania różnych (odmiennych) środków technicznych i organizacyjnych. Ww. jednostka redakcyjna zawiera ogólny obowiązek, dlatego mając na względzie na jego charakter, niesprostanie temu obowiązkowi – o ile nie jest związane z innymi, bardziej szczegółowymi obowiązkami – nie wiąże się z jakąkolwiek sankcją. Natomiast taka redakcja przepisu pozwala podkreślić, że projektodawca (a w przyszłości ustawodawca), nie tylko ma świadomość zjawiska i problemów wynikających z nadużyć telekomunikacyjnych, ale również uświadamia przedsiębiorców, że muszą te okoliczności uwzględnić prowadząc działalność telekomunikacyjną. W przedmiocie punktu trzeciego wątpliwość jest niezrozumiała, o jakim „zakazie Prezesa UKE” jest mowa w uwadze.

			3) *„czy przedsiębiorca ponosi odpowiedzialność za zastosowanie środków w przypadku zakazu Prezesa UKE?*”. Powyższe stwierdzenia pozostają aktualne. **(26.)** Do rozważenia pozostawiamy to, aby ustalić te środki w rozporządzeniu, o którym mowa powyżej.	
42.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 3 ust. 2	**Art. 3 ust. 2** Konstruując normę prawną nakładającą na przedsiębiorcę telekomunikacyjnego podejmowanie proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie projektodawca winien był wskazać w czym ma się przejawiać przedmiotowa proporcjonalność **zastosowanych środków.** **Proporcjonalność środków zastosowanych przez przedsiębiorcę telekomunikacyjnego winna być do czegoś odniesiona, winna w zapisie projektu znaleźć się jakaś miara wedle której oceniać będzie można czy proporcja wdrożonych środków została przez przedsiębiorcę zachowana, czy też nie.**	**Uwaga wyjaśniona** Środki mające na celu zapobieganie nadużyciom mają być proporcjonalne - więc zależne od wielkości podmiotu, posiadanej infrastruktury czy charakteru świadczonych usług. Przy określaniu proporcjonalnych środków można posiłkować się uznanymi międzynarodowymi standardami w zakresie zarządzania ryzykiem, np. COSO II czy ISO 31000.
43.	Związek Banków Polskich	Art. 3 ust. 2	2. Przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych, w tym działań o charakterze edukacyjnym**,** mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.	**Uwaga nieuwzględniona** W ramach środków organizacyjnych mogą mieścić się środki również o charakterze uświadamiającym użytkowników. Natomiast działania o charakterze edukacyjnym – w przeciwieństwie do innych środków, mogą być prowadzone przez różne podmioty, nie tylko

			Poza zobowiązaniem przedsiębiorców telekomunikacyjnych do podejmowania odpowiednich środków technicznych i organizacyjnych, uzasadnione jest również wskazanie inicjatyw edukacyjnych jako koniecznego elementu zapobiegania nadużyciom. Analiza przypadków nadużyć finansowych do których dochodziło w przeszłości pokazuje, że odpowiedni poziom wiedzy klientów sektora telekomunikacyjnego pozwoliłyby na uniknięcie wielu, najbardziej niekorzystnych skutków nadużyć (przede wszystkim niekorzystnych skutków finansowych).	przez przedsiębiorców telekomunikacyjnych, ale również np. przez Związek Banków Polskich czy podmioty publiczne.
44.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 4 ust. 2	**ad Art. 4. ust. 2.** CSIRT NASK na podstawie monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu. Propozycja PTI W powyższym przepisie na jego końcu, zamiast słowa ...smishingu… : *szalbierskiego esemsesa wraz z podaniem zarzutów go dotyczących.* Komentarz PTI Uważamy, iż przy każdym zablokowanym rodzaju esemesa powinny być wpisane zarzuty jego dotyczące, będące podstawą blokady. Proponowania zmiana jest związana z kolejnym przepisem z art. 5, gdyż umożliwia skuteczny sprzeciw wobec decyzji CSIRT definiującej znamiona szalbierskiego esemesa (*smishingu*).	**Uwaga nieuwzględniona** Wzorzec będzie opracowany na podstawie szeregu różnych przykładów wiadomości o charakterze smishingu. Nie jest zasadne jeszcze wskazywanie odrębnie zarzutów w stosunku do wiadomości, która w zależności od kodowania ma 160 lub 70 znaków. Proponowane rozwiązanie jest nieadekwatne.

45.	Krajowa Izba Komunikacji Ethernetowej	Art. 4-6	Smishing KIKE aktywnie wspiera propozycję monitorowania przez CSIRT NASK smishingu oraz tworzenie wzorców SMS zawierających smishing. Zwracamy jednak uwagę na kilka kwestii wymagających poprawy. Po pierwsze, przedsiębiorcy telekomunikacyjni oraz podmioty inicjujące wysyłanie SMSów A2P (integratorzy usług SMS A2P) powinni być uprawnieni do zgłaszania do CSIRT NASK SMS ze smishingiem do tworzenia wykazu wzorców w art. 4 projektowanej ustawy. Z doświadczenia członków Izby wynika, że to podmioty wysyłające SMS (przedsiębiorcy telekomunikacyjni i integratorzy SMS) szybciej wyłapują smishing niż nastąpiłoby to na podstawie zgłoszeń abonentów do CSIRT NASK, jak proponuje się w art. 4 ust. 1 projektu. Stanowczo ponownej analizy pod kątem jej proporcjonalności i celowości wymaga procedura opisana w art. 4. W szczególności: - w ust. 1 celowym byłoby rozszerzenie zakresu nadużyć, które mogą być zgłaszane CSIRT NASK także do innych nadużyć w komunikacji elektronicznej, których przedmiotem jest komunikacja SMSowa; - w ust. 2 dostęp do wykazu wzorców SMS zawierających smishing powinien mieć nie tylko przedsiębiorca telekomunikacyjny, ale też integrator SMS, który mógłby usuwać smishing zanim trafi on do sieci telekomunikacyjnej. Dzięki temu podmiot ten mógłby również korygować zlecane mu SMS A2P od jego klientów, jeśli byłyby one zbieżne z wzorami z wykazu CSIRT NASK; - w ust. 3 niejasne jest jakie informacje o wystąpieniu smishingu CSIRT NASK miałby przekazywać przedsiębiorcom telekomunikacyjnym, wraz ze wzorcem	**Uwaga częściowo uwzględniona** w zakresie otworzenia katalogu podmiotów, które sygnalizują CSIRT NASK wystąpienie smishingu **Uwaga nieuwzględniona w pozostałym zakresie** Opisany mechanizm dotyczy publikacji wzorca dla wszystkich odbiorców, a nie jego przekazania do przedsiębiorców telekomunikacyjnych. Przekazanie wzorca do przedsiębiorcy następuje niezwłocznie po jego wytworzeniu przez CSIRT NASK. W związku z tym ochrona konsumentów będzie następować w najszybszym możliwym terminie. Dopiero później wzorzec będzie dostępny publicznie. Upublicznienie wzorca równocześnie z przesłaniem go do przedsiębiorców telekomunikacyjnych mogłoby pozwolić sprawcom przestępstw natychmiast zmienić stosowane przez nich wiadomości, co przełożyłby się na zniwelowanie skuteczności projektowanego rozwiązania i tym samym godziłoby w realizację celu ustawy. W zakresie stosowania wzorca należy zauważyć, że opracowana została procedura sprzeciwu w ramach, której użytkownik będzie mógł zgłosić sprzeciw gdy jego wiadomości zostaną zablokowane jako wpisujące się w zorze. W przypadku gdy Prezes UKE uzna sprzeciw za zasadny CSIRT NASK będzie obowiązany do jego zmiany. Ta procedura będzie chroniła prawa użytkowników oraz

			wiadomości wyczerpującej znamiona smishingu i jaki byłby cel tak szerokiego informowania o wystąpieniu smishingu np. w odniesieniu do poszczególnych numerów wraz z danymi abonentów potencjalnie stanowiącymi przedmiot tajemnicy telekomunikacyjnej; - w ust. 3 niezrozumiała jest też koncepcja „wzorca" wiadomości, w szczególności czy obejmuje ona także konkretny link, który prowadził do stron służących do nadużyć. W przypadku, w którym taka informacja nie byłaby zawarta we wzorcu KIKE zwraca uwagę, że w niektórych wypadkach określenie takiego wzorca może skutkować zablokowaniem ruchu niemającego na celu popełniania nadużyć (np. standardowa informacja o paczce oczekującej na odbiór czy SMS o treści odpowiadającej autoryzacji może, ale nie musi być wykorzystywana do nadużyć). Wprowadzenie ogólnego zakazu stosowania takiego wzorca doprowadziłoby do zablokowania komunikacji o takiej treści, mogąc stanowić wręcz potencjalny i samodzielny przedmiot ataków zmierzających do ograniczenia niektórych form komunikacji; - w ust. 3 analizy pod kątem obciążenia pracy policji wymaga, czy każda informacja o wystąpieniu smishingu faktycznie winna być przekazywana Komendantowi Głównemu Policji; - w ust. 4 zaproponowany termin 14-21 dni na publikację w wykazie nowego wzorca jest okresem nie tylko niezrozumiałym (nie wiadomo która z tych dat jest właściwa i w jakiej sytuacji), ale i stanowczo zbyt długim dla tego rodzaju nadużyć. W opinii Izby publikacja stwierdzonego smishingu jako nowego wzorca powinna nastąpić w terminie maksymalnie pół godziny od jego doręczenia CSIRT NASK;	pozwoli CSIRT NASK udoskonalać wykorzystywane wzorce. To jakie informacje będzie przesyłał CSIRT NASK wraz ze wzorem będzie oceniane indywidualnie w poszczególnych przypadkach.

			- w ust. 5-6 niezrozumiałe są konsekwencje uznania co do treści zawartej we wzorcu – czy w takim wypadku dalszemu blokowaniu nie podlega wzorzec, czy konkretna wiadomość, która miała stanowić przedmiot smishingu? - w art. 5 ust. 1 dochodzi do zmiany pojęcia „wzorca" na treść, co wpływa na brak jasności przepisu, w szczególności wobec braku wskazania podmiotu, który miał uznać tę treść za wyczerpującą znamiona smishingu, - w art. 5 ust. 2 sprzeciw zawierać ma m.in. wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej, którego Prezes UKE nie zna – z CSIRT NASK otrzymuje bowiem wyłącznie treść wzorca. Cel wskazania tego numeru jest więc nieznany, - w art. 6 ust. 1 pkt 1 nie została określona forma rozpatrzenia sprzeciwu, w szczególności nie zostały poddane analizie konsekwencje związane z obciążeniem Prezesa UKE oraz sądów pracą związaną z rozpatrywaniem sprzeciwów w formie decyzji. Jest też więcej niż racjonalnym, by działanie to było poprzedzone wezwaniem właściwego przedsiębiorcy telekomunikacyjnego. Niejasna jest także relacja tej procedury do procedury reklamacji, - w art. 6 ust. 2, w wyniku uwzględnienia sprzeciwu Prezes UKE przekazuje wybranym podmiotom informację, że „treść zawarta we wzorcu wiadomości nie stanowi smishingu". Informacja ta pozostaje niespójna z przedmiotem postępowania w sprawie sprzeciwu, którego istotą zdaje się być rozpatrzenie przypadku blokady konkretnego SMSa.	
46.	Polska Izba Informatyki i Telekomunikacji	Art. 4 ust. 1	**Monitorowanie smishingu przez CSIRT NASK** (art. 4 ust. 1 projektu ustawy)	**Uwaga uwzględniona w zakresie otwarcia katalogu podmiotów, które mogą przesyłać sygnały do CSIRT NASK**

			Projekt ustawy stanowi, że CSIRT NASK na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie smishingu. Nie ulega wątpliwości, że przynajmniej część sygnałów o nadużyciach NASK będzie otrzymywał do odbiorców wiadomości SMS. Niemniej jednak zasadnym wydaje się założenie, że NASK może otrzymywać sygnały o kampaniach smishingowych nie tylko od odbiorców tych wiadomości, ale również od organów ścigania, regulatora rynku telekomunikacyjnego, podmiotów zajmujących się bezpieczeństwem, instytucji publicznych i przedsiębiorców prywatnych. A skoro tak, to nieuzasadnione jest ustawowe ograniczanie CSIRT NASK tylko do jednego źródła informacji, gdyż takie rozwiązane w sposób nieuzasadniony ograniczy skuteczność działania CSIRT NASK, który powinien móc korzystać z każdego legalnego źródła informacji do identyfikowania kampanii smishingowych. W związku z powyższym zasadnym wydaje się nadanie art. 4 ust. 1 projektu ustawy następującego brzmienia: *CSIRT NASK ~~na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS)~~ monitoruje występowanie smishingu.* Alternatywnie, analizowany przepisów mógłby uzyskać następujące brzmienie: *CSIRT NASK, w szczególności na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS), monitoruje występowanie smishingu.*	
47.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 4 ust. 1 i ust. 2	**Art. 4 ust. 1 i ust. 2**	**Uwaga wyjaśniona** Monitorowanie przez CSIRT NASK występowania smishingu oraz tworzenie

			Realizacja przedsięwzięć określonych w art. 4 projektu będzie związana z bardzo poważną ingerencją w prywatność wszystkich osób przesyłających krótkie wiadomości tekstowe (SMS), nie tylko tych, wobec których podejmowane będą próby smishingu. Odbiorcy SMS (co najmniej dwóch – tylko dwóch) zainicjuje monitorowanie przez CSIRT NASK występowanie smishingu. Na podstawie takiego monitorowania (może lepiej będzie brzmiało: po analizie wyników monitorowania) CSIRT NASK tworzy wzorzec wiadomości. W projekcie nie wskazano podmiotów (organów) oraz narzędzi weryfikujących poprawność opracowanego przez CSIRT NASK wzorca wiadomości wyczerpującej znamiona smishingu. Jedynymi przesłankami umożliwiającymi uznanie wiadomości SMS jako smishing są te, które zostały zawarte w definicji smishingu (art. 3 ust. 1 pkt 2 projektu). Wobec bardzo ogólnych przesłanek, na podstawie których kwalifikuje się zdarzenie jako nadużycie w komunikacji elektronicznej CSIRT NASK otrzymuje ustawowe prawo dużej swobody w tworzeniu wzorca wiadomości wyczerpującej znamiona smishingu. **Należałoby zatem postulować wskazanie w projekcie niezależnego podmiotu lub organu uprawnionego do zatwierdzania stworzonego przez CSIRT NASK wzorca wiadomości wyczerpującej znamiona smishingu, którego decyzja dopiero pozwalałaby na opublikowanie przedmiotowego wzorca wiadomości wyczerpującej znamiona smishingu w sposób określony w art. 4 ust. 4**	wzorców wiadomości smishingowych ma charakter czynności technicznych. Poprzez procedurę sprzeciwu zapewnia się możliwość zmiany wzorca wiadomości. W projekcie została przewidziana procedura w ramach, której wzorzec będzie ulepszany. Zapewni to nie tylko ochronę praw użytkowników, ale pozwoli ulepszyć wzorzec tak aby lepiej pełnił swoją rolę.

			projektu, względnie stanowiłaby przeciwwskazanie do dokonania tego rodzaju publikacji obligując zarazem CSIRT NASK do poprawy, czy też przeróbki wzorca wiadomości wyczerpującej znamiona smishingu. Jest to o tyle istotne, gdyż rzeczywiste zwalczanie smishingu, w sposób określony w projekcie będzie realizowane przez przedsiębiorcę telekomunikacyjnego kierującego się wzorcem wiadomości wyczerpującej znamiona smishingu opracowanym przez CSIRT NASK (art. 4 ust. 6 pkt. 1 projektu), a zupełnie wyjątkowo wedle subiektywnego przekonania przedsiębiorcy telekomunikacyjnego dokonywanego w oderwaniu od przedmiotowego wzorca (art. 7 projektu).	
48.	Polska Izba Informatyki i Telekomunikacji	Art. 4 ust. 4	**Publikowanie wzorców smishingowych** Projektowany art. 4 ust. 4 zakłada, że CSIRT NASK będzie publikował na swojej stronie internetowej wzorce wiadomości smishingowych. W naszej ocenie przepis ten powinien zostać usunięty z projektu ustawy, gdyż wzorce nie powinny być publikowane ze względów bezpieczeństwa. Opublikowane wzorce mogą stanowić dla przestępców wskazówki zarówno co do metodologii działania CSIRT NASK jak i sposobu blokowania takich wiadomości przez przedsiębiorców telekomunikacyjnych, co może służyć do opracowywania metod obchodzenia stosowanych rozwiązań anty-smishingowych.	**Uwaga nieuwzględniona** Jawność wzorca wiadomości smishingowej jest niezbędna dla zapewnienia przejrzystości procesu blokowania wiadomości a także jest niezbędne dla zagwarantowania praw użytkowników i możliwości skorzystania z instytucji sprzeciwu przez nadawcę wiadomości, która została zablokowana jako wpisująca się we wzorzec.
49.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 4 ust. 4	**Art. 4 ust. 4** Przedmiotowa regulacja wymaga dokonania precyzyjnej korektury.	**Uwaga częściowo uwzględniona** Przepis zostanie doprecyzowany aby jasno wskazywał, że CSIRT NASK publikuje wzorzec nie wcześniej niż po 14 dniach (i nie później

			O ile określenie terminu końcowego udostępnienia przez CSIRT NASK wzorca wiadomości wyczerpującej znamiona smishingu nie nastręcza nadmiernych trudności (21 dni od dnia przekazania wzorca przedsiębiorcy telekomunikacyjnemu w sposób określony w ust. 3), to już określenie początkowego terminu publikacji tegoż wzorca w rzeczywistości jest zawieszone w prawnej próżni. W sytuacji gdy projektodawca podaje, że wzorzec zostaje udostępniony na stronie internetowej CSIRT NASK w terminie 14 dni, nie później jednakże niż 21 dni od dnia przekazania wzorca przedsiębiorcy telekomunikacyjnemu w sposób określony w ust. 3 termin początkowy winien być do czegoś odniesiony. Tymczasem w proponowanej regulacji nie wiemy w odniesieniu do jakiegoż momentu w czasoprzestrzeni należy odnieść ten termin 14- dniowy, czy termin ten liczony jest od dnia stworzenia przez CSIRT NASK przedmiotowego wzorca(akurat tak określony moment byłby trudny do zweryfikowania), czy też liczony jest od przekazania wzorca przedsiębiorcy telekomunikacyjnemu w sposób określony w art. 4 ust. 3 projektu. Od razu należy wskazać, że w przedmiotowym przepisie tak naprawdę jedynym istotnym terminem jest termin końcowy publikacji wzorca, bo ten termin początkowy w tego rodzaju regulacji prawnej pozbawiony jest jakiegokolwiek znaczenia, skoro istotne jest by ten wzorzec opublikować w terminie 21 dni od dnia udostepnienia przedsiębiorcy w sposób opisany w art. 4 ust. 3 projektu.	niż 21 dni) od przekazania wzorca za pomocą systemu teleinformatycznego.

			Inna sprawa to ta, że przedmiotowa norma pozbawiona jest jakiegokolwiek „ostrza”, bo co się stanie jeśli CSIRT NASK nie zachowa terminu ustawowego opublikowania na swojej stornie internetowej przedmiotowego wzorca. Czy w takim przypadku np. publikując wzorzec przed 14 dniem liczonym od nie wiadomo jakiego momentu, czy też po upływie 21 dnia od przekazania przedsiębiorcy telekomunikacyjnemu tegoż wzorca w sposób określony w art. 4 ust. 3 projektu wzorzec nie nabędzie mocy obowiązującej i nie będzie wywoływał skutków prawnych związanych z jego opublikowaniem, a zatem nie będzie mógł stanowić podstawy do blokowania SMS-ów, czy tez uchybienie temu terminowi wywoła inne skutki prawne, których projektodawca nam niestety nie ujawnia. W takim przypadku możnaby wprowadzić regulację przewidującą, iż w razie uchybieniu terminowi publikacji wzorca CSIRT NASK byłby zobowiązany do zapłaty kary administracyjnej w wysokości 1 mln zł na Fundusz Cyberbezpieczeństwa. W tym miejscu z przykrością należy stwierdzić, że projektodawca przewidując kary administracyjne o charakterze pieniężnym w art. 15 i art. 16 projektu nie przewiduje kary nakładanej na CSIRT NASK w razie uchybienia terminowi opublikowania wzorca wiadomości wyczerpującej znamiona smishingu, przewidując jedynie kary nakładane na przedsiębiorców telekomunikacyjnych. **Podsumowując tę część rozważań na okoliczność niewskazania w projekcie jakichkolwiek skutków prawnych związanych z uchybieniem przez CSIRT NASK terminowi opublikowania wzorca wiadomości**	

			wyczerpującej znamiona smishingu proponujemy w art. 4 ust. 4 projektu ograniczyć regulację jedynie do wskazania, że przedmiotowy wzorzec CSIRT NASK opublikuje na swojej stronie internetowej bez określania terminu początkowego oraz końcowego dokonania publikacji albowiem w proponowanej wersji przepisu terminy te pozbawione są jakiegokolwiek znaczenia prawnego. **Jeżeli natomiast w projekcie projektodawca zdecyduje się na wprowadzenie regulacji przewidującej lub przewidujących skutki prawne powiązane z zachowaniem przez CSIRT NASK terminu publikacji przedmiotowego wzorca, wówczas proponujemy usunięcie terminu początkowego przewidzianego w art. 4 ust. 4 projektu, a pozostawienie wyłącznie terminu końcowego, do którego przedmiotowy wzorzec winien zostać opublikowany albowiem w proponowanej obecnie regulacji ten termin początkowy, w dodatku liczony od bliżej nieokreślonego momentu w czasoprzestrzeni, nie odgrywa jakiejkolwiek prawem określonej roli.**	
50.	Związek Banków Polskich	**Art. 4 ust. 6 pkt 3**	**3) poinformowania podmiotu, pod który podszywa się nadawca wiadomości, o której mowa w ust. 3. W przypadku podszycia się pod podmiot, o którym mowa w art. 106d ust. 1 lub 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.) przedsiębiorca telekomunikacyjny jest zobowiązany do poinformowania centrum wymiany i analizy informacji utworzone na podstawie art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.);**	**Uwaga nieuwzględniona** w związku z nieuwzględnieniem uwagi o zmianach w Prawie bankowym.

			Kluczowe dla przeciwdziałania skutkom nadużycia w komunikacji elektronicznej jest niezwłoczne poinformowanie o fakcie smishingu lub spoofingu podmiotu, pod który podszywają się przestępcy. Tego rodzaju działanie pozwala na odpowiednio wczesne ostrzeżenie klientów (w przypadku przedsiębiorcy), co jest szczególnie istotne w przypadku klientów sektora finansowego. Banki oraz FinCERT.pl – BCC ZBP niezwłocznie po zidentyfikowaniu takich zagrożeń opracowują ostrzeżenia, które są propagowane używanymi kanałami komunikacji z klientami. Przekazanie tych informacji do centrum wymiany i analizy informacji dla sektora finansowego – FinCERT.pl – BCC ZBP ma istotne znaczenie w kontekście poinformowania innych instytucji o prowadzonych kampaniach przestępczych.	
51.	Związek Telewizji Kablowych Izba Gospodarcza	**Art. 4 ust. 6 pkt 1, art. 7**	Proponowana wersja przedmiotowego przepisu razi małą precyzyjnością z czym nie możemy mieć do czynienia w przypadku przepisów, które wdrażane są w celach zapewnienia bezpieczeństwa w komunikacji elektronicznej. Określenie bowiem zawarte w tym przepisie nakładające na przedsiębiorcę telekomunikacyjnego obowiązek „niezwłocznego” blokowania SMS-ów zawierających treści zawarte we wzorcu prowadzi do stosowania pojęcia niedookreślonego, stanowiącego autostradę wręcz do różnorakich interpretacji. W sprawach cywilnych wedle ukształtowanych od lat w orzecznictwie sadowym zapatrywań niezwłoczność	**Uwaga wyjaśniona** W przypadku tej regulacji nie należy wykładać pojęcia „niezwłoczności” jako 14 dni tak jak jest to wyrażone w niektórych liniach orzeczniczych sądów powszechnych do art. 455 Kodeksu cywilnego. Mamy tutaj do czynienia z przepisami prawa administracyjnego, a nie prawa prywatnego. Zostanie wyjaśnione w uzasadnieniu, że niezwłoczność należy rozumieć w ten sposób, że przedsiębiorca telekomunikacyjny będzie obowiązany zablokować wiadomości smishingowe najszybciej jak będzie mógł, a więc z zachowaniem zasady *impossibilium nulla obligatio est*.

			podjęcia jakiegoś działania określano na termin 14-dniowy. W przypadku czynów zabronionych w telekomunikacji określonych w art. 3 ust. 1 pkt. 2 projektu termin 14-dniowy na zablokowanie SMS-a wyczerpującego znamiona smishingu określone we wzorcu wydaje się terminem zbyt długim i trudnym do wdrożenia w praktyce. Aby prawidłowo zastosować przedmiotowy przepis oznaczałoby to, że przedsiębiorca telekomunikacyjny przez okres nie dłuższy niż 14 dni uprawniony by był przetrzymywać wszystkie wysłane w jego sieci SMS-y, aby w tym okresie sprawdzić, czy nie spełniają one znamion smishingu określonych we wzorcu i jeśli nie spełniają to przed upływem 14 dnia od jego zatrzymania musiałby go puścić dalej, a jeśli spełniają wówczas byłby obowiązany z nastaniem 14 dnia od zatrzymania SMS- a dokonać jego zablokowania. Regulacja taka wydaje się wręcz absurdalna, zaś zatrzymywanie wszystkich SMS-ów wysłanych w sieci telekomunikacyjnego danego operatora przez okres nie dłuższy niż 13 dni jeśli nie spełniają znamion smishingu oraz ich blokowanie z 14 dniem od ich zatrzymania w przypadku, gdy spełniają znamiona smishingu w zasadzie przeczy instytucji krótkiej wiadomości tekstowej albowiem żaden abonent nie będzie zainteresowany korzystaniem z usługi odnośnie której będzie wiedział, że wysłana wiadomość do adresata może dotrzeć np. w 13 dniu od wysłania i wszystko w takim przypadku będzie znajdowało oparcie w obowiązującym prawie.	Wskazać również należy, że opóźnienie blokowania wiadomości smishingowych może spowodować straty wizerunkowe po stronie przedsiębiorcy telekomunikacyjnego, ponieważ mimo tego, że wiedział o złośliwych wiadomościach to zezwolił na ich przesłanie co naraża jego klientów na ryzyko strat.

			Takie rozwiązanie jest wręcz niebezpieczne albowiem możemy sobie wyobrazić sytuację, że turysta spada zimą w przepaść i łamie nogę i wysyła do TOPR-u lub GOPR-u sms- a z prośbą o pomoc lub ratunek, który przez 13 dni jest przetrzymywany przez przedsiębiorcę telekomunikacyjnego celem przeanalizowania czy rzeczona wiadomość nie spełnia znamion smishingu i dopiero z 13 dniem zgodnie z prawem przedsiębiorca telekomunikacyjny puszcza tego sms-a do TOPR-u lub GOPR-u. W takiej sytuacji niewątpliwie ratownicy górscy winni ze sobą wziąć jedynie worek na zwłoki, bo sprzęt medyczny nie będzie już do niczego przydatny. **W projekcie i to tak w art. 4 ust. 6 pkt. 2 w odniesieniu do dokonania przez przedsiębiorcę telekomunikacyjnego oceny czy SMS spełnia znamiona smishingu określone we wzorcu, jak i w art. 7 w odniesieniu do dokonania przez przedsiębiorcę telekomunikacyjnego oceny czy SMS spełnia znamiona smishingu określone w art. 3 ust. 1 pkt. 2 projektu nieujęte we wzorcu opublikowanym przez CSIRT NASK na stronie internetowej CSIRT NASK należy określić maksymalny, stosunkowo krótki okres czasu liczony w minutach, w którym przedsiębiorca może dokonać oceny, a na jej podstawie dokonać decyzji o zablokowaniu SMS- a lub też o jego puszczeniu dalej do adresata.**	
52.	IAB Polska	Art. 5, Art. 6	**UWAGA:** W Art. 5 UZNKE zostało uregulowane prawo nadawcy krótkiej wiadomości tekstowej (SMS) do wniesienia sprzeciwu do Prezesa UKE wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu.	**Wyjaśnienie** Rozpatrzenie sprzeciwu nie następuje w drodze decyzji administracyjnej i nie wymaga zachowania szczególnej formy. Jest to w ocenie projektodawcy tzw. inna czynność z

			Z przepisów UZNKE **nie wynika, w jakim trybie jest rozpatrywany sprzeciw Prezesa UKE**, m.in. przy uwzględnieniu przepisów jakiej procedury powinna być badana przez Prezesa UKE zasadność sprzeciwu złożonego przez nadawcę SMS, jaką formę prawną przybiera rozstrzygnięcie Prezesa UKE uwzględniające lub nieuwzględniające sprzeciwu lub czy nadawca, który nie jest zadowolony z rozstrzygnięcia Prezesa UKE, mam możliwość zakwestionowania zasadności i legalności takiej decyzji, dzięki instancji odwoławczej. **PROPOZYCJA:** Projektodawca powinien doprecyzować tę kwestię, m.in. określić, czy Prezes UKE powinien stosować przepisy postępowania administracyjnego przy podejmowaniu decyzji o uwzględnieniu sprzeciwu, jaką formę prawną powinny przyjąć rozstrzygnięcia podejmowane w tej kwestii przez Prezesa UKE i czy istnieje możliwość badania zasadności i legalności tych rozstrzygnięć.	zakresu administracji publicznej, która podlega kontroli sądu administracyjnego.
53.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 5	**ad Art. 5. ust. 1.** Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu. **ust. 2.** Sprzeciw zawiera: 1) uzasadnienie wyjaśniające dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu; <u>Komentarz PTI</u> W przypadku zaakceptowania propozycji PTI powyżej do art. 4 ust. 2 powyższy przepis nie budzi wątpliwości. Jednakże pozostawienie takiej treści art. 5.1 i 2 bez proponowanej zmiany PTI w art. 4 ust. 2 spowoduje, iż nie będzie możliwe skuteczne sprzeciwienie się zarzutowi	**Uwaga wyjaśniona** Przepisy ustawy wyraźnie wskazują, że użytkownicy będą mogli zgłaszać sprzeciw do Prezesa UKE i przez to wskazywać, że wzorzec przygotowany przez NASK jest niedoskonały. W przypadku gdy prezes UKE uwzględni sprzeciw, CSIRT NASK będzie musiał zmienić swój wzorzec. Będzie to skuteczny sposób podważania wzorca smishingu. Ponadto, zmiana wzorca będzie mogła nastąpić w trybie autokontroli przez CISRT NASK (przedsiębiorcy telekomunikacyjnemu w sposób, o którym mowa w ust. 3. 6. CSIRT NASK, w przypadku gdy uzna, że:

			szalbierstwa w esemesie (smishingu), ponieważ nie będą jawne wskazane (nie będą ogłoszone) zarzuty uzasadniające blokadę. Byłoby to sprzeczne z jedną spośród zasad prawodawstwa, iż wymagane może być tylko prawo ogłoszone.	1) treść zawarta we wzorcu wiadomości nie stanowi smishingu, lub 2) niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zgodnych ze wzorcem wiadomości niezwłocznie - informuje o tym podmioty, o których mowa w ust. 3 oraz zamieszcza na stronie internetowej informacje o okresie w jakim wzorzec obowiązywał).
54.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 5 ust. 1	**Art. 5 ust. 1** Przedmiotowa regulacja budzi uzasadnioną wątpliwość natury prawnej. Projektodawca uznał, że sprzeciw winien być wnoszony od uznania treści krótkiej wiadomości tekstowej za wyczerpującą znamiona smishingu, gdy tymczasem rzeczywistym powodem jego wniesienia przez nadawcę SMS- a jest zablokowanie krótkiej wiadomości tekstowej przez przedsiębiorcę telekomunikacyjnego, a nie powody dokonania blokady (art. 4 ust. 6 pkt. 1 projektu, art. 7 projektu). Mało tego, można sobie przecież wyobrazić sytuację, że przedsiębiorca telekomunikacyjny, mimo iż uznał, że krótka wiadomość tekstowa spełnia znamiona smishingu, a jednak nie zdecydował się na jej zablokowanie. O ile sytuacja taka zupełnie wyjątkowo może zaistnieć w przypadku SMS- a spełniającego znamiona smishingu określone we wzorcu takiej wiadomości, gdyż w takim przypadku przedsiębiorca telekomunikacyjny zobowiązany jest do zablokowania takiej wiadomości (art. 4 ust. 6 pkt. 1 projektu), to już w przypadku krótkiej	**Uwaga wyjaśniona** Nadawca będzie mógł zgłosić sprzeciw od zablokowania sms wobec zablokowania krótkiej wiadomości tekstowej (SMS) zawierającej treści zawarte we wzorcu wiadomości. W zakresie stosowania wzorca należy zauważyć, że opracowana została procedura sprzeciwu w ramach, której użytkownik będzie mógł zgłosić sprzeciw gdy jego wiadomości zostaną zablokowane. W przypadku gdy Prezes UKE uzna sprzeciw za zasadny CSIRT NASK będzie obowiązany do jego zmiany. Ta procedura będzie chroniła prawa nadawcy oraz pozwoli CSIRT NASK udoskonalać wykorzystywane wzorce. Sprzeciw nie będzie przysługiwał od zablokowania wiadomości przez przedsiębiorcę telekomunikacyjnego w związku z uzupełniającym uprawnieniem (art. 7 projektu). W przypadku zablokowania na tej podstawie użytkownik końcowy będzie mógł skorzystać m.in. z reklamacji.

			wiadomości tekstowej spełniającej znamiona smishingu określone w art. 3 ust. 1 pkt. 2 projektu nie objęte jednakże wzorcem opublikowanym na stronie internetowej CSIRT NASK taka sytuacja może wręcz stanowić prawidłowość, gdyż wolą projektodawcy w takim przypadku od woli przedsiębiorcy telekomunikacyjnego zależy czy taką wiadomość zablokuje, czy też nie, skoro projektodawca na taką okoliczność przyznał przedsiębiorcy telekomunikacyjnemu prawo, a nie obowiązek(jak w art. 4 ust. 6 pkt. 1 projektu) blokowania takich wiadomości (art. 7 projektu). Jeżeli zatem krótka wiadomość tekstowa zostanie uznana za spełniającą znamiona smishingu, ale przez przedsiębiorcę telekomunikacyjnego nie zostanie zablokowana, to w takim przypadku zupełnie bezprzedmiotowe staje się przyznanie nadawcy SMS-a uprawnienia do wniesienia sprzeciwu, skoro SMS nie został zablokowany. Mało tego, w takim przypadku regulacja art. 5 ust. 1 projektu przyznająca nadawcy SMS-a prawo do wniesienia sprzeciwu do Prezesa UKE, mimo niezablokowania SMS- a spełniającego znamiona smishingu kłóci się z pojęciem strony uregulowanym w art. 28 k.p.a. albowiem trudno byłoby przyznać w postępowaniu administracyjnym status strony nadawcy SMS-a, który nie został zablokowany, mimo spełnienia znamion smishingu, gdyż tenże nadawca nie posiadałby żadnego interesu prawnego w zaskarżeniu uznania krótkiej wiadomości tekstowej za spełniającą znamiona smishingu, w sytuacji, gdyby przedsiębiorca telekomunikacyjny nie zablokował tegoż SMS-a.	Do instytucji sprzeciwu nie będą stosowane przepisy KPA.

			Regulację art. 5 ust. 1 projektu uznać należy za wadliwą jeszcze z jednego powodu, a mianowicie z uwagi na jej nieracjonalność. W jakiej bowiem sytuacji zdaniem projektodawcy dojdzie do powzięcia przez nadawcę krótkiej wiadomości tekstowej wiedzy o tym, iż przedsiębiorca telekomunikacyjny uznał nadanego SMS-a za wyczerpujący znamiona smishingu, skoro nie doszło do zablokowania jego wysyłki. Nie posiadając zaś wiedzy o uznaniu SMS-a za spełniający wymogi smishingu wobec jego niezablokowania nadawca tejże wiadomości nie mógłby wnieść sprzeciwu, skoro nie wiedziałby o dokonaniu takiej oceny przez przedsiębiorcę telekomunikacyjnego. **W kwestionowanej zatem regulacji przedmiotem sprzeciwu wnoszonego do Prezesa UKE nie powinno być uznanie treści SMS-a za wyczerpującą znamiona smishingu, ale zablokowanie przez przedsiębiorcę telekomunikacyjnego krótkiej wiadomości tekstowej z powodu uznania rzeczonej wiadomości przez przedsiębiorcę telekomunikacyjnego za spełniającą znamiona smishingu**.	
55.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 5 ust. 2 pkt 2	**VI. [TREŚĆ SPRZECIWU – ART. 5 UST. 2 PKT 2)]** **(27.)** W tym zakresie wskazano, że wymaganiem koniecznym (brakiem formalnych) jest *„wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS)*”. **(28.)** Zwracamy uwagę, że często wiadomość SMS może nie być identyfikowana przez numer, ale nazwę. Na	**Uwaga nieuwzględniona** Obecne regulacje dotyczące sprzeciwu są uregulowane w taki sposób aby umożliwić skuteczne wniesienie sprzeciwu. Sprzeciw dotyczy wiadomości, która została zablokowana ze względu na wpisanie się we wzorzec wiadomości wyczerpującej znamiona smishingu, a więc będzie zgłaszany przez wysyłającego wiadomość. Wysyłający zna

			przykład alerty są opisywane nie numerem ale nazwą (np. „ALERT RCB”). **(29.)** W konsekwencji jak się wydaje ten element sprzeciwu powinien brzmieć *„wskazanie numeru lub nazwy wykorzystanej do nadania krótkiej wiadomości tekstowej (SMS)*”.	numer, który wykorzystywał a więc nie dojdzie do sytuacji w której zgłaszający sprzeciw nie będzie znał wykorzystywanego numeru. Nie jest więc konieczne wprowadzanie proponowanej zmiany.

56.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 5 ust. 3	**Art. 5 ust. 3** Zdecydowanie należy sprzeciwić się wymogowi opatrywania sprzeciwu podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnoszeniu tegoż sprzeciwu za pomocą środków komunikacji elektronicznej. Wyobraźmy sobie 100- letniego pana, który jako tako radzi sobie z komórką i mieszka w Bieszczadach lub innych wysokich górach, gdzie dostęp do Internetu jest iluzoryczny, czy wręcz żaden. Czy autorzy projektu oczekują, że ten 100- letni starszy pan posiada wyrobiony jakikolwiek podpis elektroniczny którego brak pozbawia jego osobę możliwości wniesienia sprzeciwu przeciwko uznania treści jego krótkiej wiadomości tekstowej nadanej do wnuczki za spełniającą znamiona smishingu. Co więcej, projektodawca oczekuje od tego 100- letniego starszego pana umiejętności korzystania ze środków komunikacji elektronicznej, bo tylko tą drogą można wnieść sprzeciw do Prezesa UKE. Mało tego, gdyby nawet ten 100- letni starszy pan zamieszkujący w wysokich górach jakimś cudem zadbał o posiadanie jakiegokolwiek podpisu elektronicznego i w dodatku posiadł umiejętność korzystania ze środków komunikacji elektronicznej (chyba wszyscy czujemy, że są to założenia mało prawdopodobne do zaistnienia), to w sytuacji gdy zamieszkuje w tych wysokich górach będąc osobą mocno schorowaną nie ma żadnych szans wysłania sprzeciwu przy wykorzystaniu środków komunikacji elektronicznej, gdyż środki te w tamtym terenie po prostu nie działają z uwagi na brak dostępu do Internetu, a	**Uwaga nieuwzględniona** Uprawnionym do wniesienia sprzeciwu jest nadawca wiadomości, która została zablokowana w zw. z zastosowaniem wzorca wiadomości wyczerpującej znamiona smishingu. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Profil zaufany to bezpłatna metoda potwierdzania tożsamości obywatela w systemach podmiotów publicznych. Można za jego pomocą zalogować się do takiego systemu, a w razie takiej potrzeby złożyć podpis elektroniczny (podpis zaufany), który wobec podmiotów publicznych jest równie skuteczny jak podpis własnoręczny. Podpis osobisty to zaawansowany podpis elektroniczny związany z e-dowodem (dowodem osobistym z warstwą elektroniczną). Prawdziwość danych posiadacza podpisu potwierdza certyfikat podpisu osobistego, zawierający imię (imiona), nazwisko, obywatelstwo oraz numer PESEL. Aby certyfikat podpisu osobistego znalazł się w e-dowodzie, należy wyrazić na to zgodę podczas składania wniosku o nowy dokument. Wprowadzenie takiego rozwiązania dla którego komunikacja z urzędem odbywa się drogą elektroniczną jest rozwiązaniem proporcjonalnym i adekwatnym. Pozwala jednoznacznie i w prosty sposób zidentyfikować personalia osoby wnoszącej

			trudno oczekiwać, by ten pan mieszkając w 200- letniej drewnianej chałupie posiadał tam dostęp do Internetu satelitarnego. Należy zważyć, że Prezes UKE rozpoznając sprzeciw wydaje decyzję administracyjną (art. 104 1 k.p.a. w zw. z art. 206 ust. 1 prawa telekomunikacyjnego). Ponieważ decyzja w przedmiocie rozpoznania sprzeciwu nie należy do grupy decyzji wymienionych w art. 206 ust. 2 prawa telekomunikacyjnego, przeto od decyzji w przedmiocie rozpoznania sprzeciwu nie wnosi się odwołania do Sądu Ochrony Konkurencji i Konsumentów lecz zaskarżając ją składa się wniosek o ponowne rozpoznanie sprawy przez Prezesa UKE (art. 127 § 3 k.p.a. w zw. z art. 5 § 2 pkt. 4 k.p.a. w zw. z art. 206 ust. 1 prawa telekomunikacyjnego). Oznacza to, iż od decyzji wydanej przez Prezesa UKE w przedmiocie rozpatrzenia wniosku o ponowne rozpatrzenie sprawy zaskarżającego decyzję w przedmiocie rozpoznania sprzeciwu strona postępowania może zaskarżyć do Wojewódzkiego Sądu Administracyjnego w Warszawie stosowną skargą[art. 3 § 2 pkt. 1 ustawy z dnia 30.08.2002 r. prawo o postepowaniu przed sądami administracyjnymi (tekst jedn .Dz. U. z 2022 r. poz. 329 z późn. zm.), zwanej dalej p.p.s.a.]. W przedstawionym przez nas stanie faktycznym, a przecież porównywalnych stanów faktycznych może być o wiele więcej, projektodawca art. 5 ust. 3 pozbawia obywatela będącego nadawcą krótkiej wiadomości tekstowej konstytucyjnie mu przysługującego prawa do sądu albowiem skoro nie wniesie on sprzeciwu, bo nie	sprzeciw, co zmniejszy możliwość obstrukcji organu oraz możliwość podważania wzorców przez osoby, które podszywałyby się pod nadawcę, oraz zapewni prawne procesowanie tego specyficznego postępowania. Przedmiotem tego postępowania jest zmiana wzorca ze skutkiem dla wszystkich uczestników obrotu, a nie jedynie realizowanie indywidualnych uprawnień, które są zapewnione innymi instytucjami prawnymi.

			posiada jakiegokolwiek podpisu elektronicznego, osobistego lub zaufanego lub nie włada środkami komunikacji elektronicznej, czy też przedmiotowe środki nie mogą być w jego sytuacji życiowej wykorzystane, a najczęściej wszystkie te trzy ograniczenia wystąpią łącznie, jak w podanym przez nas przykładzie. Regulacja zatem art. 5 ust. 3 projektu jako pozbawiająca potencjalną stronę postępowania administracyjnego przysługującego jej konstytucyjnego prawa do sądu przewidzianego w art. 45 ust. 1 w zw. z art. 77 ust. 2 Konstytucji Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz. U. nr 78 poz. 483 z późn. zm.), zwanej dalej Konstytucją RP, a zatem łamiąca najwyższe prawo obowiązujące w naszym kraju znajdujące bezpośrednie zastosowanie w wewnętrznym porządku prawnym (art. 8 Konstytucji RP), jako norma niekonstytucyjna ostać się nie może. Wniesienie zatem sprzeciwu winno być przez projektodawcę dopuszczone w każdej formie prawnej dopuszczonej przez przepisy k.p.a., w tym i w formie pisemnej. **W zaistniałej sytuacji proponujemy zatem skreślenie regulacji art. 5 ust. 3 projektu** albowiem formy prawne wniesienia sprzeciwu będą wówczas regulowane przez przepisy k.p.a.	
57.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 6	**VII. [FORMA PRAWNA ROZPATRZENIA SPRZECIWU]** **(30.)** Projekt nie wskazuje w jakiej formie Prezes UKE będzie rozstrzygał o zasadności sprzeciwu.	**Uwaga nieuwzględniona** Wprowadzenie decyzji administracyjnej jako instytucji prawnej wysoko sformalizowanej przy sprzeciwie od uznania SMS za smishing jest skrajnie nieadekwatne biorąc pod uwagę

			(31.) Naszym zdaniem powinna to być decyzja administracyjna (jako władcza forma działania administracji).	m.in. skalę. CSIRT NASK od kwietnia 2021 r. do końca maja 2020 r. zidentyfikował ok 31 000 złośliwych wiadomości sms. Dla przykładu załóżmy, że od 1% tych wiadomości zostałby złożony sprzeciw. Oznaczałoby to 310 postępowań administracyjnych prowadzonych przez Prezesa UKE. Byłoby to znaczne obciążenie organizacyjne dla tego organu. Co istotne, odformalizowana procedura sprzeciwu zapewni szybkość procedowania sprawy.
58.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 6 ust. 1 pkt 1	**Art. 6 ust. 1 pkt. 1** Trudno doprawdy zrozumieć czemu ma służyć określenie terminu 14- dniowego na rozpatrzenie sprzeciwu przez Prezesa UKE w stosunku do podstawowego terminu na rozpoznanie sprawy przez organ administracji publicznej wynoszący jeden miesiąc (art. 35 § 3 in principio k.p.a.). Tym bardziej regulacja ta pozbawiona jest jakiegokolwiek znaczenia, skoro jeśli Prezes UKE uzna sprawę za szczególnie skomplikowaną, wówczas w świetle regulacji art. 35 § 3 k.p.a. może uznać, że ma na jej rozpoznanie 2 miesiące. Ponadto należy podkreślić, że organ administracji publicznej, zwany dalej o.a.p., w przypadku niezałatwienia sprawy administracyjnej w terminie ustawowym obowiązany jest jedynie informację o niezałatwieniu sprawy w terminie przekazać do strony postepowania informując zarazem o przyczynach zwłoki w jej załatwieniu(z winy organu) lub też nawet wówczas, gdy uchybienie terminowi załatwienia sprawy nastąpiło z przyczyn od organu niezależnych (art. 36 k.p.a.).	**Wyjaśnienie** Wskazanie 14 dni na rozpatrzenie sprawy jest motywowane faktem, że sprzeciw nie ma charakteru decyzji administracyjnej, a więc nie będą stosowały się do niego przepisy KPA. Wprowadzenie instytucji zbliżonej do „milczącej zgody" mogłoby doprowadzić do sytuacji, że organ w przypadku wystąpienia dużej liczby sprzeciwów mógłby w sposób milczący uwzględnić sprzeciwy przestępców. Takie rozstrzygnięcie byłoby nieakceptowalne i podważałoby cel ustawy.

			W przypadku z kolei złożenia wniosku o ponowne rozpatrzenie sprawy Prezes UKE ma kolejny miesiąc na rozpatrzenie takiego wniosku (art. 35 § 3 in fine k.p.a. w zw. z art. 127 § 3 k.p.a.), a w razie niezałatwienia sprawy w terminie ustawowym Prezes UKE będzie zobowiązany do zawiadomienia storn postępowania o przyczynie niezałatwienia tej sprawy w terminie (art. 36 k.p.a.). Po rozpatrzeniu sprawy przez prezesa UKE jako przez organ odwoławczy decyzja może być zaskarżona do wojewódzkiego sądu administracyjnego(art. 3 § 2 pkt. 1 p.p.s.a.), a postępowanie sądowoadministracyjne jest postępowaniem dwuinstancyjnym(art. 176 ust. 1 Konstytucji RP). Skrócenie zatem w kwestionowanym przepisie terminu na rozpatrzenie przez Prezesa UKE sprzeciwu do 14 dni w rzeczywistości nie ma żadnego znaczenia, skoro SMS w tym czasie cały czas jest zablokowany (art. 4 ust. 6 pkt. 1 projektu, art. 7 projektu). **Termin 14- dniowy na rozpatrzenie sprawy przez Prezesa UKE miałby jakikolwiek sens, gdyby z niezałatwieniem sprawy w terminie projektodawca powiązałby określone skutki prawne, przykładowo wskazując pod postacią obowiązku odblokowania SMS- a przez przedsiębiorcę telekomunikacyjnego lub też uznania z mocy prawa wniesionego przez nadawcę SMS- a sprzeciwu za uzasadniony**. Takie jak ostatnio zaproponowane rozwiązanie nie byłoby odosobnione na gruncie prawa polskiego albowiem w art. 44 ust. 7 ustawy z dnia 29.12.1992 r. o radiofonii i telewizji (tekst jedn. Dz. U. z 2020 r. poz. 805 z późn. zm.), zwanej dalej ustawą o rtv, ustawodawca przewiduje, że jeżeli	

			Przewodniczący Krajowej Rady Radiofonii i Telewizji w terminie miesiąca od dnia zgłoszenia nie odmówił rejestracji programu rozprowadzanego w rejestrze programów telewizyjnych nadawanych wyłącznie w systemie teleinformatycznym oraz programów rozprowadzanych, wówczas operator może legalnie rozpocząć rozprowadzanie takiego programu.	
59.	Związek Telewizji Kablowych Izba Gospodarcza	Art.. 6 ust. 1 pkt 2	**Art. 6 ust. 1 pkt 2** Odnośnie przedmiotowej regulacji wskazać należy, że skoro Prezes UKE rozpoznając sprzeciw wydaje decyzję administracyjną (art. 104 § 1 k.p.a. w zw. z art. 206 ust. 1 prawa telekomunikacyjnego), to na zupełnym nieporozumieniu zasadza się wprowadzanie w kwestionowanym przepisie jakiejś odrębnej, poza doręczeniem decyzji administracyjnej, informacji o sposobie rozpatrzenia sprzeciwu. I tak istotne w tej sprawie nie będzie doręczenie tego rodzaju pozbawionej skutków prawnych informacji lecz doręczenie ostatecznej decyzji administracyjnej wydanej po rozpoznaniu wniosku o ponowne rozpatrzenie sprawy lub niezaskarżonej tymże środkiem odwoławczym z art. 127 § 3 k.p.a., natomiast w przypadku wniesienia skargi do sądu administracyjnego na ostateczną decyzję Prezesa UKE istotne będzie dopiero wydanie wyroku prawomocnego, którym może być w razie wniesienia skargi kasacyjnej wyrok Naczelnego Sądu Administracyjnego, a co najmniej wyrok Wojewódzkiego Sądu Administracyjnego w warszawie.	**Wyjaśnienie** Do sprzeciwu nie będą stosowane przepisy KPA.

			Z przytoczonych powyżej względów natury prawnej z uwagi na pozbawioną jakiegokolwiek znaczenia prawnego informację uregulowaną w art. 6 ust. 1 pkt. 2 projektu proponujemy wykreślenie normy art. 6 ust. 1pkt. 2 projektu jako normy pozbawionej jakiegokolwiek znaczenia prawnego regulującej sytuację prawnie nieistotną.	
60.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 6 ust. 2	**Art. 6 ust. 2** Regulacja art. 6 ust. 2 projektu budzi kilka wątpliwości natury prawnej. Po pierwsze, przewiduje iż w przypadku uwzględnienia sprzeciwu przez Prezesa UKE CSIRT NASK przekazuje informację o tym, że treść zawarta we wzorcu wiadomości stworzonym przez CSIRT NASK nie stanowi smishingu lub że niecelowe jest dalsze blokowanie SMS-ów zgodnie z wzorcem opracowanym przez CSIRT NASK. Regulacja taka jest o tyle zaskakująca, że o ile można by ją uznać za uzasadnioną w sytuacji, gdy sprzeciw został wniesiony z tego powodu, że krótka wiadomość tekstowa została uznana za spełniającą znamiona smishingu zgodnie z wzorcem opracowanym przez CSIRT NASK (art. 4 ust. 6 pkt. 1 projektu), o tyle zupełnie niezrozumiałe jest przekazywanie tego rodzaju informacji przez CSIRT NASK w sytuacji gdy przedsiębiorca telekomunikacyjny zablokował SMS- a uznając go za wyczerpującego znamiona smishingu określone w art. 3 ust. 1 pkt. 2 projektu, mimo iż nie została tego rodzaju treść SMS-a ujęta we wzorcu opracowanym przez CSIRT NASK (art. 7 projektu).	**Uwaga częściowo uwzględniona** Sprzeciw będzie przysługiwał w sytuacji, gdy przedsiębiorca telekomunikacyjny zablokował SMS zgodnie ze wzorcem. Do postępowania ws. rozpatrzenia sprzeciwu nie będą stosowane przepisy KPA. Przepisy ustawy wyraźnie wskazują, że użytkownicy będą mogli zgłaszać sprzeciw do Prezesa UKE i przez to wskazywać, że wzorzec przygotowany przez NASK jest niedoskonały. W przypadku gdy Prezes UKE uwzględni sprzeciw, CSIRT NASK będzie musiał zmienić swój wzorzec. Będzie to skuteczny sposób podważania wzorca smishingu.

			Trudno zrozumieć dlaczegóż to CSIRT NASK miałby kogokolwiek informować o uwzględnieniu sprzeciwu przez Prezesa UKE, w sytuacji gdy sprzeciw nie był wniesiony w związku z faktem, że treść SMS-a spełniała wymogi smishingu określone we wzorcu przygotowanym przez CSIRT NASK albowiem należy zauważyć, że sprzeciw wnoszony jest przez nadawcę SMS-a wobec uznania jego treści za wyczerpującą znamiona smishingu niezależnie od tego czy przedsiębiorca telekomunikacyjny opierał się w swojej ocenie na wzorcu opracowanym przez CSIRT NASK(art. 4 ust. 6 pkt. 1 projektu), czy też na definicji legalnej przewidzianej w art. 3 ust. 1 pkt.2 projektu w sytuacji nieobjęcia treści konkretnego SMS-a wzorcem opracowanym przez CSIRT NASK (art. 7 projektu)[art. 5 ust. 1 projektu]. Po drugie, skoro stronami postępowania administracyjnego wszczętego wniesionym sprzeciwem jest nadawca krótkiej wiadomości tekstowej oraz przedsiębiorca telekomunikacyjny, który uznał konkretną wiadomość za spełniającą znamiona smishingu (art. 5 ust. 1 projektu w zw. z art. 28 k.p.a.), to zupełnie niezrozumiałe jest nałożenie na CSIRT NASK obowiązku powiadomienia konkretnych podmiotów o treści informacji ujętej w art. 4 ust. 5 projektu, skoro podmiot ten nie będąc stroną postepowania administracyjnego wszczętego wniesionym sprzeciwem nie posiada żadnej wiedzy o rozstrzygnięciu takiej sprawy przez Prezesa UKE. Po trzecie wreszcie, regulację art. 6 ust. 2 projektu uznać należy także częściowo za absurdalną. Absurdalność tej regulacji zasadza się w tym, że na okoliczność uwzględnienia sprzeciwu przez Prezesa UKE nakładając na CSIRT NASK obowiązek przekazania	

			informacji określonej w art. 4 ust. 5 projektu podmiotom wymienionym w art. 4 ust. 3 projektu dochodzi do przekazania tej informacji Prezesowi UKE, który uwzględnił sprzeciw oraz przedsiębiorcy telekomunikacyjnemu, który zablokował SMS-a uznając, że spełnia wymogi smishingu określone w wadliwym wzorcu stworzonym przez CSIRT NASK, a zatem tym podmiotom, które doskonale wiedzą, że w oparciu o wzorzec opracowany przez CSIRT NASK niezasadne będzie uznawanie krótkich wiadomości tekstowej za spełniające znamiona smishingu, gdyż właśnie z tego powodu Prezes UKE sprzeciw nadawcy SMS-a uwzględnił. **Propozycja zmiany tego przepisu zmierza do:** **a/ wprowadzenia w tym przepisie obowiązku poinformowania przez Prezesa UKE CSIRT NASK o uwzględnieniu sprzeciwu od uznania przez przedsiębiorcę telekomunikacyjnego krótkiej wiadomości tekstowej za spełniającą znamiona smishingu dokonanego w oparciu o wzorzec stworzony przez CSIRT NASK,** **b/wyłączenia obowiązku przekazania przez CSIRT NASK informacji określonej w art. 4 ust. 5 projektu Prezesowi UKE oraz przedsiębiorcy telekomunikacyjnemu, który był stroną postępowania administracyjnego, w którym Prezes UKE decyzją ostateczną uwzględnił sprzeciw wniesiony przez nadawcę SMS-a**.	
61.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 7	**VIII. [BLOKOWANIE SMS WYCZERPUJĄCYCH ZNAMIONA SMISHINGU, INNE NIŻ ZAWARTE REJESTRZE – ART. 7]**	**Uwaga nieuwzględniona** W tym przypadku nie jest zasadne wprowadzanie regulacji o charakterze szczególnym. Przedsiębiorca

			(32.) Pragniemy podkreślić, że w tym zakresie Projektodawca przewidział pewną swobodę. Niemniej jednak w takim przypadku przedsiębiorca nie powinien ponosić żadnej odpowiedzialności (o charakterze publicznoprawnym ani wobec użytkowników). Wnosimy zatem o wyłączenie takich konsekwencji.	telekomunikacyjny niezasadnie blokujący SMS na podstawie art. 7 będzie podlegał odpowiedzialności kontraktowej za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej.
62.	Krajowa Izba Komunikacji Ethernetowej	Art. 7	**Izba sprzeciwia się proponowanej w art. 7 projektu regulacji w zakresie, w którym uprawnienie przedsiębiorców telekomunikacyjnych (a właściwie operatorów sieci mobilnych) do blokowania także takich SMS, które nie są zawarte we wzorcu opracowanym przez CSIRT NASK nie podlegało żadnej kontroli**. Przede wszystkim projekt ustawy nie określa żadnych środków odwoławczych od decyzji przedsiębiorcy telekomunikacyjnego ani nawet możliwości kontroli przez organy publiczne kryteriów stosowanych przez te podmioty do oceny treści. Generalnie każdy MNO będzie mógł dowolnie blokować SMS przychodzące nie tylko od jego klientów, ale przede wszystkim z sieci innych przedsiębiorców telekomunikacyjnych lub urządzeń integratorów SMS, w dodatku bez żadnej kontroli i konsekwencji. Regulacja ta spowoduje problemy z interoperacyjnością usług SMS pomiędzy podmiotami biorącymi udział w ich przesyłaniu oraz blokowanie SMS, które nie są smishingiem. Generalnie Izba zwraca uwagę, że to uprawnienie przyznane MNO stoi w sprzeczności z regulacją o roli CSIRT NASK jako instytucji monitorującej smishing i inicjującej reakcję na nowe przypadki czy z rolą Prezesa UKE jako organy decydującego czy dany SMS jest smishingiem czy nie (art. 6 projektu). Izba wskazuje, że w przypadku wątpliwości co do SMS nieodpowiadających treści wzorców CSIRT NASK, należy co najmniej	**Wyjaśnienie** Przedsiębiorca telekomunikacyjny niezasadnie blokujący SMS na w zw. z projektowanym uprawnieniem o charakterze uzupełniającym będzie podlegał odpowiedzialności kontraktowej za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej.

			przeprowadzić konsultacje robocze z podmiotem, z którego sieci/urządzenia taki SMS został wysłany, czy też zawiadomić o tym CSIRT NASK i Prezesa UKE. Izba wskazuje, że poleganie na systemach automatycznie blokujących połączenia głosowe czy przesyłanie SMS rodzi wiele nieporozumień i częstego blokowania prawidłowych usług. Z tego względu na rynku przyjęto zasadę analizy wątpliwych przypadków przez wyznaczonego pracownika przedsiębiorcy telekomunikacyjnego lub nawet spotkań roboczych w celu omówienia wątpliwości przed podjęciem decyzji o zablokowaniu kwestionowanej usługi. Proponowana w ustawie regulacja uniemożliwia „ludzką" analizę usług telekomunikacyjnych i konsultacje międzyoperatorskie lub z klientem w przypadku kwestionowanego komunikatu. Niezależnie od wprowadzenia postulowanych przez KIKE zmian wynikających z konieczności wprowadzenia nadzoru nad stosowaniem uprawnień przez przedsiębiorców telekomunikacyjnych, należy dodać zapisy o odpowiedzialności MNO za blokowanie SMS nie będących smishingiem zarówno w formie kar finansowych jak i formie odszkodowawczej. W przypadku nadużywania przez MNO uprawnienia z art. 7 projektu Prezes UKE mógłby nakazać modyfikację wykorzystywanego systemu stosującego wadliwą identyfikację smishingu. Izba wskazuje, że taką karą finansową mogłaby być 50-krotność opłaty za zablokowane SMSy niebędące smishingiem (taką stawkę stosują operatorzy w przypadku nadużycia telekomunikacyjnego związanego z podmianą numeru A abonenta wywołującego).	

63.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 7 wz z art. 4 ust. 6 pkt 1	**Art. 7 oraz art. 4 ust. 6 pkt. 1** Art. 7 projektu oraz art. 4 ust. 6 pkt. 1 projektu dają przedsiębiorcy telekomunikacyjnemu bardzo szerokie uprawnienia kontroli wszystkich SMS-ów przesyłanych w jego sieci telekomunikacyjnej i blokowania tych SMS-ów, które zdaniem przedsiębiorcy telekomunikacyjnego spełniają znamiona smishingu, czy to przewidziane we wzorcu stworzonym przez CSIRT NASK, czy też nieobjęte tym wzorcem.. Aby zidentyfikować SMS podlegający blokowaniu przedsiębiorca telekomunikacyjny za pomocą systemu informatycznego musi skontrolować („przeczytać") wszystkie SMS-y przesyłane w sieci telekomunikacyjnej, przeanalizować ich treść, ocenić ich treść pod kątem zgodności z definicją smishingu oraz ze wzorcem opracowanym, przez CSIRT NASK, a następnie zablokować te SMS, które przedsiębiorca uzna za „wyczerpujące znamiona smishingu". Wobec bardzo szerokiej i niejednoznacznej definicji smishingu zawartej w art. 3 ust. 1 pkt 2 projektu przy jednoczesnej niemożności zastosowania wzorca przedsiębiorca telekomunikacyjny może blokować SMS według własnego wzorca informacji wyczerpującej znamiona smishingu. **Poważnie należy się zastanowić, czy przyznanie przedsiębiorcy telekomunikacyjnemu tak daleko idących kompetencji ingerowania w treść wszystkich sms- ów przechodzących w jego sieci telekomunikacyjnej nie została zbyt daleko posunięta**.	**Uwaga wyjaśniona** Przepisy projektu nie zwalniają przedsiębiorcy telekomunikacyjnego z obowiązku ochrony tajemnicy telekomunikacyjnej.

64.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 8	**IV. [ŚRODKI NIEZBĘDNE W CELU ZAPOBIEGANIA CLI SPOOFINGU – ART. 8]** **(15.)** Przepis art. 8 stanowi o obowiązku blokowania połączeń głosowych. **(16.)** Wskazujemy, że **przedsiębiorcy telekomunikacyjni zrzeszeni w Izbie nie wiedzą w jaki sposób identyfikować połączenia noszące znamiona CLI spoofing**. Niezbędnym jest wypracowanie i zdefiniowanie metod identyfikacji zachowań noszących znamiona CLI spoofing. **(17.)** Otwartymi pozostają pytania: 1) czy przedsiębiorca będzie ponosił odpowiedzialność za niezasadne zablokowanie połączeń (chodzi w tym o odpowiedzialność publicznoprawną oraz wobec abonenta)? W tym kontekście w Prezentacji wskazano na następujące wątpliwości: *„co w przypadku, gdy zablokowany lub ograniczany będzie ruch legalny? Kto decyduje o jego „nielegalnym" charakterze? Czy w ogóle dokonanie takiej oceny jest możliwe?*" *„czy możliwość ograniczenia ruchu dotyczyć będzie wyłącznie pojedynczego użytkownika czy całego ruchu w przypadku jego tranzytu/roamingu?*" 2) jaki będzie nadzór Prezesa UKE nad realizacją tego obowiązku. **(18.)** Jeszcze raz powołujemy się w tym zakresie na Prezentację. MC jako argument dla krytyki jednej z propozycji Rynku wskazał, że *„definicja posługuje się nieostrymi pojęciami, brak jest wyraźnie stypizowanych i*	**Uwaga nieuwzględniona** Projektodawca proponuje, aby środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie CLI spoofing były doprecyzowane w porozumieniu zawartym a Prezesem UKE. Ten model samoregulacji ma z jednej strony zapewnić bezpieczeństwo regulacyjne dla przedsiębiorców telekomunikacyjnych, a z drugiej jest on na tyle elastyczny, aby można było dostosować środki do ciągle rozwijających się nowych technologii jak i zagrożeń. Dzięki takiemu rozwiązaniu przedsiębiorcy telekomunikacyjni wraz ze wsparciem i nadzorem UKE będą mogli wypracować najlepsze rozwiązania techniczne i organizacyjne, które pozwolą im zwalczać nadużycia w komunikacji elektronicznej. Bezpieczeństwo regulacyjne w przypadku prawidłowego wykonywania porozumienia da odpowiednią korzyść do pracy nad porozumieniem i jego wdrożeniem. Dla mniejszych przedsiębiorców telekomunikacyjnych, którzy mogliby nie być w stanie wypełnić obowiązków które będę określone w porozumieniu, Prezes UKE będzie wydawał rekomendacje. Prawidłowe wykonywanie rekomendacji Prezesa UKE będzie wyłączało ich odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej tych przedsiębiorców.

			konkretnych zachowań kwalifikujących je jako nadużycie telekomunikacyjne". Obecnie projektowana propozycja nie sprostała ww. wymaganiom prezentowanym przez ówczesne MC. **(19.)** Jak się wydaje, służyć ma temu wypracowanie przez Prezesa UKE z przedsiębiorcami telekomunikacyjnymi *„środków organizacyjnych i technicznych, które* (przedsiębiorcy – dopisek) *będą stosowali przy realizacji obowiązków, o których mowa w art. 8*" (art. 10 ust. 1 Projektu). Jednakże zwracamy uwagę, że Projekt wskazuje na fakultatywność zawarcia tego porozumienia, a ponadto porozumienie może być zawarte z niektórymi przedsiębiorcami (którzy niekoniecznie mogą być zainteresowani problemem nadużyć). **(20.)** Z drugiej strony niewykonywanie obowiązku, o którym mowa w art. 8 jest penalizowane (z tym, że kara ma być fakultatywna). **(21.)** Przedsiębiorca telekomunikacyjny z reguły dowiaduje się o połączeniu o charakterze CLI spoofingu ex post (po jego wykonaniu). Tym bardziej niezrozumiałe jest wprowadzenie obowiązku blokowania połączeń. **(22.)** Jednocześnie podkreślamy, że nie rozumiemy sensu anonimizacji połączeń (przedsiębiorca *„ukrywa identyfikację numeru wywołującego dla użytkownika końcowego*"). **(23.)** W konsekwencji wnosimy alternatywnie o:	

			1) wprowadzenie fakultatywnego blokowania połączeń (oraz wyłączenie penalizowania takiego typu naruszenia) (jako rozwiązanie docelowe lub przejściowe) albo 2) określenie metod identyfikacji zachowań spełniających znamiona CLI spoofingu oraz proporcjonalnych środków technicznych i organizacyjnych służących do zwalczania tego zjawiska przez akt o charakterze normatywnym albo 3) wprowadzenie postulowanego przez Rynek zakazu wykorzystywania numeracji nie przyznanej (w bramkach internetowych) oraz ustawowego obowiązku niezmienności numeru A na całej drodze połączenia (co faktycznie powinno wyłączyć połączenia o cechach CLI spoofingu). Propozycja przepisów [rozwiązanie 1) i 2)]: ***Art. 8.*** *1. W celu zapobiegania i zwalczania wykrytych przez przedsiębiorcę telekomunikacyjnego przypadków CLI spoofing przedsiębiorca telekomunikacyjny blokuje takie połączenie głosowe. W takim przypadku użytkownikowi nie przysługuje jakiekolwiek odszkodowanie.* *2. Minister właściwy do spraw cyfryzacji określi, w drodze rozporządzenia, sposoby identyfikacji zachowań posiadających znamiona CLI spoofing oraz środki organizacyjne i techniczne, które będą stosowali przy realizacji obowiązków, o których mowa w ust. 1*. Przepis przejściowy: ***Art. YYY****. Do czasu wejścia w życie rozporządzenia, o którym mowa w art. 8 ust. 2 w celu zapobiegania i zwalczania wykrytych przypadków CLI spoofing przedsiębiorca telekomunikacyjny może zablokować takie*	

			połączenie głosowe. W takim przypadku użytkownikowi nie przysługuje jakiekolwiek odszkodowanie.	
65.	Krajowa Izba Komunikacji Ethernetowej	Art. 8	W art. 8 projektu ustawy jako formę zwalczania spoofingu nakazuje się samodzielne blokowanie połączeń głosowych przez operatora (bez żadnych trybów czy interwencji UKE/NASK) lub ukrycie identyfikacji numeru wywołującego. **Izba wskazuje po pierwsze, że regulacja ta jest korzystna wyłącznie dla dużych operatorów, którzy na tej postawie będą mogli blokować kwestionowany przez siebie ruch telekomunikacyjny (bez względu czy jest on nadużyciem telekomunikacyjnym czy nie).** Po drugie jest ona błędna w kwestiach technicznych. Blokowanie połączeń ma być realizowane (jako obowiązek a nie uprawnienie) w celu zapobiegania i zwalczania spoofingu. Nie jest jasne jaka jest równica między zapobieganiem a zwalczaniem. Wg Izby istnieje zagrożenie, że w celu zapobiegania spoofingowi dopuszczalne będzie blokowanie prezencyjne połączeń z określonych punktów styku, określonej numeracji czy z określonego zakończenia sieci bez względu czy faktycznie jest to spoofing czy nie. Izba wskazuje, że przepis ten powinien umożliwiać blokowanie tylko takich połączeń, które są spoofingiem. Przedsiębiorca telekomunikacyjny z kolei ma pewność, że dane połączenie jest spoofingiem wyłącznie, jeśli jest ono inicjowane w jego własnej sieci (wie, że to zakończenie sieci ma inny numer niż wykazywany w systemie). Z tego względu przepis ten powinien uprawniać przedsiębiorców telekomunikacyjnych do blokowania połączeń ze spoofingiem tylko jeśli są inicjowane z jego własnej sieci. W przypadku połączeń spoza jego sieci operator nie będzie miał takiej wiedzy i może to	**Uwaga nieuwzględniona** Projektowany art. 8 musi być odczytywany wraz z art. 3 definiującym to nadużycie oraz art. 10 mówiącym o porozumieniu oraz rekomendacjach Prezesa UKE. Mniejsi operatorzy telekomunikacyjni, którzy nie będą mogli dołączyć do porozumienia z prezesem UKE, będą mogli oprzeć swoje działania na rekomendacjach Prezesa UKE określających środki organizacyjne i techniczne, które powinny być stosowane przy wykonywaniu obowiązku określonego w art. 8. Co istotne prawidłowe stosowanie rekomendowanych środków będzie zwalniało z odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem wprowadzonych tych środków. Rekomendacje te będą dostosowane do możliwości technicznych operatorów. W zakresie ukrywania identyfikacji numeru wywołującego obowiązek ten dotyczy jedynie ukrycia identyfikacji przed użytkownikiem końcowym a nie przed innym operatorem.

			stwierdzić dopiero post factum badając rekordy ze swojego punktu styku. Za całkowicie wadliwe należy uznać mechanizm przeciwdziałania spoofingowi polegający na ukrywaniu identyfikacji numeru wywołującego. Po pierwsze jest to możliwe tylko w przypadku połączeń w obrębie jednej sieci telekomunikacyjnej. Zgodnie z zasadami międzyoperatorskimi połączenie głosowe przychodzące na punkt styku bez numeru A abonenta wywołującego jest automatycznie traktowane jako fraudowe i blokowane na punkcie styku (lub też rozliczane jako oszustwo międzyoperatorskie z ciężkimi karami finansowymi). Żaden więc przedsiębiorca telekomunikacyjny nie będzie mógł ukryć identyfikację numeru wywołującego.	
66.	Polska Izba Komunikacji Elektronicznej	Art. 8	**Sposoby zapobiegania i zwalczania spoofingu *(art. 8)*** Projekt ustawy przewiduje nałożenie na przedsiębiorców telekomunikacyjnych obligatoryjnych dwóch sposobów zapobiegania i zwalczania CLI spoofing. Tymi sposobami są blokowanie połączenia głosowanego i ukrywanie identyfikacji numeru wywołującego dla użytkownika końcowego. **Izba negatywnie ocenia proponowane rozwiązanie.** W pierwszej kolejności wskazać należy, że ustawa nie powinna ograniczać katalogu środków stosowanych w ramach zapobiegania i zwalczania CLI spoofing. Spowodowane jest to przede wszystkim możliwością stosowania innych, równie skutecznych mechanizmów działania. *Ratio legis* wprowadzenia tego przepisu jest klarowne – ustawa ma wprowadzić narzędzie możliwie skuteczne, aby zapobiegać naruszeniom. W opinii Izby natomiast, wykładnia projektowanego przepisu nakazuje przyjąć, że wprowadza on **katalog zamknięty**	**Uwaga wyjaśnienie** Projektodawca proponuje, aby środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie CLI spoofing były doprecyzowane w porozumieniu zawartym w Prezesem UKE. Ten model samoregulacji ma z jednej strony zapewnić bezpieczeństwo regulacyjne dla przedsiębiorców telekomunikacyjnych, a z drugiej jest on na tyle elastyczny, aby można było dostosować środki do ciągle rozwijających się nowych technologii jak i zagrożeń.

			stosowanych środków. Wynika to przede wszystkim z tego, że przepis wprowadza obowiązek ich stosowania przez przedsiębiorców telekomunikacyjnych. Zdaniem Izby, wprowadzenie katalogu zamkniętego środków zapobiegania i zwalczania CLI spoofing nie będzie rozwiązaniem optymalnym. **W dalszych pracach nad ustawą powinno się rozważyć zastąpienie katalogu zamkniętego tych mechanizmów katalogiem otwartym, które umożliwi ich dostosowanie do możliwości technicznych i finansowych przedsiębiorców telekomunikacyjnych**. Po drugie, art. 8 należy koniecznie doprecyzować wskazaniem, że jakiekolwiek działania przedsiębiorców telekomunikacyjnych powinny następować *ex post*, a zatem dopiero po wykryciu przypadków CLI spoofing. Działania nie powinny być oparte o abstrakcyjną analizę potencjalnych przypadków nadużycia, w szczególności o automatyczne modele predykcyjne, ale powinny dotyczyć takich przypadków, w których naruszenia byłyby dostatecznie **zweryfikowane**. Należy zatem wziąć pod rozwagę, że rozwiązania *ex ante* mogą nie być rozwiązaniem optymalnym. Przepisy nie powinny ponadto pozostawiać tak szerokiego zakresu swobody doboru środków działania, który pozwalałby wykorzystywać przewidziane w przepisach mechanizmy do nieuczciwych praktyk konkurencyjnych. Wprowadzenie obowiązku stosowania działań mających na celu jedynie zapobieganie CLI spoofing rodzi poważne **ryzyko nadużywania regulacji**. W szczególności ryzyko to odnosi się do podejmowania działań wobec właściwych ruchów w sieci tytułem zapobiegania tym niewłaściwym. To z kolei może przerodzić się w praktyce w liczne spory	

			między operatorami telekomunikacyjnymi, a nawet w spory z abonentami. W dalszej mierze podkreślić należy, że art. 8 skonstruowany jest niezwykle szczątkowo, co sprzyja niewłaściwej wykładni nałożonych na przedsiębiorców telekomunikacyjnych obowiązków. Prawidłowe zastosowanie tego przepisu mogłoby zostać zapewnione wyłącznie poprzez jego doprecyzowanie. Konieczność doprecyzowania tym bardziej uzasadnia penalizacja niewykonywania obowiązków, o których mowa w art. 8, na mocy art. 15 ust. 2 pkt 2).	
67.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 8	**ad Art. 8.** W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo *ukrywa identyfikację numeru wywołującego* dla użytkownika końcowego. Propozycja PTI Zamienić cały powyższy przepis na poniższy: *W celu zapobiegania i zwalczania odbioru połączeń z szalbierczych numerów dzwoniących przedsiębiorca telekomunikacyjny blokuje połączenie głosowe i podaje informację o zablokowaniu połączenia i jego przyczynie.* Komentarz PTI Ukrycie identyfikacji szalbierczego numeru wywołującego nie tylko nie wystarczy, ale doprowadzi do skutku przeciwnego niż zamierzony przez regulację – połączenie będzie odbierane bez świadomości szalbierstwa.	**Uwaga nieuwzględniona** Ukrycie numeru ma nastąpić w sytuacji gdy przedsiębiorca telekomunikacyjny ma wątpliwości czy połączenie nie jest spoofowane, ale tej pewności nie ma. Użytkownik końcowy widząc taką informację (a w zasadzie jej brak) powinien nabrać wątpliwości co do tego połączenia. Część odbiorców nie odbierze takiego połączenia, a pozostali mimo tego, że odbiorą, będą moglinabrać wątpliwości, dlaczego np. znajoma osoba albo osoba podająca się za pracownika instytucji – policji, banku – dzwoni z numeru prywatnego.
68.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 8	**Art. 8**	**Wyjaśnienie** Nieuprawnione modyfikowanie informacji adresowej (nie tylko w kontekście CLI Spoofing) również zostało uznane za

			Art. 8 projektu daje przedsiębiorcy telekomunikacyjnemu bardzo szerokie uprawnienia dotyczące blokowania połączeń głosowych Przedsiębiorca telekomunikacyjny samodzielnie podejmuje decyzję o zablokowania połączenia głosowego. Przed zablokowaniem połączenia głosowego musi stwierdzić, że użytkownik wywołujący połączenie głosowe nie jest uprawniony do posługiwania się „informacją adresową" (niezdefiniowana w projekcie) wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik. Dalej przedsiębiorca musi jednoznacznie stwierdzić, że to połączenie głosowe służy podszyciu się pod inny podmiot niż ww. użytkownik. Następnie przedsiębiorca telekomunikacyjny musi jednoznacznie zbadać cel wykonania połączenia i po stwierdzeniu, że takim celem jest nakłonienie odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing) blokuje takie połączenie. Stwierdzenie „podszywania" się użytkownika wywołującego pod numer telefoniczny należący do innego użytkownika jest czynnością techniczną i może to być wykonane za pomocą sytemu informatycznego bez potrzeby większej ingerencji w połączenia. Wskazanie, że jest to połączenie głosowe „służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji	nadużycie w komunikacji elektronicznej. Rozmowy przeprowadzone z przedsiębiorcami telekomunikacyjnymi wskazują, że będą oni w stanie rozpoznawać tak zdefiniowane nadużycia i im przeciwdziałać. Nie można też zgodzić się, że przedsiębiorcy telekomunikacyjni będą mieli tak duży zakres swobody przy blokowaniu połączeń. Wciąż będą oni związani postanowieniami umownymi, a nieprawidłowe zablokowanie wiadomości będzie wiązało się z odpowiedzialnością umowną.

			oprogramowania (CLI spoofing).", wykonane przed zestawieniem połączenia, zdaniem opiniujących jest niemożliwe. Podkreślić należy, że aby przedsiębiorca mógł legalnie zablokować połączenie muszą być spełnione wszystkie przesłanki zawarte w definicji CLI spoofingu (art. 3 ust. 1 pkt 3 projektu). **Pojawia się zatem pytanie, czy w omawianym przypadku nie mamy do czynienia z przepisem niemożliwym do zrealizowania w praktyce, co świadczyłoby o nieracjonalności ustawodawcy (projektodawcy), a co świadczyłoby o obrazie konstytucyjnej zasady demokratycznego państwa prawnego (art. 2 Konstytucji RP).**	
69.	Krajowa Izba Komunikacji Ethernetowej	Art. 9	Izba popiera tworzenie przez Prezesa UKE wykazu numerów, z których nie mogą być inicjowane połączenia telefoniczne z art. 9 projektu ustawy. Jest to metoda, której domagają się sami członkowie Izby oraz ich klienci. Regulacja ta wymaga jednak kilku poprawek. Po pierwsze, wykaz nie powinien być publikowany w biuletynie informacji publicznej UKE, gdyż wymagałoby to podłączenie do niego systemów każdego przedsiębiorcy telekomunikacyjnego i ręcznego monitorowania wykazu. Zamiast tego wykaz ten powinien być częścią systemu PLI CBD, zarządzającego lokalizacją numeracji i jej przenoszenia, do którego systemu każdy przedsiębiorca już jest podłączony (i to w dodatku automatycznie zaciągane są dane). Rozwiązanie to będzie praktyczniejsze i tańsze. Po drugie, w ust. 3 powinno być uprawnienie przedsiębiorców telekomunikacyjnych oraz ich użytkowników do wpisywania numerów usług infolinii i biura obsługi	**Uwaga nieuwzględniona** Przyjęte procedury zapewniają również efektywność obsługi wniosków o wpis do wykazu. Zakres podmiotów mogących wnioskować o wpis jest ukształtowany od strony świadczącego usługę (usługodawcy), a nie korzystającego z niej (usługobiorcy). Biorąc pod uwagę pożądany skutek i cel ustawy jest to rozwiązanie właściwe. Proponowane procedury związane z działaniem wykazu mają zapewnić efektywne wykonywanie zadań przez UKE. Taka forma wykazu jest najłatwiejsza do wdrożenia (od integracji z PLICBD czy PIT jak wskazuje UKE).

			klienta wykorzystywanych przez użytkowników a nie przez samych przedsiębiorców telekomunikacyjnych. Jednocześnie Izba wskazuje, że w art. 9 ust. 9 projektu ustawy powinien być zapis o wniosku o usunięciu numeru z wykazu Prezesa UKE zamiast o wycofaniu wniosku o wpis tego numeru. Taka regulacja jest bardziej elastyczna zwłaszcza w przypadku przeniesienia numeru do innego operatora lub zmian właścicielskich w firmie dysponującym numerem wpisanym do wykazu. Postępowanie o usunięcie numeru z wykazu odbywałoby się samodzielnie bez konieczności „kontynuowania" postępowania o umieszczenie numeru w wykazie.	
70.	Polska Izba Komunikacji Elektronicznej	Art. 9	**Wykaz numerów telefonów służących wyłączenie do odbierania połączeń głosowych *(art. 9)*** W odniesieniu do propozycji wprowadzenia jawnego wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych Izba nie zgłasza stanowczo negatywnych uwag. PIKE zgłasza jedynie prośbę o przedstawienie motywów wprowadzenia wykazu wraz z wizją jego zastosowania w praktyce, w szczególności przez przedsiębiorców telekomunikacyjnych. Poza tym, zgłaszamy również potrzebę przedstawienia przez projektodawcę sposobu synchronizacji systemów przedsiębiorców telekomunikacyjnych z tym wykazem. Powyższa prośba uzasadniona jest szczególnie przez nieprecyzyjną konstrukcję przepisów i zawarte w nich błędy legislacyjne (np. art. 9 ust. 3). Ponownie dostrzegamy potrzebę przygotowania przepisów klarownych, by ograniczyć wątpliwości interpretacyjne. Uwaga ta odnosi się do art. 9 w całości.	**Uwaga wyjaśniona** Rozwiązanie pozwoli skutecznie zapobiegać połączeniom spoofingowym z numerów, które zostaną umieszczone w wykazie. Połączenia z wykorzystaniem takiego numeru będą przerywane przez przedsiębiorców telekomunikacyjnych i nie zostaną terminowane u użytkownika końcowego – projekt przewiduje blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu. Szczególnie istotne jest, że kluczowe instytucje finansowe takie jak banki zamieszczą swoje numery w tym wykazie. Ich numery są często wykorzystywane przez przestępców aby wzbudzić zaufanie i wprowadzić w błąd już od momentu odebrania połączenia przez użytkownika końcowego.

71.	Polska Izba Informatyki i Telekomunikacji	Art. 9 ust. 1	**Wykaz numerów służących wyłącznie do odbierania połączeń** Projektowana ustawa zakłada, że Prezes UKE będzie prowadził wykaz numerów, które służą wyłącznie do odbierania połączeń (art. 9 ust. 1 projektu ustawy). Przedsiębiorcy telekomunikacyjni mają blokować połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu (art. 9 ust. 12 projektu ustawy). Jednocześnie projektowana ustawa zakłada, że Prezes UKE będzie mógł nałożyć karę pieniężną za naruszenie przez przedsiębiorcę telekomunikacyjnego obowiązku blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu (art. 15 ust. 2 pkt 3) projektu ustawy). Jeśli przedsiębiorcy telekomunikacyjni mają działać w reżimie obowiązku, pod groźbą kary (nawet jeśli ma to być kara fakultatywna) to konieczne będzie uzupełnienie przepisów projektowanej ustawy o regulacje, które precyzyjnie określają w jaki sposób Prezes UKE będzie udostępniał informacje zawarte w wykazie (na stronie internetowej, poprzez system informatyczny, inaczej), jak również o przepisy określające, ile czasu - od momentu przekazania informacji przez Prezesa UKE o wpisie do wykazu - ma przedsiębiorca telekomunikacyjny na zaimplementowanie w swojej sieci i rozpoczęcie blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu. Mechanizm taki musi: • być niezawodny i dostępny, aby każdy przedsiębiorca telekomunikacyjny w kraju mógł wywiązać się z obowiązku;	**Uwaga częściowo uwzględniona** Projektodawca przewiduje, że wykaz numerów, które służą wyłącznie do odbierania połączeń będzie prowadzony za pomocą systemu teleinformatycznego i będzie miał on charakter rejestru publicznego. Ponadto obowiązek przedsiębiorcy telekomunikacyjnego został doprecyzowany: „Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu do wykazu, blokuje połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu.”. **W zakresie zmiany obowiązku na uprawnienie po stronie przedsiębiorców telekomunikacyjnych i kwestii kar** Projektowane rozwiązania, po uwzględnieniu uwag, są wystarczające precyzyjnie. Aby skutecznie walczyć z nadużyciami w komunikacji elektronicznej powinien zostać nałożony obowiązek prawny (obowiązki) na przedsiębiorców telekomunikacyjnych. W przypadku przyznania uprawnienia przedsiębiorca telekomunikacyjny mógłby, ale nie musiałby podejmować działań mających na celu zwalczanie nadużyć. Natomiast ryzyko nałożeniu sankcji w przypadku niewypełnienia obowiązków m.in. realizuje funkcję prewencyjną i represyjną.

			• być racjonalny kosztowo, zarówno z perspektywy kosztów, jakie poniesie Prezes UKE na stworzenie i utrzymanie wykazu jak i z perspektywy kosztów, jakie będą musieli ponieść przedsiębiorcy telekomunikacyjni na wdrożenie i utrzymanie rozwiązania; • dawać przedsiębiorcom telekomunikacyjnych czas niezbędny na pobranie informacji z wykazu oraz jej implementację w sieciach telekomunikacyjnych i rozpoczęcie blokowania; termin na wykonanie obowiązku – liczony od momentu przekazania przez Prezesa UKE informacji o wpisie numeru do wykazu – nie może być krótszy niż 3 dni robocze; • komunikacja z wykazem powinna dawać się automatyzować (oczywiście z uwzględnieniem postulatu racjonalności kosztów), co oznacza, że nawet jeśli komunikacja z wykazem przyjmie postać pobierania pliku ze strony Prezesa UKE, to nie należy stosować rozwiązań takich jak CAPTCHA, uniemożliwiających automatyzację procesu. Powyższe wymagania muszą być spełnione, jeśli przedsiębiorcy telekomunikacyjni mają działać w reżimie obowiązku pod groźbą kary. Brak przepisów precyzujących powyższe zagadnienia spowoduje, że ani Prezes UKE ani przedsiębiorcy telekomunikacyjni nie będą wiedzieli, czy w danym przypadku powstaje już zagrożenie karą czy nie. Szczegółowe określanie na poziomie ustawy zasad funkcjonowania wykazu nie będzie jednak konieczne,	

			jeśli Projektodawca, zgodnie z naszym ogólnym postulatem, zastąpi obowiązek uprawnieniem do blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu albo co najmniej, jeśli Projektodawca (pozostawiając reżim obowiązku) zrezygnuje z możliwości nakładania kary pieniężnej za niewykonanie tego obowiązki. Zatem alternatywnie, w stosunku do postulatu uzupełnienia projektu ustawy o szczegółowe zasady funkcjonowania wykazu, proponujemy usunięcia z projektu ustawy art. 15 ust. 2 pkt 3) (przewidującego możliwość nałożenia kary za niewywiązanie się z analizowanego obowiązku).	
72.	Związek Banków Polskich	Art. 9 ust. 1-4 , 6-9 i 12 oraz ust. 13 (nowy)	1.Prezes UKE, prowadzi jawny wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych **oraz wykaz numerów służących do inicjowania połączeń głosowych** i udostępnia je w Biuletynie Informacji Publicznej na swojej stronie podmiotowej. 2. Prezes UKE dokonuje wpisu do wykazów, o których mowa w ust. 1, na wniosek: 1) jednostki sektora finansów publicznych, o której mowa w art. 9 z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. 2021 r. poz. 305, z późn. zm.)), 2) banku **3) spółdzielczej kasy oszczędnościowo-kredytowej** **4) centrum analizy i wymiany informacji utworzone na podstawie art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)** **5) podmioty wchodzące w skład Krajowego Systemu Cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.)**	**Uwaga częściowo uwzględniona w zakresie dodania SKOK do listy podmiotów uprawnionych do wpisu do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych.** **W pozostałym zakresie uwaga nieuwzględniona** W pozostałym zakresie należy zauważyć, że obecne zasady związane z funkcjonowaniem tego rejestru są w wystarczający sposób określone w ustawie. Chcemy aby do rejestru były wpisane podmioty, których numery szczególnie często są wykorzystywane przez przestępców. Są to przede wszystkim podmioty z sektora finansowego. W związku z tym niecelowe byłoby dołączenie do wykazu podmiotów krajowego systemu cyberbezpieczeństwa. Równocześnie obowiązek zwalczania spoofingu, zwłaszcza blokowania połączeń jest

			3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykaz**ów**, o których mowa w ust. 1, wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii. 4. Wniosek, o którym mowa w ust. 2 i 3, zawiera wskazanie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych **lub numeru służącego do inicjowania połączeń głosowych** 6. Prezes UKE dokonuje wpisu numeru do wyka**zów**, o któr**ych** mowa w ust. 1, w terminie 5 dni od dnia otrzymania wniosku. 7. Wpis do wyka**zów**, o któr**ych** mowa w ust. 1, jest czynnością materialno-techniczną. 8. Prezes UKE odmawia wpisu do wyka**zów**, o któr**ych** mowa w ust. 1, w drodze decyzji, jeżeli wniosek został złożony przez podmiot nieuprawniony lub dotyczy on numeru niewykorzystywanego przez ten podmiot. 9. Podmiot, który złożył wniosek, o którym mowa w ust. 2 i 3, może w każdym czasie go wycofać. W takim przypadku Prezes UKE niezwłocznie, jednak nie później niż w terminie 5 dni od dnia złożenia wniosku o wycofanie numeru z wykazu, wykreśla numer z wyka**zów**, o któr**ych** mowa w ust. 1.	już zawarty w przygotowywanej ustawie jak choćby w projektowanym art. 8. Zgodnie z zasadami techniki prawodawczej nie należy powtarzać norm prawnych.

			12. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych blokuje połączenia inicjowane z wykorzystaniem numeru wpisanego do **wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych.** 13. **Przedsiębiorca telekomunikacyjny obowiązany jest do podjęcia szczególnych działań organizacyjnych i technicznych służących zapobieganiu oraz zwalczaniu CLI spoofing wykonywanego przy wykorzystaniu numerów wskazanych w wykazie numerów służących do inicjowania połączeń głosowych** W opinii sektora bankowego stworzenie rejestru numerów służących wyłącznie do odbierania połączeń (oraz zobowiązanie przedsiębiorców telekomunikacyjnych do blokowania połączeń wychodzących z tych numerów) może okazać się niewystarczające. W związku z powyższym, proponujemy stworzenie drugiego rejestru, który zawierałby numery zgłoszone przez wymienione podmioty, charakteryzujące się kluczowym znaczeniem dla działalności danego podmiotu (np. numery centrali telefonicznej, infolinii, działu bezpieczeństwa itp.). Jednocześnie, przedsiębiorca telekomunikacyjny powinien w przypadku tych numerów (umożliwiających również wykonywanie połączeń wychodzących) podejmować nadzwyczajne środki przeciwdziałające występowaniu zjawiska spoofingu. Praktyka pokazuje, że znaczna część przestępstw spoofingowych jest popełniania przy wykorzystaniu właśnie tego rodzaju numerów, umożliwiających wykonywanie połączeń wychodzących. Proponujemy również uwzględnienie w przedmiotowym katalogu instytucji uprawnionych do zgłaszania numerów	

			do obu wykazów, spółdzielczych kas z uwagi na charakter działalności tego rodzaju podmiotów, który może być wykorzystywany do nadużyć w komunikacji elektronicznej. Ponadto, proponujemy uwzględnienie w katalogu, instytucji tworzonych przez banki wspólnie z bankową izbą gospodarczą – tj. centrum wymiany i analiz informacji, których tworzenie byłoby możliwe na podstawie znowelizowanych przepisów ustawy - Prawo Bankowe wskazanych poniżej, a także podmioty wchodzące w skład Krajowego Systemu Cyberbezpieczeństwa. Wskazane podmioty były celem ataków spofingowych/vishingowych i jako instytucje zaufania publicznego były i mogą być narażone na materializację ryzyka utraty reputacji.	
73.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 9 ust. 1	**Art. 9 ust. 1** Prezes UKE prowadzi wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych wykorzystywanych przez jednostki sektora finansów publicznych, banki lub przez przedsiębiorców telekomunikacyjnych. Jest to w rzeczywistości niewielki tylko odsetek wszystkich numerów telefonów, które mogą być wykorzystane do nadużyć. **Sugeruje się zatem rozszerzenie katalogu podmiotów, które mogą zgłosić swoje numery telefonów wykorzystywanych wyłącznie do odbierania połączeń głosowych**.	**Uwaga uwzględniona** Katalog podmiotów uprawnionych do złożenia przedmiotowego wniosku zostanie rozszerzony m. in. o SKOK.

74.	Polska Izba Informatyki i Telekomunikacji	Art. 9 ust. 3	**Wpis numeru do wykazu numerów służących wyłącznie do odbierania połączeń** Projektowana ustawa w art. 9 ust. 3 przewiduje możliwość wpisu numeru do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych, oraz wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii. Takiego wpisu dokonuje Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego,. Rozumiemy, iż intencją ustawodawcy jest, aby przedsiębiorcy telekomunikacyjni zyskali możliwość wpisania do wykazu numerów własnych wykorzystywanych w swojej działalności biznesowej do kontaktu klientów z przedsiębiorcą, np. w celach obsługowych. W przeszłości zdarzały się również przypadki podszywania się oszustów pod takie numery biura obsługi klientów lub infolinii. W ramach Izby, otrzymaliśmy sygnały, iż wskazany przepis może być interpretowany i wykorzystany przez klientów, w szczególności klientów B2B z którymi przedsiębiorca ma zawarte umowy o świadczenie usług, jako obowiązek zgłaszania przez przedsiębiorcę telekomunikacyjnego numerów udostępnionych tym klientom (w ramach świadczonych usług) i wykorzystywanych przez klientów na potrzeby biura obsługi klientów lub infolinii. W ocenie Izby, aby uniknąć tych wątpliwości, przepis należy doprecyzować tak, aby mówił o numerach wykorzystywanych przez przedsiębiorcę na	**Uwaga częściowo uwzględniona** Przepis zostanie dookreślony poprzez dodanie „własne”.

			potrzeby <u>własne</u> biura obsługi klientów lub infolinii. *3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykazu, o którym mowa w ust. 1, wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby <u>własne</u> biura obsługi klientów lub infolinii.* Jeżeli projektodawca ocenia jednak, iż istniałaby potrzeba, aby do wykazu numerów służących wyłączenie do odbierania połączeń głosowych wpisywały się także inne podmioty niż wskazane w art. 9 ust. 2, warto rozważyć dodanie zapisów, które to uwzględnią. Inne podmioty mogłyby dopisywać się do takiego wykazu, jeżeli wykazałyby Prezesowi UKE np. swój interes faktyczny.	
75.	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 9 ust. 12	**X. [BLOKOWANIE POŁĄCZEŃ – ART. 9 UST. 12]** **(36.)** Proponujemy zmianę zapisów w art. 9 ust 12, który dotyczy sposobu postępowania z połączeniami wykonywanymi z numerów umieszczonych w wykazie numerów. Przedsiębiorca telekomunikacyjny powinien blokować połączenia **przychodzące** do jego sieci z numerów telefonów służących wyłącznie do odbierania połączeń głosowych. Połączenia z tych numerów nie będą inicjowane. Wiele przypadków spoofingu dotyczy połączeń tranzytowanych i przychodzących z sieci innych operatorów.	**Uwaga uwzględniona** Przepis został zmieniony zgodnie z uwagą, że mowa jest o połączeniach przychodzących. „Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu do wykazu, blokuje połączenia przychodzące do jego sieci z wykorzystaniem numeru wpisanego do wykazu.”.

			„12. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych blokuje połączenia przychodzące z wykorzystaniem numeru wpisanego do wykazu.”	
76.	Krajowa Izba Komunikacji Ethernetowej	Art. 10	W art. 10 wprowadza się w fakultatywne porozumienie przedsiębiorcy telekomunikacyjnego z Prezesem UKE o środkach technicznych i organizacyjnych zwalczania spoofingu, które pozwala na zwolnienie od odpowiedzialności za blokowane połączenia telefoniczne w ramach walki ze spoofingiem. Regulacja ta budzi poważne zastrzeżenia Izby biorąc pod uwagę jej ogólny i niejasny charakter z ogromnymi konsekwencjami. Nie jest jasne jak miałoby wyglądać takie porozumienie, z iloma podmiotami i jak bardzo musiałoby być szczegółowe. Z uwagi na zwolnienie od odpowiedzialności za blokowanie ruchu, porozumienie to powinno być zarówno bardzo szczegółowe jak też jawne, gdyż będzie ono elementem sporów międzyoperatorskich. Przykładowo operator A zablokuje ruch telekomunikacyjny od operatora B, argumentując, że robi to w celu zapobiegania spoofingowi i robi to zgodnie z zawartym przez siebie porozumieniem z Prezesem UKE. Tymczasem operator B nie może zweryfikować tych twierdzeń, czy porozumienie operatora A z Prezesem UKE rzeczywiście uprawnia do dokonanej blokady ruchu. Co więcej, porozumienie to zwalnia operatora A od odpowiedzialności względem operatora B za zablokowanie legalnego ruchu. Biorą pod uwagę praktykę zawierania porozumień przez Prezesa UKE tylko z dużymi podmiotami gospodarczymi, regulacja ta doprowadzi do dyskryminacji tych przedsiębiorców telekomunikacyjnych, którzy nie zawrą porozumienia z Prezesem UKE (w pierwszej kolejności MŚP, a więc członków KIKE). Izba postuluje rezygnację z	**Uwaga wyjaśniona** Ustawa będzie wskazywać, że porozumienie z Prezesem UKE mogą zawrzeć operatorzy świadczący usługi telekomunikacyjne dla co najmniej 50 000 abonentów. Do pozostałych operatorów telekomunikacyjnych Prezes UKE będzie mógł skierować rekomendacje określające środki organizacyjne i techniczne. Kwestie szczegółowe związane z porozumieniem nie powinny znaleźć się w ustawie ze względu na swój techniczny charakter i zostaną doprecyzowane w ramach współpracy między UKE a przedsiębiorcami. Projektodawca proponuje, aby środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie CLI spoofing były doprecyzowane w porozumieniu zawartym z Prezesem UKE. Ten model samoregulacji ma z jednej strony zapewnić bezpieczeństwo regulacyjne dla przedsiębiorców telekomunikacyjnych, a z drugiej jest on na tyle elastyczny, aby można było dostosować środki do ciągle rozwijających się nowych technologii jak i zagrożeń. Dzięki takiemu rozwiązaniu przedsiębiorcy telekomunikacyjni wraz ze wsparciem i nadzorem UKE będą mogli wypracować najlepsze rozwiązania techniczne i organizacyjne, które pozwolą im zwalczać

			porozumień z Prezesem UKE na rzecz niedyskryminacyjnych i proporcjonalnych regulacji ogólnorynkowych oraz zwolnienie od odpowiedzialności wyłącznie za zablokowanie usług, które faktycznie były nadużyciem. Dodatkowo wątpliwości Izby budzi zakres podmiotowy art. 10 ust. 1 projektu, gdzie wskazuje się, że porozumienie z Prezesem UKE w zakresie spoofingu mogą zawrzeć tylko operatorzy, a nie dostawcy usług komunikacji głosowej.	nadużycia w komunikacji elektronicznej. Bezpieczeństwo regulacyjne w przypadku prawidłowego wykonywania porozumienia da odpowiednią korzyść do pracy nad porozumieniem i jego wdrożeniem. Dla mniejszych przedsiębiorców telekomunikacyjnych, którzy mogliby nie być w stanie wypełnić obowiązków które będę określone w porozumieniu, Prezes UKE będzie wydawał rekomendacje. Prawidłowe wykonywanie rekomendacji Prezesa UKE będzie wyłączało ich odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej tych przedsiębiorców.
77.	Polska Izba Komunikacji Elektronicznej	Art. 10	**Porozumienie w zakresie realizacji obowiązków, o których mowa w art. 8 *(art. 10)*** W zakresie możliwości zawarcia porozumienia między operatorem a Prezesem UKE PIKE nie zgłasza negatywnych uwag. Zwracamy jednak uwagę, że zmianę należy wprowadzić w OSR projektu, ze względu na konieczność wprowadzenia zmian w regulaminach rozpatrywania reklamacji przez przedsiębiorców telekomunikacyjnych w przypadku zawarcia porozumienia.	**Uwaga uwzględniona** W OSR zostanie uwzględniona stosowna wzmianka.
78.	Krajowa Izba Komunikacji Ethernetowej	Art. 11	W art. 11 ust. 2 wprowadza się fakultatywne porozumienie przedsiębiorcy telekomunikacyjnego z Prezesem UKE w zakresie domen internetowych służących do spoofingu oraz fakultatywną możliwość blokowania dostępu do takich domen. Projekt ustawy tego nie	**Uwaga nieuwzględniona** Mechanizm proponowany w ustawie funkcjonuje obecnie – jest nim lista ostrzeżeń przed niebezpiecznymi stronami prowadzona przez NASK-PIB[3].

[3] https://cert.pl/posts/2020/03/ostrzezenia_phishing/

			precyzuje, ale uprawnienie do blokowania wskazanych domen internetowych dotyczy przede wszystkim dostawców dostępu do sieci Internet, a nie samych dostawców usług głosowych. Biorąc pod uwagę poziom wiedzy technicznej oszustów korzystających ze spoofingu proponowany mechanizm będzie nieskuteczny i należy z niego zrezygnować (np. korzystanie z VPN). Ponadto mechanizm ten jest pozbawiony kontroli innych rejestrów zablokowanych domen i może poradzić do blokowania domen niezwiązanych z realnymi nadużyciami w komunikacji elektronicznej. Obecny zapis jest tak szeroki i niejasny, że może pod niego podlegać np. Facebook, Twitter, allegro czy każdy sklep internetowy.	
79.	Polska Izba Informatyki i Telekomunikacji	Art. 11	**Lista ostrzeżeń NASK** Art. 11 ust. 6 projektu ustawy stanowi, że przedsiębiorca telekomunikacyjny może uniemożliwić dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1 art. 11. Przy obecnym brzmieniu może powstać wątpliwość, czy przedsiębiorca telekomunikacyjny będzie mógł uniemożliwić dostęp do domen obecnych na liście CSIRT NASK, ale należących do zakresu domen wskazanych w ust. 2 art. 11 (skoro przepis upoważniający do uniemożliwienia dostępu referuje do ust. 1 w art. 11 projektu ustawy). W ocenie Izby, aby uniknąć tych wątpliwości, analizowany przepis należy doprecyzować tak, aby odsyłał do listy, o której mowa w ust. 3 (a nie ust. 1): *Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych*	**Uwaga uwzględniona**

			wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 3. To właśnie ust. 3 w art. 11 projektu ustawy mówi o liście prowadzonej przez CSIRT NASK (a na listę tę składają się dwa zakresy domen, wymienione w ust. 1 i 2 w art. 11).	
80.	Polska Izba Komunikacji Elektronicznej	Art. 11	**Porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych *(art. 11)*** Art. 11 projektu przewiduje możliwość zawarcia fakultatywnego porozumienia w zakresie prowadzenia i utrzymywania: 1) jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu (ust. 1) 2) jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron (ust. 2) oraz uniemożliwienia dostępu do tych stron. Izba przede wszystkim zgłasza swoje wątpliwości co do zasadności prowadzenia wskazanych powyżej list ostrzeżeń w proponowanym kształcie. Przeszkodą w praktycznym zastosowaniu tych list i uniemożliwiania dostępu do poszczególnych stron jest bowiem brak dostosowania do realnych nadużyć. Podkreślenia wymaga fakt, że podmioty doprowadzające do nadużyć w komunikacji elektronicznej posługują się szeroką wiedzą oraz zaawansowanymi technologiami. Z tego względu należy stwierdzić, że **przedmiotowa regulacja**	**Uwaga nieuwzględniona** Mechanizm proponowany w ustawie funkcjonuje obecnie – jest nim lista ostrzeżeń przed niebezpiecznymi stronami prowadzona przez NASK-PIB[4].

[4] https://cert.pl/posts/2020/03/ostrzezenia_phishing/

			nie sprosta wyzwaniom stawianym przez strony internetowe służące do wyłudzania danych i środków finansowych.	
81.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 11 ust. 1	**ad Art. 11. ust. 1.** W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwienia dostępu do tych stron. <u>Propozycja PTI zmiany treści zapisu:</u> *W celu ochrony użytkowników internetu przed szalbierczymi stronami internetowymi wyłudzającymi dane,w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących szalbierczych stron internetowych oraz uniemożliwienia do nich dostępu.* <u>Komentarz PTI</u> Takimi szalbierczymi stronami mogą być tylko niektóre strony z danej domeny. Wobec tego blokowanie całej domeny jest działaniem nadmiarowym – należy się ograniczyć tylko do blokowania stron.	**Uwaga nieuwzględniona** Praktyka pokazuje, że z reguły niebezpieczne są całe domeny.
82.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 11 ust. 2	**ad Art. 11. ust.2.** W celu ochrony użytkowników internetu przed CLI spoofing, elementem porozumienia, o którym mowa w ust. 1, może być jawna lista ostrzeżeń dotyczących domen	**Uwaga wyjaśniona** W tym przepisie chodziło o domeny, za pomocą których oszuści dokonują CLI spoofing. Ze względu na odmienny, bardziej

			internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron. Komentarz PTI Ten ustęp jest zbędny, gdyż CLI spoofing dotyczy połączeń głosowych a nie stron internetowych, chyba że chodzi tutaj o strony internetowe, które służą podmianie lub ukryciu prawdziwego numeru dzwoniącego. W tym przypadku można je po prostu uznać za strony szalbiercze i potraktować jak te z ust.1. Ale też przy istnieniu VPN uniemożliwianie dostępu do tych stron może być mało skuteczne.	skomplikowany charakter decyzji o wpisie takich domen do listy, proponuje się usunięcie regulacji projektowanego art. 11 ust. 2.
83.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 11 ust. 3, 4, 5, 6	**ad Art. 11 ust 3. , 4., 5., 6.** Propozycja PTI zmiany treści zapisu: W tych ustępach należy wpisać strony internetowe, a nie domeny internetowe.	**Uwaga nieuwzględniona** Praktyka pokazuje, że z reguły niebezpieczne są całe domeny.
84.	Związek Banków Polskich	Art. 11 ust. 4	4. Stronami porozumienia są: 1) Prezes UKE; 2) minister właściwy do spraw informatyzacji; 3) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, oraz 4) przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni, **5) centrum analizy i wymiany informacji utworzone na podstawie art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)**	**Uwaga nieuwzględniona w związku z nieuwzględnieniem zmian w Prawie bankowym**

			Postulujemy uwzględnienie w katalogu podmiotów będących stronami porozumienia dotyczącego zgłaszania domen internetowych, instytucji tworzonych przez banki wspólnie z bankową izbą gospodarczą – tj. centrum wymiany i analiz informacji. FinCERT.pl – BCC ZBP jako reprezentant sektora finansowego winien mieć możliwość w imieniu np. banków wnioskowania o prowadzenie do rejestru zidentyfikowanych przestępczych domen. Taka możliwość usprawni przepływ informacji z i w ramach sektora finansowego.	
85.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 11 ust. 5	**ad Art. ust.5** Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady zgłaszania domen internetowych, wpisania oraz usuwania ich z listy ostrzeżeń, o której mowa w ust. 1. Propozycja PTI zmiany treści zapisu – należy go zmodyfikować jak poniżej: *Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady i podstawy zgłaszania, wpisania, blokowania oraz zwalniania stron internetowych z listy ostrzeżeń, o której mowa w ust. 1.* Komentarz PTI Uważamy, iż przyczyny powodujące zgłoszenie muszą być jawne, gdyż łączne z proponowaną zmianą w ust. 6 art. 11 nie spowoduje to dezorientacji użytkownika w sytuacji odmowy świadczenia usługi dostępu do konkretnej strony. Ponadto proponowane uzupełnienie zapobiegnie arbitralnemu blokowaniu dostępu do stron internetowych.	**Uwaga wyjaśniona** Art. 11 ust. 5 zawiera otwarty katalog elementów, które ma regulować porozumienie. Jest to minimalny zakres porozumienia. Nie ma potrzeby uszczegóławiania tego przepisu, tym bardziej, że propozycja PTIIR również zmierza do określenia katalogu otwartego. Ponadto, proponuje się, aby uprawnienie dot. sprzeciwu umieszczeniu domeny na liście ostrzeżeń wynikało wprost z przepisów rangi ustawowej.

86.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 11 ust. 6	**ad Art. 11 ust. 6.** Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych wpisanych na listę, o której mowa w ust. 1. Propozycja PTI Należy dodać przed końcową kropką poniższy fragment: *, wraz z podaniem przyczyny blokady.* Komentarz PTI W związku w danym przepisem w przypadku zaakceptowania propozycji PTI powyżej do art. 11 ust. 1 powyższy przepis nie spowoduje dezorientacji użytkownika końcowego, gdyż odmowa świadczenia usługi (blokada) będzie umotywowana prawnie, ale nie technicznie, np. w postaci kodów błędów protokołu http.	**Uwaga nieuwzględniona** Przepis to norma zobowiązująca przedsiębiorcę telekomunikacyjnego do podjęcia określonego działania w przypadku tych domen, które zostały umieszczone na liście ostrzeżeń. Nie ma potrzeby jego doprecyzowywania.
87.	IAB Polska	Art. 12 ust. 1 pkt 1 w związku z art. 2 pkt 15	**UWAGA:** Wątpliwości budzi definicja użytkownika, odwołująca się do definicji z ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (art. 2 pkt 49). Zgodnie z definicją z Prawa telekomunikacyjnego użytkownikiem jest „*podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi*”. Odwołanie się do definicji z Prawa telekomunikacyjnego jest **niewłaściwe**, ponieważ **usługa poczty elektronicznej nie jest publicznie dostępną usługą telekomunikacyjn**ą, a jak – sama definicja poczty elektronicznej określa (art. 2 pkt 8 UZNKE) – jest to „*usługa komunikacji interpersonalnej niewykorzystująca numerów*”, a więc	**Uwaga uwzględniona** Przepisy zostały zmienione tak, że nie mówią już o „użytkowniku” a o „użytkowniku poczty”, co mityguje ryzyko niewłaściwej interpretacji.

			żadna **osoba korzystająca z usługi poczty elektronicznej nie może być uznana za użytkownika w rozumieniu tej definicji**. **PROPOZYCJA:** IAB Polska proponuje, aby projektodawca zaproponował inną definicję użytkownika, która będzie adekwatna w stosunku do usług, z jakich użytkownicy będą korzystali.	
88.	IAB Polska	Art. 12 ust. 1 pkt 3	**UWAGA:** Z UZNKE nie wynika, **co należy rozumieć przez „*aktywne konto pocztowe*”**, czym jest konto pocztowe i kiedy konto pocztowe należy uznać za aktywne lub nieaktywne. Ponadto dostawca poczty elektronicznej, który spełnia przesłankę posiadania 500 000 użytkowników określoną w art. 12 ust. 1 pkt 1 UZNKE, będzie najczęściej spełniać przesłankę posiadania 500 000 aktywnych kont pocztowych (jeśli za aktywne konto pocztowe uzna się np. konto, z którego można wysyłać i odbierać e-maile). Użytkownik konta pocztowego będący osobą fizyczną najczęściej korzysta tylko z jednego konta pocztowego, zatem sama przesłanka posiadania przez dostawcę poczty elektronicznej 500 000 użytkowników powinna być wystarczająca dla oceny, czy dostawca poczty elektronicznej powinien spełniać obowiązki określone w art. 12 UZNKE. **PROPOZYCJA:** IAB Polska proponuje wykreślenie z art. 12 ust. 1 UZNKE pkt 3: „*obsługujący co najmniej 500 000 aktywnych kont pocztowych*”.	**Uwaga uwzględniona** Zostanie usunięte odwołanie „aktywnego konta pocztowego”.
89.	IAB Polska	Art. 12 ust. 1	**UWAGA:**	**Uwaga wyjaśniona** Uzasadnienie zostanie skorygowane.

			Art. 12 ust. 1 UZNKE wskazują, że dostawca poczty elektronicznej będzie zobowiązany stosować jednocześnie trzy mechanizmy uwierzytelniania poczty elektronicznej (DMARC – Domain-based Message Authentication Reporting and Conformance, DKIM – DomainKeys Identified Mail oraz SPF – Sender Policy Framework). Z kolei z uzasadnienia do projektu UZNKE wynika, że dostawcy poczty elektronicznej będą mieli obowiązek stosować jeden z tych mechanizmów, co oznacza, że być może na poziomie redakcji tekstu UZNKE **powstała nieścisłość konieczna do skorygowania**. **PROPOZYCJA:** IAB Polska wnosi – zgodnie z przedstawioną poniżej propozycją art. 12 ust. 1 UZNKE, aby dostawca poczty elektronicznej nie był zobowiązany do stosowania łącznie wszystkich mechanizmów uwierzytelniania poczty elektronicznej, a jedynie **jeden z tych wskazanych w art. 12 ust. 1 UZNKE, wybrany samodzielnie przez dostawcę poczty elektroniczne**j. *Art. 12. 1. Dostawca poczty elektronicznej:* *1) dla co najmniej 500 000 użytkowników,* *2) dla podmiotu publicznego, lub* *~~3) obsługujący co najmniej 500 000 aktywnych kont pocztowych~~* *– ma obowiązek stosowania jednego z następujących mechanizmów: SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance)* ***lub*** *DKIM (DomainKeys Identified Mail).*	Zamiarem projektodawcy jest, aby dostawcy poczty elektronicznej stosowali wszystkie 3 wskazane mechanizmy co ograniczy zjawisko spoofowania emaili.
90.	Nazwa.pl sp. z o.o.	Art. 12	Z uzasadnienia do Projektu ustawy wynika, że celem projektu ustawy jest wprowadzenie odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji	**Uwaga wyjaśniona**

			elektronicznej. Z założenia, *„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".* Z uwagi na powyższe, w Projekcie ustawy przewidziano obowiązek wprowadzenia określonych mechanizmów uwierzytelniania poczty elektronicznej przez następujących dostawców poczty elektronicznej: (1) dla co najmniej 500 000 użytkowników, (2) dla 500 000 aktywnych kont pocztowych, lub (3) dla podmiotów publicznych. Jednocześnie z Oceny Skutków Regulacji wynika, że na etapie projektowania ustawy nie zgromadzono informacji o liczbie dostawców poczty elektronicznej, którzy zostaną objęci nowymi regulacjami. Potwierdza to fakt, że w tabeli w pkt 4 Oceny Skutków Regulacji dotyczącej podmiotów, na które oddziałuje Projekt ustawy, przy oznaczeniu dostawców poczty elektronicznej widnieje informacja: *„brak danych".* Tymczasem w ocenie Spółki przewidziany w Projekcie ustawy próg 500 000 (użytkowników lub aktywnych kont pocztowych) jest zdecydowanie zbyt wysoki, przez co nowe obowiązki wynikające z Projektu ustawy mogłyby dotyczyć jedynie bardzo niewielkiego fragmentu rynku dostawców poczty elektronicznej.	Przy projektowaniu regulacji konieczne jest zachowanie równowagi pomiędzy obowiązkami nakładanymi na dostawców poczty elektronicznej a środkami bezpieczeństwa. Nałożenie nowych obowiązków na wszystkich dostawców poczty elektronicznej mogłoby nieproporcjonalnie dotknąć małych i średnich przedsiębiorców.

			Spółka wskazuje, że dla dalszych prac nad Projektem ustawy przydatnym może być aktualizowany na bieżąco (ostatnia aktualizacja z dnia 7 lipca 2022 roku) ranking firm hostingowych w Polsce dostępny pod adresem toplOO.webhostingtalk.pl, prowadzony przez webhostingtalk.pl spółka z ograniczoną odpowiedzialnością (KRS: 0000695069) - por. kopia rankingu firm hostingowych w Polsce toplOO.webhostingtalk.pl stanowiąca załącznik do niniejszego pisma. Mając na uwadze powyżej przywołany ranking, w ocenie Spółki uzasadnionym byłoby, aby w miejsce przewidzianego w Projekcie ustawy progu 500 000 (użytkowników lub aktywnych kont pocztowych) wprowadzić próg 50 000 (użytkowników lub aktywnych kont pocztowych). Alternatywnie można rozważyć również powiązanie nowych obowiązków z liczbą domen, dla których serwer podmiotu będącego dostawcą usługi poczty elektronicznej jest autorytatywny -tutaj Spółka proponuje próg 25 000 nazw domen, dla których serwer dostawcy usługi poczty elektronicznej jest autorytatywny. Jako dodatkowe uzasadnienie wskazać można, że na mocy ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa w związku z rozporządzeniem Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, za dostawcę usługi kluczowej w zakresie prowadzenia autorytatywnego serwera DNS może zostać uznany podmiot, który świadczy	

			usługi DNS minimalnie dla 100 000 nazw domen, dla których serwer jest autorytatywny. W kontekście powyższego, w ocenie Spółki tym bardziej uzasadnione jest by obniżyć próg przewidziany w Projekcie ustawy, skoro przy obowiązkach wynikających z ustawy o krajowym systemie cyberbezpieczeństwa (o zdecydowanie większym ciężarze gatunkowym) przewidziano zdecydowanie mniejszy próg, uzależniony od liczby nazw domen, dla których serwer jest autorytatywny. Można dostrzec tutaj analogię do liczby użytkowników poczty elektronicznej lub aktywnych kont pocztowych, o których mowa w Projekcie ustawy. Pozwoliłoby to wyeliminować negatywny efekt (jak można zakładać - nieoczekiwany przez projektodawcę) związany z objęciem nowymi regulacjami jedynie niewielkiego procentu podmiotów będących dostawcami komercyjnej usługi poczty elektronicznej, który to efekt w konsekwencji nie przyczyniłby się do zrealizowania założeń Projektu ustawy w zakresie znaczącego zwiększenia poziomu bezpieczeństwa w komunikacji elektronicznej.	
91.	Nazwa.pl sp. z o.o.	Art. 12 ust. 1	Spółka pozytywnie ocenia przewidziany w Projekcie ustawy obowiązek wprowadzenia przez dostawców poczty elektronicznej mechanizmów SPF (Sender Privacy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail) oraz obowiązek korzystania z takich mechanizmów przez podmiot publiczny. Spółka jednocześnie rekomenduje, aby w sposób jednoznaczny wyjaśnić, że obowiązkowe jest stosowanie wszystkich trzech mechanizmów (jak wynika z Projektu ustawy), a nie	**Uwaga wyjaśniona** W ocenie projektodawcy wskazywanie konkretnych rozwiązań w zakresie bezpieczeństwa jest techniką stosowaną tylko gdy jest to absolutnie niezbędne – tak jak w tym przypadku. Na podmiotach publicznych spoczywa również ogólny obowiązek zapewnienia bezpieczeństwa swoich systemów w tym poczty. W związku z tym popieramy stosowanie rozwiązania takiego jak

			tylko jednego z nich (jak wynika z uzasadnienia Projektu ustawy). Stosowanie tylko jednego z tych zabezpieczeń w sposób oczywisty nie chroni przed zagrożeniami, które stały się podstawą do przyjęcia Projektu ustawy. Jednocześnie Spółka wskazuje, że w ocenie Spółki nieprawidłowym jest brak w Projekcie ustawy wymogu stosowania zabezpieczenia DNSSEC. Stosowanie DNSSEC powinno stać się - oprócz SPF, DMARC oraz DKIM - kluczowym filarem bezpieczeństwa w Internecie i rozwiązaniem służącym zwalczaniu nadużyć w komunikacji elektronicznej. W ocenie Spółki, weryfikowanie zabezpieczeń SPF/DKIM/DMARC, które opierają się na informacjach z DNS, z jednoczesnym pozostawieniem możliwości fałszowania informacji w DNS, nie będzie wystarczającą ochroną użytkowników. Z tego względu, w ocenie Spółki, Projekt ustawy powinien przewidywać również obowiązek stosowania rozwiązania zabezpieczającego przed możliwością fałszowania informacji przekazywanych przez system DNS, jakim jest uznawany powszechnie standard, tj. DNSSEC.	DNSSEC, ale równocześnie nie chcemy narzucać go wszystkim podmiotom.
92.	Unia Metropolii Polskich	Art. 12	**Uwaga zasadnicza 1.** – przepis w naszej ocenie jest niezasadny oraz nie potrzebny. Odpowiednie wymagania w tym zakresie wynikają już z zasad oceny ryzyka z KRI dotyczących bezpieczeństwa informacji. Być może należy wzmocnić w tym zakresie przepisy KRI – które jak wiadomo nie zostały wdrożone w terminie.	**Uwaga nieuwzględniona** Przepis ten przyczyni się do wzrostu bezpieczeństwa poczty elektronicznej. Należy też zaznaczyć, że kolejne przepisy precyzują rolę CSIRT NASK w tej kwestii: „CSIRT NASK publikuje na swojej stronie internetowej informację na temat standardów sieciowych RFC (Request for Comments) z odniesieniem do dokumentów umieszczonych na stronach internetowych organizacji Internet Engineering Task Force, które

				składają się na aktualną wersję opisów mechanizmów SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail)."
93.	Unia Metropolii Polskich	Art. 12	**Uwaga zasadnicza 2.** Brak wskazania skutków finansowych dla wprowadzonych obowiązków. Czy i w jakim zakresie wpłynie to na koszt korzystania z usług.	**Uwaga wyjaśniona** Należy zauważyć, że zaproponowane rozwiązania nie wiążą się z istotnym nakładem finansowym i nie powinny wymagać zatrudniania dodatkowych osób do ich skutecznego wprowadzenia, a ich wprowadzenie nie powinno zająć więcej niż kilka dni roboczych.
94.	Unia Metropolii Polskich	Art. 12	Przepis jest nieprawidłowo skonstruowany. Obowiązki podmiotu publicznego powinny być zawarte w tym przypadku w ustawie stanowiącej podstawę działania podmiotów w tym zakresie albo w KSC albo chociażby w ustawie o informatyzacji.	**Uwaga nieuwzględniona** Projektowany akt prawny znajduje się na styku dziedziny prawa telekomunikacyjnego i wyodrębniającego się materialnego prawa administracyjnego z zakresu cyberbezpieczeństwa. Z tego względu, a także ze względu na doniosłość materii regulowanej, zasadne jest aby przepisy te znalazły się w odrębnym akcie prawnym.
95.	Unia Metropolii Polskich	Art. 12	Przepis w naszej ocenie łamie zasadne neutralności technologicznej. Wymagania konkretne dot. Mechanizmów powinny być zawarte w rozporządzeniu.	**Uwaga nieuwzględniona** Nie można zgodzić się z zaproponową zmianą. Należy podkreślić, że obowiązki powinny być nakładane w drodze ustawy, a nie rozporządzenia. Ponadto, wskazane w przepisie mechanizmy SPF, DKIM, DMARC są najbardziej rozpowszechnione. Przepis nie zabrania stosowania dodatkowo innych mechanizmów uwierzytelnienia.

96.	Unia Metropolii Polskich	Art. 12	Brak przepisu przejściowego dla podmiotów publicznych na dostosowanie się do tego wymagania. Obowiązek wchodzi włącznie z ustawą, co w przypadku krótkiego okresu nie jest w tym przypadku możliwe do dotrzymania.	**Uwaga częściowo uwzględniona** Okres *vacatio legis* jest wystarczający na realizację nowych obowiązków. Ustawienie odpowiednich mechanizmów nie powinno zająć więcej niż kilka dni roboczych.
97.	Unia Metropolii Polskich	Art. 12	Przepis nie przewiduje skutków dla zobowiązań umownych wprowadzenia nowego obowiązku np. wygaśnięcia umów ex lege, podstawy do wypowiedzenia umowy bez terminu wypowiedzenia, lub innego mechanizmu dającego podmiotom publicznym szansę na dostosowanie się do nowego wymagania.	**Uwaga uwzględniona** Zostanie dodany przepis przejściowy, zgodnie z którym dostawca poczty elektronicznej, który świadczy usługę poczty elektronicznej na podstawie umowy, której stroną jest podmiot publiczny, obowiązującej w dniu wejścia w życie ustawy, jest obowiązany w terminie 3 miesięcy od dnia wejścia w życie ustawy do spełnienia wymagań, o których mowa w art. 15 ust. 1. 2. Jeżeli dostawca poczty elektronicznej nie spełni wymagań w terminie, o którym mowa w ust. 1, umowa ulega może zostać jednostronnie rozwiązania przez podmiot publiczny a dostawcy poczty elektroniczne nie przysługują roszczenia z tego tytułu.
98.	Unia Metropolii Polskich	Art. 12	Prezes UKE ustrojowo nie jest podmiotem upoważnionym do prowadzenia takiej kontroli, gdyż nie jest ona prowadzona w stosunku do jst jako przedsiębiorcy telekomunikacyjnego. Ewentualna kontrola powinna być prowadzona nie przez podmiot regulacyjny a administracyjny.	**Uwaga nieuwzględniona** Materia tego przepisu dotyczy kwestii komunikacji, która znajduje się we właściwości Prezesa Urzędu Komunikacji Elektronicznej.

99.	Polskie Towarzystwo Informatyczne Izba Rzeczoznawców	Art. 12 ust. 1	**ad Art. 12. ust. 1.** Dostawca poczty elektronicznej: 1) dla co najmniej 500 000 użytkowników, 2) dla podmiotu publicznego, lub 3) obsługujący co najmniej 500 000 aktywnych kont pocztowych – ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail). <u>Propozycja PTI</u> Zmodyfikować zapis powyższego ustępu na poniższy (opis modyfikacji w komentarzu): *Dostawca poczty elektronicznej:* *1) dla co najmniej 500 000 użytkowników,* *2) dla podmiotu publicznego, lub* *3) obsługujący co najmniej 500 000 zarejestrowanych kont pocztowych* *– jest zobowiązany do wyboru i do stosowania jednego lub wielu ze znanych mechanizmów potwierdzania wiarygodności podanego nadawcy mejla, w szczególności takich jak SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance), DKIM (DomainKeys Identified Mail).*	**Uwaga nieuwzględniona** Wskazane w przepisie mechanizmy SPF, DKIM, DMARC są najbardziej rozpowszechnione. Przepis nie zabrania stosowania dodatkowo innych mechanizmów uwierzytelnienia.

			Komentarz PTI Nie jest znana definicja, czym jest aktywne konto pocztowe. Wiele zarejestrowanych kont może być latami nieaktywnych, ale być dla ich właściciela użytecznymi. Jedynym kryterium dla obsługującego konta jest opłacenie lub spełnianie określonych wymagań. W związku z tym w propozycji zastąpiono określenie „aktywnych" na określenie „zarejestrowanych". W propozycji PTI nie ma wymuszania stosowania wymienionych mechanizmów (wszystkich lub jednego z nich, jak SPF, DMARC, DKIM), gdyż istnieją jeszcze inne metody (ADSP, VBR, iprev, DNSWL). W związku z tym modyfikacja ogranicza się do tego, iż dostawcy mają wyszukiwać i stosować jeden z wybranych (najlepszych) mechanizmów potwierdzania wiarygodności prawdziwości podanego nadawcy mejla. Natomiast obie redakcje budzą trzy wątpliwości. Po pierwsze dlaczego pomija się mniejszych dostawców usług poczty elektronicznej oraz dostawców zagranicznych, często szczególnie nadużywających, nawet w celach przestępczych komunikacji elektronicznej. Wydaje się, że konieczne jest określenie możliwych do realizacji sankcji wobec takich przypadków. Po drugie nie jest jasna intencja twórców propozycji jakie warunki 1), 2), 3) ma spełnić dostawca – czy łącznie 1) i 2) lub 3), czy dowolny z tych trzech? Jeśli łącznie 1) i 2), to bardziej klarownym byłoby połączenie 1) i 2). Aczkolwiek to by wyłączyło obsługę podmiotów publicznych z mniej niż 500 tys. użytkowników, co jest	

			z pewnością wbrew intencjom autorów propozycji, gdyż prawdopodobnie w skali kraju może nie być ani jednego podmiotu publicznego z taką liczbą użytkowników. Proponujemy więc z wyliczenia usunąć spójnik „lub", a przed dwukropkiem dodać „spełniający co najmniej jeden z poniższych warunków". Po trzecie brak jest uzasadnienia dla liczby 500 tysięcy użytkowników/kont. Powinno się ono znaleźć co najmniej w dokumencie OSR. <u>Komentarz ogólny</u> W odniesieniu do całej treści ustawy i w szczególności do art. 1 – projektowana regulacja nie odnosi się do innych niż ujęte w propozycji formy komunikacji elektronicznej takie jak komunikatory oraz media społecznościowe, gdzie szczególnie ostatnio silnie rośnie nadużywanie wysyłania oraz publikowania treści dezinformujących oraz wymuszających szkodliwe dla odbiorcy działania. W obecnej postaci ustawa tylko częściowo będzie spełniać rolę zwalczania nadużyć w komunikacji elektronicznej.	
100	IAB Polska	Art. 14 ust. 1-2	**UWAGA** Art. 14 ust. 1 projektu ustawy przewiduje, że przedsiębiorcy telekomunikacyjni będą mogli przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć telekomunikacyjnych. Wyjątkiem od zasady, którą ma być	**Uwaga nieuwzględniona** Przetwarzanie treści komunikatu może stanowić bardzo istotną ingerencję w prawo do prywatności. Dyrektywa o prywatności 2002/58/UE w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby

			brak możliwości przetwarzania komunikatu na potrzeby zwalczania nadużyć, ma być identyfikowanie, zapobieganie i zwalczanie smishingu – w tym konkretnym przypadku projekt ustawy dopuszcza przetwarzanie również komunikatu (art. 14 ust. 2 projektu ustawy). Zacząć należy od tego, że tak sformułowany przepis (art. 14 ust. 1 i 2) obejmuje dwa różne stany faktyczne. Pierwszy to przetwarzanie danych „własnych" przedsiębiorcy telekomunikacyjnego na potrzeby zwalczania nadużyć (bez udostępniania takich danych innym przedsiębiorcom telekomunikacyjnym). Drugi to wzajemne udostępnianie danych pomiędzy przedsiębiorcami telekomunikacyjnymi celem zwiększenia skuteczności narzędzi anty-fraudowych. W zakresie odnoszącym się do wzajemnego udostępniania danych pomiędzy przedsiębiorcami telekomunikacyjnymi należy zauważyć, że bez możliwości wymiany informacji na temat komunikatu elektronicznego skuteczność współpracy międzyoperatorskiej na rzecz zwalczania nadużyć będzie znacznie mniejsza niż mogłaby być, gdyby takiego ograniczenia nie było. O ile wzajemne udostępnianie komunikatu ma być dopuszczalne w przypadku smishingu (wiadomości SMS), o tyle taka wymiana nie będzie możliwa w przypadku nadużyć, których nośnikiem jest np. wiadomość MMS. Przestępcy wykorzystują zarówno wiadomości SMS jak i MMS do popełniania nadużyć, a o tym, czy wiadomość SMS albo MMS jest nośnikiem nadużycia o charakterze phishingowym decyduje jej treść – bez jej przetworzenia nie ma możliwości zidentyfikowania wiadomości nadużyciowych.	inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadku wynikające z prawa UE lub krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektroniczne. O ile zatem w przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-a jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do celu jakim jest ochrona przed nadużyciami, o tyle w przypadku innych rodzajów nadużyć takiego brak takiego uzasadnienia. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Dodatkowo, w przypadku smishingu – jako nadużycia zdefiniowanego i szerzej opisanego w ustawie, wprowadza się regulację „wzorca wiadomości", wraz z należytymi uprawnieniami organów (CSIRT NASK). Przetwarzanie komunikatu

			Jednocześnie nie ma żadnych podstaw do różnicowania zakresu dopuszczalnego przetwarzania danych w zależności od tego, czy nośnikiem nadużycia jest SMS czy MMS (albo inna forma komunikatu). O ile wyłączenie możliwości wzajemnego udostępniania komunikatu (za wyjątkiem smishingu) ograniczy skuteczność współpracy międzyoperatorskiej i utrudni skuteczną walkę z nadużyciami w komunikacji elektronicznej, to wyłączenie możliwości przetwarzania komunikatu tam, gdzie przetwarzanie ma dotyczyć „własnych" danych przedsiębiorcy telekomunikacyjnego (tj. danych dostępnych z poziomu sieci i usług świadczonych przez przedsiębiorcę telekomunikacyjnego), w zasadzie uniemożliwi przedsiębiorcom telekomunikacyjnym zwalczanie nadużyć, w których o nadużyciowym charakterze decyduje treść komunikatu (innych niż smishing, który nie będzie objęty wyłączeniem dotyczącym komunikatu). W praktyce oznacza to, że przedsiębiorcy telekomunikacyjni nie będą mogli podejmować działań mających na celu zwalczanie nadużyć, których nośnikiem jest np. wiadomość MMS (pamiętajmy, że wiadomości MMS nie mieszczą się, i na obecnym etapie nie powinny mieścić się, w definicji smishingu). **PROPOZYCJA:** W naszej ocenie wyłączenie możliwości przetwarzania i udostępniania komunikatu jest szkodliwe z perspektywy celu, jakim ma być skuteczna walka z nadużyciami, w związku z czym obecne ust. 1 i 2 w art. 14 projektu ustawy	elektronicznego powinno być ograniczone wyłącznie do zwalczania nadużyć ściśle w ustawie określonych.

			powinny zostać zastąpione przepisem o następującym brzmieniu: *"Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej."* Przepis w takim kształcie pozwala na przetwarzanie wszystkich informacji, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, zarówno jeśli chodzi o przetwarzanie „własnych" danych jak i o ich wzajemne udostępnianie, pozwalając na walkę z obecnie znanymi formami nadużyć, jak i z takimi nadużyciami, które dopiero pojawią się w przyszłości, bez nieuzasadnionego różnicowania zakresu dopuszczalnego przetwarzania danych od tego, jaka usługa telekomunikacyjna (SMS, MMS itd.) jest nośnikiem nadużycia. Jednocześnie zaproponowany przepis jednoznacznie przesądza, że przetwarzane i wzajemnie udostępniane mogą być tylko te dane, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, co zapobiegnie przetwarzaniu i wzajemnym udostępnianiu danych innych niż niezbędne. Przykładowo, przy takim zapisie komunikat będzie mógł być przetwarzany i wzajemnie udostępniany tylko i wyłącznie wtedy, gdy o nadużyciom charakterze decyduje treść komunikatu (phishingowe SMS oraz MMS). Jednocześnie komunikat nie będzie przetwarzany i wzajemnie udostępniany w przypadku takich nadużyć,	

			w których treść komunikatu nie ma znaczenia dla oceny, czy ruch ma charakter nadużyciowy.	
101	Polska Izba Komunikacji Elektronicznej	Art. 14	**Przetwarzanie i udostępnianie informacji objętych tajemnicą telekomunikacyjną *(art. 14)*** Wprowadzenie odstępstwa od obowiązku zachowania tajemnicy telekomunikacyjnej przy przetwarzaniu i udostępnianiu danych w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej należy skrytykować o tyle, że przepisy art. 13 są w tym zakresie nieprecyzyjne. Zdaniem Izby należy konkretnie wyszczególnić cele przetwarzania i udostępniania danych, aby wykluczyć potencjalne niepożądane wykorzystanie informacji. Ponadto, w opinii Izby należy skonstruować przepis w taki sposób, by warunkiem odstępstwa od nałożonej tajemnicy telekomunikacyjnej było wykorzystanie danych na potrzeby spełnienia konkretnych celów wskazanych w przepisie. Regulacja wprost powinna określać, że to odstępstwo możliwe jest wyłącznie przy wypełnianiu obowiązków nałożonych w drodze ustawy, w szczególności tych z art. 4 ust. 6 oraz art. 8. Poważne zastrzeżenia Izby budzi przede wszystkim ujęte w ogólnym stopniu przyzwolenie na przetwarzanie i wzajemne udostępnianie informacji. W przypadku niedoprecyzowania tej regulacji istnieje ryzyko, że przedsiębiorcy telekomunikacyjni będą wykorzystywać dane objęte tajemnicą telekomunikacyjną dla własnej korzyści, przygotowując na ich podstawie chociażby działania marketingowe. Warto również rozważyć wprowadzenie sankcji administracyjnych (np. finansowych) za naruszenie tego przepisu, by możliwie ograniczyć ryzyko nadużycia.	**Uwaga nieuwzględniona** Zgodnie z aktualnym brzmieniem przepisów projektu odstępstwo od tajemnicy telekomunikacyjnej dotyczy wyłącznie przetwarzania i udostępniania celem identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej. Wskazany w przepisie cel wyczerpuje znamiona wykorzystywania danych na potrzeby spełnienia konkretnego celu – zgodnie z przekazaną uwagą.

102	Polska Izba Informatyki i Telekomunikacji	Art. 14 ust. 1	**Przetwarzanie komunikatu na potrzeby zwalczania nadużyć (art. 14 ust. 1 i 2 projektu ustawy).** Art. 14 ust. 1 projektu ustawy przewiduje, że przedsiębiorcy telekomunikacyjni będą mogli przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć telekomunikacyjnych. Wyjątkiem od zasady, którą ma być brak możliwości przetwarzania komunikatu na potrzeby zwalczania nadużyć, ma być identyfikowanie, zapobieganie i zwalczanie smishingu – w tym konkretnym przypadku projekt ustawy dopuszcza przetwarzanie również komunikatu (art. 14 ust. 2 projektu ustawy). Zacząć należy od tego, że tak sformułowany przepis (art. 14 ust. 1 i 2) obejmuje dwa różne stany faktyczne. Pierwszy to przetwarzanie danych „własnych" przedsiębiorcy telekomunikacyjnego na potrzeby zwalczania nadużyć (bez udostępniania takich danych innym przedsiębiorcom telekomunikacyjnym). Drugi to wzajemne udostępnianie danych pomiędzy przedsiębiorcami telekomunikacyjnymi celem zwiększenia skuteczności narzędzi anty-fraudowych. W zakresie odnoszącym się do wzajemnego udostępniania danych pomiędzy przedsiębiorcami telekomunikacyjnymi należy zauważyć, że bez możliwości wymiany informacji na temat komunikatu elektronicznego skuteczność współpracy międzyoperatorskiej na rzecz zwalczania nadużyć będzie znacznie mniejsza niż mogłaby być, gdyby takiego ograniczenia nie było. O ile wzajemne udostępnianie	**Uwaga nieuwzględniona** Przetwarzanie treści komunikatu może stanowić bardzo istotną ingerencję w prawo do prywatności. Dyrektywa o prywatności 2002/58/UE w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadku wynikające z prawa UE lub krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektroniczne. O ile zatem w przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-a jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do

			komunikatu ma być dopuszczalne w przypadku smishingu (wiadomości SMS), o tyle taka wymiana nie będzie możliwa w przypadku nadużyć, których nośnikiem jest np. wiadomość MMS. Przestępcy wykorzystują zarówno wiadomości SMS jak i MMS do popełniania nadużyć, a o tym, czy wiadomość SMS albo MMS jest nośnikiem nadużycia o charakterze phishingowym decyduje jej treść – bez jej przetworzenia nie ma możliwości zidentyfikowania wiadomości nadużyciowych. Jednocześnie nie ma żadnych podstaw do różnicowania zakresu dopuszczalnego przetwarzania danych w zależności od tego, czy nośnikiem nadużycia jest SMS czy MMS. O ile wyłączenie możliwości wzajemnego udostępniania komunikatu (za wyjątkiem smishingu) ograniczy skuteczność współpracy międzyoperatorskiej i utrudni skuteczną walkę z nadużyciami w komunikacji elektronicznej, to wyłączenie możliwości przetwarzania komunikatu tam, gdzie przetwarzanie ma dotyczyć „własnych" danych przedsiębiorcy telekomunikacyjnego (tj. danych dostępnych z poziomu sieci i usług świadczonych przez przedsiębiorcę telekomunikacyjnego), w zasadzie uniemożliwi przedsiębiorcom telekomunikacyjnym zwalczanie nadużyć, w których o nadużyciowym charakterze decyduje treść komunikatu (innych niż smishing, który nie będzie objęty wyłączeniem dotyczącym komunikatu). W praktyce oznacza to, że przedsiębiorcy telekomunikacyjni nie będą mogli podejmować działań mających na celu zwalczanie nadużyć, których nośnikiem jest np. wiadomość MMS (pamiętajmy, że wiadomości	celu jakim jest ochrona przed nadużyciami, o tyle w przypadku innych rodzajów nadużyć takiego brak takiego uzasadnienia. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Dodatkowo, w przypadku smishingu – jako nadużycia zdefiniowanego i szerzej opisanego w ustawie, wprowadza się regulację „wzorca wiadomości", wraz z należytymi uprawnieniami organów (CSIRT NASK). Przetwarzanie komunikatu elektronicznego powinno być ograniczone wyłącznie do zwalczania nadużyć ściśle w ustawie określonych.

			MMS nie mieszczą się i nie powinny mieścić się, w definicji smishingu). W naszej ocenie wyłączenie możliwości przetwarzania i udostępniania komunikatu jest wadliwe z perspektywy celu, jakim ma być skuteczna walka z nadużyciami, w związku z czym obecne ust. 1 i 2 w art. 14 projektu ustawy powinny zostać zastąpione przepisem o następującym brzmieniu: *Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.* Przepis w takim kształcie pozwala na przetwarzanie wszystkich informacji, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, zarówno jeśli chodzi o przetwarzanie „własnych" danych jak i o ich wzajemne udostępnianie, pozwalając na walkę z obecnie znanymi formami nadużyć, jak i z takimi nadużyciami, które dopiero pojawią się w przyszłości, bez nieuzasadnionego różnicowania zakresu dopuszczalnego przetwarzania danych od tego, jaka usługa telekomunikacyjna (SMS, MMS) jest nośnikiem nadużycia. Jednocześnie zaproponowany przepis jednoznacznie przesądza, że przetwarzane i wzajemnie udostępniane mogą być tylko te dane, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, co zapobiegnie przetwarzaniu i wzajemnym udostępnianiu danych innych niż niezbędne. Przykładowo, przy takim zapisie komunikat będzie mógł być przetwarzany i wzajemnie udostępniany tylko i	

			wyłącznie wtedy, gdy o nadużyciom charakterze decyduje treść komunikatu (phishingowe SMS oraz MMS). Jednocześnie komunikat nie będzie przetwarzany i wzajemnie udostępniany w przypadku takich nadużyć, w których treść komunikatu nie ma znaczenia dla oceny, czy ruch ma charakter nadużyciowy. Jeśli jednak z jakichś powodów powyższa propozycja brzmienia przepisu nie zostanie zaakceptowana przez Projektodawcę proponujemy alternatywne brzmienie art. 14 ust. 1 i 2 projektu ustawy: *Art. 14. 1. Przedsiębiorcy telekomunikacyjni mogą przetwarzać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, niezbędne do identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej.* *2. Przedsiębiorcy telekomunikacyjni mogą wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, niezbędne do identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej.* Tak skonstruowany przepis, zapewni przedsiębiorcom telekomunikacyjnym możliwość przetwarzania i wzajemnego udostępniania danych w zakresie stanowiącym absolutne minimum niezbędne do skutecznego identyfikowania, zapobiegania i zwalczania nadużyć. Ponadto przedstawiona powyżej propozycja brzmienia art. 14 ust. 1 i 2 porządkuje analizowane zagadnienie, rozdzielając obszar przewarzania „własnych” danych (ust. 1) od wzajemnego udostępniania danych (ust. 2), precyzyjnie określając	

			zakres danych, które mogą być przetwarzane w każdym z tych dwóch przypadków: • na podstawie ust. 1 przedsiębiorca telekomunikacyjny będzie miał możliwość przetwarzania (ale nie wzajemnego udostępniania) danych (w tym komunikatu elektronicznego) niezbędnych do zwalczania wszystkich form nadużyć w komunikacji elektronicznej (SMS, MMS, w których o nadużyciowym charakterze decyduje treść komunikatu); • na podstawie ust. 2 przedsiębiorcy telekomunikacyjni będą mogli wzajemnie udostępniać informacje niezbędne do zwalczania nadużyć, za wyjątkiem komunikatu elektronicznego.	
103	Polska Izba Informatyki i Telekomunikacji	art. 13 oraz art. 14 ust. 1 – 3	**Dopuszczalny zakres przetwarzania danych związanych ze zwalczaniem wiadomości *smishingowych*** (art. 13 oraz art. 14 ust. 1 – 3 projektu ustawy). Wydaje się, że zachodzi wewnętrzna sprzeczność, a co najmniej niespójność wewnętrzna, jeśli chodzi o przepisy określające zasady przetwarzania danych na potrzeby zwalczania smishingu (SMS). Co więcej, obecna konstrukcja projektowanych przepisów rodzi uzasadnione obawy o spójność przetwarzania danych telekomunikacyjnych na gruncie projektowanej ustawy z zasadami przetwarzania tych danych wynikającymi z ustawy – Prawo telekomunikacyjne. Jeśli chodzi o spójność w ramach projektowanej ustawy to należy zwrócić uwagę, że pierwszym przepisem	**Uwaga nieuwzględniona** Art. 13 projektowanej ustawy wskazuje cele przechowywania związane z danymi o niewykonanych usługach telekomunikacyjnych w ramach prowadzenia rejestru. Wskazano, iż przechowywanie danych następuje w zakresie umożliwiającym rozpatrzenie reklamacji. Art. 14 projektowanej ustawy wskazuje w szerszym zakresie niż art. 13 dane możliwe do przetwarzania (nie tylko przechowywania), których przetwarzanie konieczne jest również do zrealizowania obowiązków wynikających z ustawy. Tym samym obejmuje ona zarówno – komplementarnie z art. 13 –przetwarzanie danych celem dochodzenia roszczeń, jak i realizację obowiązków przez przedsiębiorców

			projektowanej ustawy, który reguluje przetwarzanie danych na potrzeby zwalczania smishingu jest art. 13 ust. 1 projektu ustawy, który przewiduje, że przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji danych o usługach, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku (art. 4 ust. 6) i uprawnienia (art. 7) do blokowania wiadomości smishingowych (SMS), tak, aby przedsiębiorca telekomunikacyjny był w stanie wywiązać się z obowiązku rozpatrzenia reklamacji, która w takim przypadku może być wniesiona przez abonenta. Jednocześnie art. 13 ust. 2 określa czas, przez jaki przedsiębiorca telekomunikacyjny ma przechowywać te dane (co najmniej przez okres 12 miesięcy, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu). Jak widać więc art. 13 ust. 1 i 2 określają zasady przetwarzania danych związanych z blokowaniem smishingowych wiadomości SMS. Okazuje się jednak, że również art. 14 ust. 3 projektu ustawy określa zasady przetwarzania danych związanych ze zwalczaniem smishingowych wiadomości SMS, ale w sposób odmienny od art. 13, gdyż w art. 14 ust. 3 wskazany jest enumeratywnie katalog przepisów projektu ustawy, których realizacja legalizuje przetwarzanie tych danych (wskazane są art. 3 ust. 2, art. 4 ust. 6, art. 7, art. 8 a także na cele związane z dochodzeniem roszczeń – taka redakcja przepisów zmusza do uznania, że przetwarzanie będzie legalne tylko w tych przypadkach). Art. 13 dotyczy przetwarzania informacji o niewykonanych usługach w związku ze zwalczaniem smishingu, a art. 14 ust. 3 dotyczy przetwarzania treści smishingowych wiadomości SMS (ust. 3 pkt 1)) oraz danych o niewykonanych usługach	związanych z walką z nadużyciami w komunikacji elektronicznej. Celem rejestru nie jest zaś realizacja obowiązków związanych z walką z nadużyciami, zaś przechowanie danych koniecznych do ewentualnego rozpatrzenia reklamacji, rozliczalności. Przepis jest zgodny z przepisami ustawy Prawo telekomunikacyjne, wyrażonymi w art. 165 i 168, jak również z projektowanymi przepisami ustawy Prawo komunikacji elektronicznej (art. 386 ust. 2). Projektowana ustawa stanowi *lex specialis* względem ustawy - Prawo telekomunikacyjne, opierając się jednak na przepisach z niej wynikających, w tym określających okres retencji danych, jak i prawo dostępu służb do określonych danych.

			(ust. 3 pkt 2), pokrywając się w tym zakresie z art. 13 ust. 1). Sytuację dodatkowo komplikuje fakt, że art. 14 ust. 1 i 2 projektu ustawy (czytane razem) pozwalają na przetwarzanie wszystkich niezbędnych danych, w tym danych objętych tajemnicą telekomunikacyjną, na potrzeby identyfikowania, zapobiegania i zwalczania smishingu. I choć sama regulacja zawarta w art. 14 ust. 1 i 2 jest bardzo potrzebna, to oczywistym staje się, że regulacje zawarte w art. 13 oraz art. 14 ust. 1 – 3 są wewnętrznie niespójne, przynajmniej jeśli chodzi o zwalczanie smishingu, gdyż każdy z tych przepisów dotyczy zwalczania smisningu, ale zakres dopuszczalnego przetwarzania danych wyznacza odmiennie. Ponadto projektowana ustawa w zakresie dotyczącym przetwarzania danych powinna być tak skonstruowana, aby uniknąć konfliktu z ustawą – Prawo telekomunikacyjne, która kompleksowo reguluje zasady i zakres przetwarzania danych telekomunikacyjnych. Przykładowo, art. 14 ust. 3 projektowanej ustawy, wskazujący enumeratywnie na przypadki, w których dane mogą być przetwarzane, budzi wątpliwości co do spójności z ustawą – Prawo telekomunikacyjne, gdyż – jedynie przykładowo – wydaje się włączać możliwość przetwarzania wiadomości SMS choćby na potrzeby wywiązania się przez przedsiębiorców telekomunikacyjnych z obowiązków zapewnienia dostępu i utrwalania na rzecz uprawnionych podmiotów, sądu lub prokuratora (art. 179 ustawy – Prawo telekomunikacyjne). Biorąc pod uwagę, że ustawa - Prawo telekomunikacyjne kompleksowo reguluje zasady przetwarzania danych stanowiących tajemnicę telekomunikacyjną, a RODO	

			kompleksowo reguluje przetwarzanie danych osobowych, znacznie lepszym rozwiązaniem byłoby posłużenie się w projektowanej ustawie odesłaniem do ustawy – Prawo telekomunikacyjne oraz RODO, tak, aby zasadą było, że dane stanowiące tajemnicę telekomunikacyjną są przetwarzane na zasadach określonych w ustawie – Prawo telekomunikacyjne, a dane osobowe na zasadach określonych w RODO. W projektowanej ustawie należy natomiast uwzględnić jedynie te przepisy dotyczące przetwarzania danych, które będą stanowiły *lex specialis* wobec ogólnych zasad wynikających z Prawa telekomunikacyjnego oraz RODO – przykładem takich przepisów szczególnych powinny być projektowany art. 14 ust. 1 i 2 (jako *lex specialis* wobec ustawy - Prawo telekomunikacyjne) oraz projektowany art. 14 ust. 4 (jako wyjątek od RODO). W tym celu należy stworzyć odpowiednie przepisy odsyłające do Prawa telekomunikacyjnego i RODO oraz usunąć z projektu ustawy te przepisy, które w sposób nieuzasadniony i niespójny z ustawą – Prawo telekomunikacyjne ograniczają zakres dopuszczalnego przetwarzania danych.	
104	Związek Banków Polskich	Art. 14 ust. 1 - 2	Art. 14. 1. Przedsiębiorcy telekomunikacyjni **oraz podmioty, o których mowa w art. 106d ust. 1 i 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)** mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej, z uwzględnieniem ust. 2.	**Uwaga nieuwzględniona w związku z nieuwzględnieniem zmian w Prawie bankowym**

			2. Przedsiębiorcy telekomunikacyjni **oraz podmioty, o których mowa w art. 106d ust. 1 i 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)** mogą przetwarzać i wzajemnie udostępniać również komunikat elektroniczny w celu identyfikacji, zapobiegania i zwalczania smishingu. W związku z ewoluującymi zagrożeniami oraz coraz bardziej rozwiniętymi formami przestępczości zorganizowanej, coraz większe znaczenie ma zapewnienie efektywnej, międzysektorowej wymiany informacji prawnie chronionych. Proponujemy zatem rozszerzenie katalogu podmiotów uprawnionych do wymiany informacji, w tym informacji objętych tajemnicą telekomunikacyjną o podmioty, które na gruncie ustawy – Prawo Bankowe uprawnione są do przetwarzania informacji objętych tajemnicą bankową w razie wystąpienia określonych przesłanek przewidzianych w rt.. 106d ust. 1 pkt 1-3 ww. ustawy. Takie rozwiązanie umożliwiłoby wielostronną wymianę informacji w celu zapobiegania przestępstwom (uwzględniającą przedstawicieli sektora przedsiębiorców telekomunikacyjnych). Monetyzacja nadużyć w komunikacji elektronicznej odbywa się z wykorzystaniem elektronicznych usług finansowych co tworzy konieczność integrowania działań sektora finansowego i sektora telekomunikacyjnego, w tym poprzez stworzenie warunków prawnych do wymiany informacji z wykorzystaniem centrum wymiany i analizy informacji	

			Przepis ten koresponduje również z propozycją stosownych zmian w treści ustawy - Prawo Bankowe.	
105	IAB Polska	Art. 14 ust. 4	**UWAGA:** Artykuł 23 ust. 1 RODO pozwala krajowym prawodawcom wprowadzić przepisy służące ograniczeniu administratorom danych lub podmiotów przetwarzających zakresu obowiązków i praw przewidzianych w art. 12-22 RODO i w art. 34 RODO, a także w art. 5 RODO pod warunkiem, że: a) takie przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 RODO b) ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym i służy realizacji celów, które zostały enumeratywnie wymienione w art. 23 ust. 1 pkt a-j RODO. IAB Polska stoi na stanowisku, że proponowane w projekcie UZNKE wyłączenie stosowania art. 14 i art. 15 RODO w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego jest konieczne, aby podmioty te mogły skutecznie przeciwdziałać przestępstwom popełnianym na ich szkodę. Niemniej jednak przepis w obecnym kształcie znajdzie zastosowanie tylko w tych przypadkach, w których doszło do przestępstwa na szkodę przedsiębiorcy telekomunikacyjnego. Takie zawężenie może spowodować, że będzie to przepis martwy, gdyż w	**Uwaga uwzględniona w zakresie odwołania do nadużyć w komunikacji elektronicznej** Przepis zostanie zmieniony zgodnie z propozycją. **Uwaga uwzględniona** Proponuje się zmianę zapisu na nadużycia, wraz z odpowiednim rozbudowaniem opisu artykułu w uzasadnieniu projektu ustawy, uwzględniając przy tym art. 23 RODO.

			systemie, w którym obowiązuje domniemanie niewinności od popełnienia przestępstwa do stwierdzenie w sposób prawomocny, że przestępstwo zostało popełnione mija zazwyczaj wiele miesięcy albo i lat. Walka z nadużyciami wymaga podejmowania działań natychmiastowych. **PROPOZYCJA:** Biorąc powyższe pod uwagę proponujemy następującą zmianę brzmienia art. 14 ust. 4 projektu ustawy: *Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 14 i 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania ~~przestępstw na szkodę przedsiębiorcy telekomunikacyjnego~~ nadużyć w komunikacji elektronicznej.*	
106	Polska Izba Informatyki i Telekomunikacji	Art. 14 ust. 4	**Relacja projektowanej ustawy do RODO (art. 14 ust. 4 projektu ustawy**) Projekt ustawy w art. 14 ust. 4 zawiera potrzebny przepis, który w sposób precyzyjny wskazuje, które przepisy RODO nie będą stosowane w zakresie, w jakim jest to niezbędne do identyfikowania i zwalczania nadużyć. Niemniej jednak przepis ten, w obecnym kształcie znajdzie zastosowanie tylko w tych przypadkach, w których doszło do przestępstwa na	**Uwaga uwzględniona** Proponuje się zmianę zapisu na nadużycia, wraz z odpowiednim rozbudowaniem opisu artykułu w uzasadnieniu projektu ustawy, uwzględniając przy tym art. 23 RODO.

			szkodę przedsiębiorcy telekomunikacyjnego. Takie zawężenie może spowodować, że będzie to przepis martwy, gdyż w systemie, w którym obowiązuje domniemanie niewinności od popełnienia przestępstwa do stwierdzenie w sposób prawomocny, że przestępstwo zostało popełnione mija zazwyczaj wiele miesięcy albo i lat. Walka z nadużyciami wymaga podejmowania działań natychmiastowych. Biorąc powyższe pod uwagę proponujemy następującą zmianę brzmienia art. 14 ust. 4 projektu ustawy: *Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 14 i 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania ~~przestępstw na szkodę przedsiębiorcy telekomunikacyjnego~~ nadużyć w komunikacji elektronicznej.*	
107	Krajowa Izba Komunikacji Ethernetowej	Art. 14	Przechowywanie danych dot. smishingu W art. 14 projektu wprowadza się zasady przetwarzania i wzajemnego przekazywania zastrzeżonych danych, w tym stanowiących tajemnicę telekomunikacyjną w zakresie identyfikacji, zapobiegania i zwalczania smishingu. Izba wskazuje, że przepis ten powinien wprowadzić regulacje zapobiegające wykorzystywaniu tych danych do celów innych niż związane z smishingiem.	**Uwaga częściowo uwzględniona** Doprecyzowane zostanie uzasadnienie w zakresie przetwarzania danych. Równocześnie należy zauważyć, że Dyrektywa o prywatności 2002/58/UE w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania,

			Co więcej, należy dokładnie zdefiniować na czym ma polegać zapobieganie smishingowi i czym się ono się różni od identyfikacji tego nadużycia i jego zwalczania. Zdaniem Izby obecny zapis związany z celem „zapobiegania smishingu" może prowadzić do nadużyć ze strony MNO polegających na kontroli legalnych SMS pod pozorem zapobiegania smishingowi. Generalnie należy zwrócić uwagę, że uprawnienie z art. 14 ust. 1 i 2 projektu ustawy jest zbyt szerokie. Możliwość udostępniania komunikatów elektronicznych między przedsiębiorcami telekomunikacyjnymi jest nadmierna i powoduje, iż prywatne komunikaty użytkowników przestaną być poufne. Zapis może naruszać art. 49 Konstytucji RP, gwarantującej ochronę tajemnicy komunikowania się. Poważne zastrzeżenia Izby budzi regulacja art. 14 ust. 3 w zakresie przechowywania danych o SMS oraz o usługach, które nie zostały świadczone w związku ze zwalczaniem smishingu. Nie jest jasne o jaki zakres danych związanych z usługami SMS tutaj chodzi. Czy chodzi tu o dane z nadawcą oraz dane niedoszłych odbiorców? Izba wyjaśnia, że przy smishingu będą to dane dziesiątków tysięcy abonentów. Wątpliwości Izby budzi kwestia przechowywanie również treści zablokowanych SMS na cele związane z roszczeniami. Czy celem tej regulacji było, aby abonenci mogli w procesie reklamacyjnym otrzymywać treść SMS, których byli nadawcami, czy też których mieli być odbiorcami? W obu przypadkach Izba nie widzi powodu do przechowywania treści zablokowanego SMS (nadawca sam go posiada). Czy przechowaniu ma podlegać jeden SMS o danej treści czy wszystkie jego kopie jakie były wysyłane do tysięcy abonentów?	nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadku wynikające z prawa UE lub krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektroniczne. O ile zatem w przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-a jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do celu jakim jest ochrona przed nadużyciami, o tyle w przypadku innych rodzajów nadużyć takiego brak takiego uzasadnienia. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Obecne przepisy w odpowiedni sposób kształtują podstawę prawną do przetwarzania wiadomości. Jednym z

			Nie jest również zrozumiały zakres czasowy przez jaki przedsiębiorcy muszą przechowywać te dane. Czy chodzi tu o konieczność przechowywania wszystkich danych z art. 14 ust. 3 przez okres co najmniej 12 miesięcy? Izba zwraca uwagę, że jest to znaczące obciążenie dla przedsiębiorców telekomunikacyjnych, którzy dotychczas nie przechowywali (i nie mogli przechowywać bez zgody abonentów) blokowanych przez siebie SMS ze smishingiem. W opinii izby okres przechowywania danych o zablokowanych usługach powinien być nie dłuższy niż 30 dni, a jedynie wydłużony dla tych przypadków, w których złożono reklamację w tym czasie. 10 Ponadto Izba proponuje wprowadzenie zapisów związanych z karami za przetwarzanie i wzajemne przekazywanie danych (w tym tajemnicy telekomunikacyjnej) w celach niezwiązanych z identyfikacją i zwalczaniem smishingu. *„art. 15 ust. 2a. Na przedsiębiorcę telekomunikacyjnego, który przetwarza lub przekazuje dane, o których mowa w art. 14 ust. 1, 2 i 3 w celach niezwiązanych z identyfikacją lub zwalczaniem smishingu może zostać nałożona kara pieniężna”.* Dodatkowo Izba wskazuje, że przepisy RODO nie przewidują delegacji, aby pojedyncze ustawy krajowe mogły wyłączyć stosowanie art. 14 i 15 RODO. Ograniczenie informowania na gruncie art. 14 RODO jest przewidziane w art. 14 ust. 5 RODO. Jeśli żadna z sytuacji opisanych w tym przepisie nie zachodzi, to wówczas przedsiębiorca telekomunikacyjny ma obowiązek poinformować osobę, że przetwarza jej dane. Wyjątkiem	obowiązków przedsiębiorców komunikacji elektronicznej będzie przeciwdziałanie smishingowi. W związku z powyższym, dla zapewnienia realnej możliwości wypełnienia tego obowiązku, konieczne jest zawarcie w przepisach podstawy prawnej dla przetwarzania danych na potrzeby jego realizacji. Zawarty w przepisach okres przechowywania danych ma stanowić gwarancję dla użytkowników pozwalająca im dochodzić swoich praw w przypadku zablokowania ich wiadomości. W ocenie projektodawcy nie jest konieczne uzupełnienie ustawy o dodatkowe przepisy karne. Doprecyzowano również w przepisach kwestię stosowania RODO: „Administrator danych osobowych może wykonać obowiązek, o którym mowa w art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 rozporządzenia 2016/679, przez udostępnienie informacji, o których mowa w tych przepisach, na swojej stronie internetowej lub przez umieszczenie stosownych informacji w miejscach widocznych w siedzibie lub miejscu działania administratora danych osobowych.".

			są sytuacje opisane w art. 4 oraz 5 ustawy o ochronie danych osobowych. Przepisy RODO nie przewidują delegacji, aby można było ograniczyć stosowanie art. 14 i 15 RODO w odniesieniu do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.	
108	Krajowa Izba Komunikacji Ethernetowej	Art. 15	Kary finansowe Izba zwraca uwagę, że zawarte w art. 15 i kary pozbawienia wolności z art. 16 projektu ustawy mają być stosowane równolegle za to samo działanie przed dwie różne instytucje (Prezesa UKE i sąd), co wg izby jest nieprawidłową regulacją. Ponadto sankcje finansowe, z uwagi na ich dolegliwy charakter i potencjalnie dużą wysokość, wymagają poważnego doprecyzowania. Wyjaśnienia w projekcie ustawy wymaga kwestia odpowiedzialności finansowej podmiotów zagranicznych inicjujących lub biorących aktywnie udział w nadużyciach telekomunikacyjnych. Wg wiedzy Izby większość nadużyć w komunikacji elektronicznej jest wprowadzana do polskich sieci telekomunikacyjnych z zagranicy. Zdaniem Izby, projekt powinien przewidywać regulacje związane z karaniem podmiotów zagranicznych, które są głównym źródłem nadużyć w polskich sieciach telekomunikacyjnych. Kwestie kar finansowych powinny ulec doprecyzowaniu, za jakie konkretne czynności podlega karze finansowej przedsiębiorca telekomunikacyjny lub podmiot biorący udział w przekazywaniu komunikatów elektronicznych. Wskazujemy, że podmioty te oraz przedsiębiorcy telekomunikacyjni nie są inicjatorami smishingu czy	**Uwaga wyjaśniona** Administracyjne kary pieniężnych będą miały charakter fakultatywny. Ponadto nawet po wszczęciu postępowania będą mogły znaleźć zastosowanie przesłanki odstąpienia od ukarania określone w art. 189e i 189f KPA. Przepisy wyraźnie wskazują, które obowiązki przedsiębiorców za powiązane z odpowiedzialnością karną.

			spoofingu a jedynie wbrew ich woli ich sieci lub urządzenia są wykorzystywane do tego procederu,. Z tego względu kary finansowe powinny być związane z konkretnymi uchybieniami w zakresie zabezpieczania sieci lub urządzeń czy braku stosowania minimalnych środków zapobiegawczych. Przykładowo wskazujemy, że nie powinien być karany przedsiębiorca telekomunikacyjny, za przesłanie SMS zgodnych ze wzorcem (ale nie będących smishingiem), gdyż wg jego wiedzy pochodziły one z legalnego źródła (np. firmy kurierskiej będącej jego klientem). Nie powinno się również wprowadzać kary finansowej za niewykonanie obowiązku blokowania spoofingu, gdyż powodem takiego zaniechaniu w większości przypadków będzie brak środków technicznych do identyfikacji spoofingu. Karze finansowej powinno podlegać zaniechanie zwalczania spoofingu a nie nieskuteczne jego zwalczanie.	
109	Unia Metropolii Polskich	Art. 15 ust. 5	Przepisy powinny w tym zakresie dawać możliwość skutecznej realizacji tego obowiązku z uwagi poprzez rozwiazywanie umów, wygaśniecie umów itp. odpowiednie vacatio legis itp.	**Uwaga wyjaśniona** Zawarte w ustawie *vacatio legis* oraz przepisy przejściowe kompleksowo regulują tę sytuację.
110	Unia Metropolii Polskich	Art. 15 ust. 5	nie jest zasadne nakładanie kary w przypadku braku określenia, chociażby szacunkowych skutków finansowych wykonania tych obowiązków.	**Uwaga wyjaśniona** Należy zauważyć, że zaproponowane rozwiązania nie są związane z istotnymi kosztami i nie powinny wymagać zatrudniania dodatkowych osób do ich skutecznego wprowadzenia.
111	Unia Metropolii Polskich	Art. 15 ust. 5	Nawet jeżeli przepis o karze zostanie pozostawiony – co w naszej ocenie nie jest zasadne - to nie ma uzasadnienia aby każe podlegał kierownik podmiotu. Kara powinna zostać nałożona na podmiot, dlatego też, że obowiązek	**Uwaga nieuwzględniona** Nałożenie kary na podmiot publiczny finansowany z budżetu państwa nie będzie prowadziła do realizacji celów ustawy. Kara

			jest nałożony na podmiot tak jak większość przepisów związanych z bezpieczeństwem.	musi wywołać realną dolegliwość aby realizować swój cel w zakresie prewencji. Z tego względu, w przypadku podmiotów publicznych musi być nakładana na kierownika jednostki. Nałożenie kary na jednostkę prowadziłoby tylko do przesuwania środków publicznych z jednego miejsca w inne.
112	Unia Metropolii Polskich	Art. 15 ust. 5	należy w uzasadnieniu wskazać, czy do stosowania kar stosuje się przepisy o kpa ?.	**Uwaga Wyjaśniona** W zakresie kar stosowane będą przepisy niniejszej ustawy w zw. z odpowiednimi przepisami KPA.
113	Krajowa Izba Komunikacji Ethernetowej	Art. 16	Kary pozbawienia wolności Zdaniem Izby należy wskazywać, że sankcjom karnym podlegają wyłącznie podmioty, które świadomie inicjują lub wspierają określone nielegalne działania. Obecny zapis jest nieprecyzyjny, gdyż nie wskazuje, jaki podmiot podlega sankcjom karnym i za jakie konkretnie działania. Przykładowo, nie powinien podlegać sankcjom karnym przedsiębiorca telekomunikacyjny czy integrator SMS, jeśli nie brał on udział świadomie w wykorzystywaniu jego sieci lub urządzeń przez oszusta (pomocnictwo). Kwestia braku odpowiednich zabezpieczeń powinna być wyłączenie domeną kar finansowych, a nie karnych. Podmiotem podlegającym sankcjom karnym powinien być wyłącznie sam oszust, a przedsiębiorca telekomunikacyjny wyłącznie w sytuacji, gdy świadomie aktywnie brał udział w oszustwie czerpiąc z tego korzyści finansowe. Uszczegółowieniu podlegać powinna również definicja samych zakazanych nadużyć, gdyż obecna regulacja oprócz nieprecyzyjnego technicznego ich opisu zawiera również nieprecyzyjny opis motywacji oszusta (np.	**Uwaga uwzględniona w zakresie ujednolicenia stosowania pojęć „nadawaniem widomości SMS" a „inicjowania ich wysyłania"** **Uwaga nieuwzględniona w pozostałym zakresie** Zgodnie z ogólnymi zasadami prawa karnego założeniem jest umyślne działanie sprawców tych przestępstw. Nie istnieje więc możliwość ukarania za te czyny nieświadomego ich przedsiębiorcy telekomunikacyjnego. Wykorzystane w przepisach karnych sformułowania w wystarczający sposób określają znamiona czynów zabronionych.

			spowodowania nieświadomego/niekorzystnego rozporządzania majątkiem przez ofiarę). Izba wskazuje, że przedmiot gospodarczy za pomocą którego sieci/urządzeń dokonano oszustwa (np. wyłudzono dane bankowe) nie zna motywów działania oszusta. Tymczasem definicje nadużyć telekomunikacyjnych opierają się nie tylko na aspektach technicznych, ale również na motywach sprawcy, którym nie jest przedsiębiorca telekomunikacyjny. Przykładowo projekt ustawy uzależnia nielegalność posłużenia się cudzą informacją adresową od celu w jakim to oszust zrobił (np. instalacji oprogramowania). Przedsiębiorca telekomunikacyjny nie może znać celu rozmowy telefonicznej czy wysłanego SMS. Przedsiębiorca zna jedynie motywy własnego działania lub zaniechania i tylko z tym powinna być związana jego obowiązywalność i obowiązki. Z tego względu ewentualna odpowiedzialności przedsiębiorców telekomunikacyjnych czy integratorów SMS powinna być związana wyłącznie z technicznymi aspektami działalności oszustów a nie ich motywacją.. Kwestia motywacji/ celu nadużycia telekomunikacyjnego powinna być wyłącznie wskazana w przepisach karnych. Generalnie izba również wskazuje, że proponowane kary pozbawienia wolności są odmienne niż obecnie w kodeksie karnym. Przykładowo generowanie sztucznego ruchu z art. 3 ust. 1 pkt 1 projektu może pokrywać się zakresem z kradzieżą impulsów telekomunikacyjnych z art. 285 kk a jednocześnie jest zagrożone wyższą karą. Oszustwo z kolei w kk jest zagrożone karą wyższą, mimo że oszustwo przy użyciu smishingu może mieć charakter masowy, a więc poważniejszy. Zdaniem izby, przepisy karne o nadużyciach (ale nie o karach finansowych)	

			dublują obecne regulacje z kodeksu karnego (np. w zakresie oszustwa, jakim jest bez wątpienia spoofing). Izba ponownie zwraca uwagę na brak wyjaśnienia jaka jest równica między nadawaniem widomości SMS a inicjowaniem ich wysyłania (a także jaka jest równica między samym nadawaniem a wysyłaniem – oba zwrot wydają się być stosowane w projekcie zamiennie). Nakładanie kar z tytułu dopuszczania się działań, które są nie tylko niezdefiniowane, ale i niemające jednoznacznego powszechnego znaczenia jest niedopuszczalne.	
114	Polska Izba Informatyki i Telekomunikacji	Art. 15 Art. 16	**Kary** Jak już wcześniej zostało podniesione kluczowe jest, aby ryzyko kary ciążyło na sprawcach dopuszczających się nadużyć w komunikacji elektronicznej i tą funkcję mają realizować art. 15 ust. 1 oraz art. 16 projektu ustawy. Jednocześnie projektowana ustawa jako zasadę powinna przewidywać uprawnienie dla przedsiębiorców telekomunikacyjnych do zwalczania nadużyć w komunikacji elektronicznej, a działanie w reżimie obowiązku można sobie wyobrazić jako wyjątek od zasady (jaką powinno być uprawienie) tylko dla blokowania SMS wpisujących się we wzorzec przekazany przez NASK (art. 4 ust. 6 projektu ustawy) oraz połączeń głosowych inicjowanych z wykorzystaniem numeru wpisanego do wykazu numerów służących wyłącznie do odbierania połączeń głosowych, prowadzonego przez Prezesa UKE (art. 9 ust. 12 projektu ustawy). Nie jest konieczne wprowadzanie ryzyka kar pieniężnych za niewywiązanie się z obowiązku blokowania SMS albo połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu, jeśli jednak w ocenie	**Uwaga nieuwzględniona** Kary mają zapewnić skuteczność projektowanych obowiązków. Podkreślić należy, że kary będą fakultatywne i za niewykonanie konkretnych obowiązków. Ponadto nawet po wszczęciu postępowania będą mogły znaleźć zastosowanie przesłanki odstąpienia od ukarania określone w art. 189e i 189f KPA.

			Projektodawcy takie kary są niezbędne, to powinny one dotyczyć tylko tych dwóch obowiązków i powinny mieć charakter fakultatywny. Jeśli zwalczanie CLI spoofingu ma się obywać w reżimie obowiązku (art. 8 projektu ustawy) pod groźbą kary pieniężnej ze strony Prezesa UKE (art. 15 ust. 2 pkt 2) projektu ustawy) to konieczne będzie wyznaczenie organu państwa, który będzie identyfikował konkretne połączenia głosowe jako CLI spoofing i przekazywał taką informację przedsiębiorcom telekomunikacyjnym celem zablokowania tak zidentyfikowanych połączeń (analogicznie do zaprojektowanego mechanizmu identyfikowania smishingowych wiadomości SMS przez NASK). Tak zidentyfikowane przez organ państwa połączenia głosowe przedsiębiorcy telekomunikacyjni mogą blokować w reżimie obowiązku. Jeśli jednak nie jest możliwe wyznaczenie organu państwa odpowiedzialnego za identyfikowanie spoofowanych połączeń głosowych, to: • projekt ustawy należy przeredagować tak, aby obowiązek w tym zakresie (art. 8 projektu ustawy) zmieć w uprawnienie: *Art. 8. W przypadku uzasadnionego podejrzenia wystąpienia CLI spoofingu przedsiębiorca telekomunikacyjny może zablokować takie połączenie albo wyeliminować prezentację identyfikacji numeru wywołującego.* • należy usunąć z projektu ustawy ryzyko kary przewidziane w art. 15 ust. 2 pkt 2).	

			Przedsiębiorcy telekomunikacyjni budują sieci i świadczą usługi telekomunikacyjne na podstawie standardów, norm, wytycznych i zasad, które są ustalane oraz koordynowane na poziomie międzynarodowym – ITU, ETSI, 3GPP. Stosując powszechnie uznane, międzynarodowe standardy techniczne dochowujemy najwyższej możliwej staranności, zapewniając naszym klientom interoperacyjne, niezawodne i bezpieczne usługi telekomunikacyjne o zasięgu globalnym. Istniejące standardy techniczne dla sieci telekomunikacyjnych nie przewidują gotowych rozwiązań i narzędzi, które można by wykorzystać do identyfikowania połączeń telekomunikacyjnych, które są zestawiane zgodnie z przyjętymi normami technicznymi, a które są inicjowane przez przestępców dla osiągnięcia niezgodnych z prawem celów (CLI spoofing). Takie rozwiązania i mechanizmy zapobiegające nadużyciom musimy próbować tworzyć sami, na gruncie współpracy międzyoperatorskiej i w porozumieniu z pozostałymi krajowymi operatorami. Tym celom ma służyć mechanizm, który zgodnie z art. 10 projektu ustawy ma działać w oparciu o porozumienie z Prezesem UKE. Prawidłowe realizowanie porozumienia ma oznaczać prawidłowe wykonywanie obowiązku wynikającego z art. 8 (tak wynika, i słusznie, z art. 10 ust. 2 i 3 projektu ustawy), jednak nie każdy przedsiębiorca telekomunikacyjny będzie dysponował zasobami i wiedzą niezbędną do przystąpienia i realizacji porozumienia. Obowiązek oraz ryzyko kary za nieskuteczne zwalczanie CLI spoofingu (art. 8 w zw. z art. 15 ust. 2 pkt 2) projektu ustawy) z jednej strony i możliwość skorzystania z ochrony oferowanej przez przystąpienie i realizowanie porozumienia (art. 10 ust. 2 i 3 projektu ustawy) z drugiej	

			strony może spowodować, że znaczna część z kilku tysięcy przedsiębiorców telekomunikacyjnych działających w Polsce będzie chciała przystąpić do porozumienia, tylko po to, aby zminimalizować ryzyko kar, choć znaczna część z tych przedsiębiorców, nie mając własnych sieci telekomunikacyjnych, niezbędnej wiedzy i zasobów, nie będzie w stanie realizować wymagań technicznych. W efekcie może się okazać, że zawarcie i realizowanie porozumienia zostanie sparaliżowane przez wnioski o akces do porozumienia ze strony licznych przedsiębiorców telekomunikacyjnych nieposiadających własnych sieci telekomunikacyjnych, tylko po to, aby zminimalizować ryzyko kary. Ryzyko kary w tym przypadku może sprawić, że porozumienie przestanie być zarządzalne w krótkim czasie po jej uruchomieniu. W zakresie zwalczania CLI spoofingu w zupełności wystarczające jest ryzyko kary dla przedsiębiorcy telekomunikacyjnego, który nie wypełni obowiązku blokowania połączeń głosowych inicjowanych z wykorzystaniem numeru wpisanego na listę numerów służących wyłączenie do odbierania połączeń (art. 15 ust. 2 pkt 3) projektu ustawy – aczkolwiek również to ryzyko powinno być usunięte, patrz wcześniejsze uwagi). Bardziej zaawansowane technologicznie rozwiązania, w tym rozwiązania nowatorskie i wręcz eksperymentalne, powinny działać w ramach porozumienia, a samo porozumienie powinno być: • otwarte na akces operatora gotowego przyjąć na siebie ciężar realizacji porozumienia;	

			• a jednocześnie dobrowolne dla każdego operatora, a nie pośrednio wymuszane reżimem obowiązku i widmem kary pieniężnej.	
115	Polska Izba Komunikacji Elektronicznej	Art. 15 ust. 1 i 2	**Kara pieniężna za nadużycia w komunikacji elektronicznej *(art. 15 ust. 1 i 2)*** Przepis przewidujący nałożenie sankcji administracyjnej na podmioty dokonujące nadużyć (ust. 1) jest w opinii Izby niepełny i wymaga dopracowania. Przede wszystkim nieprecyzyjnie wskazuje się zakres podmiotowy przepisu. Przez to nie jest wiadome kto podlega karze - czy jest to jedynie podmiot inicjujący nadużycie (np. połączenie głosowe), czy również operator, który pośredniczy w procesie nieświadomie. Postulujemy, aby przede wszystkim regulacja określała w sposób wyraźny zakres podmiotowy oraz zakres przedmiotowy swojego zastosowania, poprzez wskazanie na konkretną sytuację, w której możliwe jest nałożenie kary administracyjnej. Dopracowanie przepisu pozwoli wprost przedstawić możliwe sytuacje, w których przedsiębiorca telekomunikacyjny byłby zagrożony poniesieniem odpowiedzialności. Podkreślić należy również, że uwagi powinno się odnieść również do ust. 2. Przepis ten zakłada możliwość nałożenia na przedsiębiorcę telekomunikacyjnego kary pieniężnej za niewypełnienie obowiązków, o których mowa w art. 4 ust. 6, art. 8, art. 9 ust. 12. Niemniej jednak, przepis ten nie wskazuje wyraźnie zakresu podmiotowego i przedmiotowego zastosowania. Na jego podstawie ponownie nie jest jasne, czy przepis dotyczy wszystkich przedsiębiorców biorących udział w procesie nadużycia (np. kilku operatorów, w których sieciach przekazywane jest to samo połączenie), czy jedynie	**Uwaga wyjaśniona** Obecne art. 15 w ust. 1-3 precyzuje odpowiedzialność poszczególnych podmiotów. Przedsiębiorcy telekomunikacyjni ponoszą odpowiedzialność administracyjną za niewypełnianie obowiązków określonych w: 1) art. 4 ust. 6, 2) art. 8, 3) art. 9 ust. 12 Obecne przepisy precyzują w wystarczającym stopniu znamiona czynów zabronionych określone w tym przepisie. W zakresie interpretacji tych przepisów należy zastosować ogólne zasady.

			przedsiębiorcę odpowiedzialnego za zainicjowanie działania stanowiącego nadużycie. Ta kwestia powinna być określona wprost. Jeżeli chodzi natomiast o zakres przedmiotowy, to w opinii Izby należy w tym przepisie wskazać wyraźnie, jakie działania lub zaniechania mogą stanowić podstawę do nałożenia kary pieniężnej (np. czy kary są związane wyłącznie ze świadomym działaniem, czy również z brakiem odpowiednich zabezpieczeń). PIKE pragnie wskazać również na poważny problem związany z pominięciem w przepisie podmiotów zagranicznych i ograniczeniem go do podmiotów polskich. Problem spowodowany jest faktem, że działania stanowiące nadużycia w ogromnej części pochodzą z zagranicznych sieci. Należy rozważyć tę kwestię, ponieważ nie jest jasne, w jaki sposób takie działania powinny być traktowane w kontekście proponowanych sankcji. Na marginesie należy również wspomnieć, że kwestie związane z nadużyciami pochodzącymi z zagranicy powinno się rozważyć w odniesieniu do całej ustawy. W przeciwnym wypadku proponowane środki okażą się najprawdopodobniej niewystarczające do spełnienia swoich funkcji. Niewzięcie pod uwagę tego aspektu w ustawie podważa jej skuteczność.	
116	Związek Banków Polskich	Art.15 ust. 2 pkt 3	art. 9 ust. 12 i 13 Konsekwencja wprowadzenia dodatkowego obowiązku jw.	**Uwaga nieuwzględniona w zw. z nieuwzględnieniem uwag do art. 9**
117	Polska Izba Komunikacji Elektronicznej	Art. 16	**Przepis karny *(art. 16)*** PIKE zaznacza, że art. 16, stanowiący w całości przepis karny, nie powinien w jej opinii znaleźć się w przedmiotowej regulacji. Przepis dubluje w pewnym zakresie rozwiązania już obecne w Kodeksie karnym – m.in. art. 190a § 2, art. 285, art. 286. Projektodawca	**Uwaga nieuwzględniona** Zdaniem projektodawcy kwestia przestępstw mających charakter nadużyć w komunikacji elektronicznej powinna być uwypuklona w odrębnym przepisie.

			powinien zatem rozważyć kwestię przeniesienia przepisu właśnie do Kodeksu karnego albo zmodyfikowania projektowanych regulacji w taki sposób, aby usuwały wątpliwości co do ich relacji do przepisów Kodeksu karnego.	
118	Polska Wytwórnia Papierów Wartościowych	art. 16 ust. 3	W art. 16 ust. 3 projektu ustawy użyto wyrażenia „osoba najbliższa". Z uwagi na brak jednoznacznego znaczenia tego wyrażenia w polskim systemie prawnym proponujemy rozważyć wprowadzenie w art. 16 ust. 3 odwołania do art. 115 § 11 kodeksu karnego lub zamieszczenie definicji pojęcia „osoba najbliższa" w art. 2 projektu ustawy.	**Uwaga wyjaśniona** Zgodnie z art. 116 Kodeksu karnego przepisy części ogólnej tego kodeksu stosuje się do innych ustaw przewidujących odpowiedzialność karną. Dlatego nie ma potrzeby dodawania definicji osoby najbliższej w projekcie. W uzasadnieniu przepisu zostanie dodane stosowne wyjaśnienie.
119	Polska Wytwórnia Papierów Wartościowych	Art. 19	Zgodnie z treścią art. 19 projektu, CSIRT NASK będzie miał obowiązek uruchomienia systemu teleinformatycznego służącego przekazywaniu informacji o wystąpieniu smishingu. Sposób działania CSIRT NASK określa przepis art. 4 projektu, który reguluje m. in. przesyłanie wiadomości do podmiotów o nadużyciach w komunikacji elektronicznej. Niemniej jednak przekazujemy do rozważenia uzupełnienie ww. regulacji i wskazanie, że CSIRT NASK zarówno uruchamia jak i utrzymuje system teleinformatyczny.	**Uwaga uwzględniona** Zostanie wskazane, że CSIRT NASK uruchamia i utrzymuje systemie teleinformatyczny.
120	IAB Polska	Art. 20, Art. 23	**UWAGA:** W przeciwieństwie do innych przedsiębiorców telekomunikacyjnych UZNKE **nie przewiduje okresu dostosowawczego dla dostawców poczty elektronicznej**, zatem będą oni mieli jedynie **30-dniowy okres *vacatio legis***, aby dostosować się do obowiązków określonych w projekcie UZNKE, co może okazać dla nich za krótkim terminem, aby przygotować się do realizacji tych obowiązków. Oznacza to ryzyko nałożenia kary pieniężnej na dostawcę poczty elektronicznej, który w tak krótkim	**Uwaga nieuwzględniona** Wdrożenie mechanizmów SPF, DKIM oraz DMARC jest stosunkowo proste a ich wdrożenie przekroczyć maksymalnie kilku dni roboczych.

			czasie nie wywiąże się z obowiązków określonych w UZNKE. **PROPOZYCJA:** IAB Polska proponuje dodanie w art. 20 UZNKE nowego punktu: *3) o której mowa w art. 15 ust. 3, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.*	
121	Polska Izba Informatyki i Telekomunikacji	Art. 20	**Okres przejściowy dla kar pieniężnych** Art. 20 projektowanej ustawy przewiduje swoistą karencję, określony czas liczony od momentu wejścia w życie ustawy, przez który Prezes UKE nie będzie nakładał na przedsiębiorców telekomunikacyjnych kar pieniężnych za niewykonanie obowiązków wynikających z projektowanej ustawy. W ocenie Izby art. 20 powinien zyskać następujące brzmienie: *Art. 20. Kary pieniężnej:* *1) o której mowa w art. 15 ust. 2 pkt 1, nie nakłada się przed upływem 6 miesięcy od dnia wejścia w życie ustawy;* *2) o której mowa w art. 15 ust. 2 pkt 2 i 3, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.* Obecnie w art. 20 projektowanej ustawy brakuje przepisu, który odnosiłby się do nakładania kary pieniężnej, w przypadku, o którym mowa w art. 15 ust. 2 pkt 3) projektu ustawy, czyli blokowania połączeń inicjowanych z wykorzystaniem numerów wpisanych do wykazu prowadzonego przez Prezesa UKE. W tym przypadku należy terminy skonfigurować tak, aby dać	**Uwaga nieuwzględniona** W ocenie projektodawcy taka zmiana nie jest konieczna. Przedsiębiorca telekomunikacyjny będzie obowiązany blokować połączenia inicjowane z numerów znajdujących się w wykazie. Jeżeli wykaz będzie w fazie tworzenia, to nie będzie aktualizował się obowiązek blokowania połączeń.

			Prezesowi UKE czas na opracowanie i wdrożenie wykazu oraz czas niezbędny przedsiębiorcom telekomunikacyjnym na uruchomienie blokowania połączeń identyfikujących się numerem wpisanym do wykazu. Jednocześnie zwracamy uwagę, że jeśli zostanie uwzględniony nasz wcześniejszy postulat dotyczący usunięcia art. 15 ust. 2 pkt 2) projektu ustawy (ryzyko kary za niewykonanie obowiązku wynikającego z art. 8) to obecny punkt 3) w ust. 2 w art. 15 zamieni się w punkt 2) i w takim przypadku nie będą konieczne żadne zmiany w art. 20 projektu ustawy.	
122	Związek Banków Polskich	Propozycje zmian w ustawie z dnia 29 sierpnia 1997 r. - Prawo bankowe	Art. 4 ust. 1 pkt 59 (nowy) **59) centrum wymiany i analiz informacji – podmiot sektora finansowego, upoważniony do przetwarzania informacji na temat podatności, zagrożeń lub incydentów, mogących lub mających wpływ na bezpieczeństwo podmiotów, o których mowa w art. 106d ust. 1 oraz 1a lub ich klientów,** **60) przedsiębiorca telekomunikacyjny – przedsiębiorca, o którym mowa w art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;** Wobec identyfikacji coraz liczniejszych podatności, zagrożeń i incydentów wpływających na bezpieczeństwo sektora finansowego i jego klientów istnieje konieczność powołania nowej kategorii instytucji, której głównym zadaniem będzie koordynowanie obsługi incydentów wymierzonych podmioty sektora finansowego i ich klientów oraz wymienianie informacji na temat podatności i zagrożeń. Powołanie centrum wymiany i analizy informacji oraz nadanie mu stosownych	**Uwaga nieuwzględniona** Regulacje dotyczące ISAC – centrum wymiany i analiz informacji znajdują się w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw.

			ustawowych uprawnień istotnie wpłynie na wykrywanie, analizowanie i przeciwdziałanie przestępstwom popełnianym na szkodę instytucji finansowych lub ich klientów oraz wspieranie organów ścigania w zakresie wykrywania i ścigania sprawców tych przestępstw. W tym celu centrum wymiany i analizy informacji oraz inne podmioty wymienione w art. 106d ust. 1 i 1a powinny mieć m. in. możliwość wymienianie się informacjami prawnie chronionymi, w tym tajemnicą bankową. Art. 106 ust. 6-8 (nowe) **6. Bankowa izba gospodarcza, wspólnie z bankami, może utworzyć centrum wymiany i analiz informacji, upoważnione do gromadzenia, przetwarzania i udostępniania informacji, w tym informacji prawnie chronionych, w celu i zakresie, o których mowa w art. 106d oraz w odrębnych przepisach.** **7. Do zadań centrum wymiany i analizy informacji należy, w szczególności:** **1) wykrywanie, analizowanie i przeciwdziałanie przestępstwom popełnianym na szkodę podmiotów, o których mowa w art. 106d ust. 1 oraz 1a lub ich klientów;** **2) koordynowanie obsługi incydentów zagrażających bezpieczeństwu podmiotów, o których mowa w art. 106d ust. 1 oraz 1a lub ich klientów;** **3) wymiana informacji, dobrych praktyk i doświadczeń dotyczących podatności, zagrożeń, obsługi incydentów oraz ich koordynacji;** **4) wspieranie banków w wykonywaniu obowiązków, o których mowa w ust. 1.**	

			8. Centrum wymiany i analizy informacji może wspierać organy ścigania w wykrywaniu i ściganiu sprawców przestępstw, o których mowa w ust. 7 pkt 1. Bankowa izba gospodarcza, wspólnie z bankami, powinna mieć prawną możliwość utworzenia centrum wymiany i analizy informacji, które będzie wspierać banki oraz inne instytucje rynku finansowego w zakresie identyfikacji podatności, neutralizacji zagrożeń oraz koordynacji obsługi incydentów zagrażających bezpieczeństwu instytucji finansowych lub ich klientów. Szczegółowe zadania centrum wymiany i analizy informacji zostały określone w propozycji art. 106 ust. 6-8. Dodatkowo, centrum wymiany i analizy informacji powinno mieć możliwość wspierania organów ścigania w zakresie wykrywania i ścigania sprawców tych przestępstw. Dotychczasowe doświadczenia FinCERT.pl – BCC ZBP, Prokuratury Krajowej i Komendy Głównej Policji oraz Komend Wojewódzkich Policji pozwalają stwierdzić, że powoływane wspólnie tzw. Grupy Operacyjne pozwalają na sprawne skoordynowanie działań po stronie sektora finansowego oraz organów ścigania co wydatnie wpływa na efektywność działań podejmowanych przez wszystkich interesariuszy. Art. 106d ust. 1-2 1. Banki, inne instytucje ustawowo upoważnione do udzielania kredytów, izby rozliczeniowe utworzone na podstawie art. 67, instytucje utworzone na mocy art. 105 ust. 4, jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, instytucje pożyczkowe, instytucje finansowe, których	

			podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przedsiębiorcy telekomunikacyjni**,** mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach: 1) uzasadnionych podejrzeń, o których mowa w art. 106a ust. 3; 2) uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim**,** przedsiębiorców telekomunikacyjnych i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom; 3) wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. 2. Podmioty określone w ust. 1 mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową oraz informacje dotyczące wyroków skazujących, w przypadkach przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art.	

			59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przedsiębiorców telekomunikacyjnych i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom. Konsekwencja wcześniej zaproponowanych zmian – uzasadnienie jw. W określonych okolicznościach, o których mowa w art. 106d ust. 1 również przedsiębiorcy telekomunikacyjni powinni mieć prawną możliwość przetwarzania informacji objętych tajemnicą bankową. Art. 106d ust. 1a **1a. W przypadkach określonych w ust. 1, do przetwarzania i wzajemnego udostępniania informacji, w tym objętych tajemnicą bankową, uprawnione są również następujące podmioty:** **1) centrum wymiany i analizy informacji, o którym mowa w art. 106 ust. 6;** **2) podmioty, które są członkami centrum wymiany i analizy informacji, o którym mowa w pkt 1 lub zawarły z nim stosowne porozumienie w zakresie, o którym mowa w ust. 1;** Uzasadnienie jw. Do przetwarzania danych osobowych przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, instytucje pożyczkowe, instytucje finansowe, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, podmioty, których	

			podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przedsiębiorców telekomunikacyjnych, przepisu art. 15 rozporządzenia 2016/679 nie stosuje się w zakresie, w jakim jest to niezbędne dla prawidłowej realizacji zadań dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zgodnie z art. 106, oraz zapobiegania przestępstwom, zgodnie z art. 106a i art. 106d. Konsekwencja wcześniej zaproponowanych zmian – uzasadnienie jw.	
123	Polska Izba Informatyki i Telekomunikacji	Uzasadnienie	**Uwagi do uzasadnienia do projektu ustawy** Akapit drugi na stronie pierwszej uzasadnienia do projektu ustawy ma następujące brzmienie (podkreślenie własne): *W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych. Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć. <u>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</u>	**Uwaga częściowo uwzględniona** Uzasadnienie zostanie uzupełnione. Usunięty został fragment o „słabości sieci” jako zbytnie uproszczenie.

			zarejestrowana dla danego numeru. Zjawisko to występuje pod nazwą CLI spoofing. Proponujemy, aby ten fragment tekstu uzyskał następujące brzmienie: *W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych. Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć.* *Proceder CLI spoofingu polega na nieuprawnionym posłużeniu się przez użytkownika (często przestępcę) wywołującego połączenie głosowe numerem wskazującym na inną osobę lub instytucję, po to, aby podszyć się pod tą osobę albo instytucję i dzięki temu móc łatwiej nakłonić ofiarę (tj. odbiorcę takiego połączenia) do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji złośliwego oprogramowania.* *Z doświadczeń krajowych operatorów wynika, że gros połączeń z numerem A wykorzystywanym przez osobę nieuprawnioną przychodzi do naszego kraju z zagranicy. Źródłem spoofingu są więc przestępcy, którzy korzystają z usług telekomunikacyjnych oferowanych przez dostawców działających w krajach o niskich standardach biznesowych i regulacyjnych. To również znacznie utrudnia organom ścigania wykrycie sprawców. W przypadku gdy połączenie ze spoofowanym numerem A*	

			przychodzi do krajowych sieci telekomunikacyjnych z zagranicy, dla krajowych operatorów takie połączenie nie różni się niczym od innych, „legalnych" połączeń. W przypadku połączeń przychodzących z zagranicznych sieci operator krajowy „widzi" numer A i numer B połączenia i na dzień dzisiejszy nie ma możliwości ustalenia w czasie rzeczywistym i bez możliwości udziału w tym procesie sieci i operatorów biorących udział w zainicjowaniu oraz pośredniczących w realizacji połączenia, czy numer A jest wykorzystywany przez osobę uprawnioną, czy przez osobę nieuprawnioną. Innymi słowy, na dzień dzisiejszy połączenie ze spoofowanym numerem A z perspektywy operatora krajowego „wygląda" dokładnie tak samo, jak połączenie, w którym numerem A posługuje się osoba uprawniona. O tym, że połączenie jest spofowane wie tylko osoba inicjująca połączenie (w momencie jego inicjowania), a w momencie odebrania połączenia albo później dowiaduje się o tym osoba odbierająca połączenie (numer B). Operator telekomunikacyjny, organy ścigania, instytucje, pod które podszył się przestępca, dowiadują się o tym, że połączenie było spoofowane, dopiero po fakcie, od ofiary (numer B), która odebrała takie połączenie. To tłumaczmy, czemu proceder CLI-spoofingu istnieje i czemu tak trudno jest go wyeliminować czy choćby ograniczyć. Celem zaproponowanej zmiany jest, aby opis zjawiska CLI spoofingu był bardziej adekwatny do tego, jak faktycznie działa ten mechanizm. Ponadto, nie możemy zgodzić się ze stwierdzeniem sugerującym, że to „słabości" sieci telekomunikacyjnych umożliwiają przestępcom działanie. Operatorzy budują sieci i świadczą usługi telekomunikacyjne na podstawie standardów, norm, wytycznych i zasad, które są ustalane oraz	

			koordynowane na poziomie międzynarodowym – ITU, ETSI, 3GPP. Stosując powszechnie uznane, międzynarodowe standardy techniczne dochowujemy najwyższej możliwej staranności, zapewniając naszym klientom interoperacyjne, niezawodne i bezpieczne usługi telekomunikacyjne o zasięgu globalnym. Istniejące standardy techniczne dla sieci telekomunikacyjnych nie przewidują gotowych rozwiązań i narzędzi, które można by wykorzystać do identyfikowania połączeń telekomunikacyjnych, które są zestawiane zgodnie z przyjętymi normami technicznymi, a które są inicjowane przez przestępców dla osiągnięcia niezgodnych z prawem celów. Fakt, że przestępcy nadużywają sieci i usług telekomunikacyjnych do popełniania przestępstw w żadnym wypadku nie świadczy o jakiejkolwiek „słabości" albo wadzie sieci telekomunikacyjnych, tak jak popełnienie przestępstwa z użyciem noża nie świadczy w żaden sposób o tym, że nóż jest w jakikolwiek sposób wadliwy. Nie można również zapominać, iż CLI-spoofing nie jest celem samym w sobie, jest narzędziem, jednym z wielu w przestępczym repertuarze, wykorzystywanym w celu zwiększenia szansy powodzenia przestępczego ataku. Zresztą przestępcy nie zawsze wykorzystują CLI-spoofing dzwoniąc do ofiary, czasami takie połączenia są realizowane z numeru zastrzeżonego albo z dowolnego innego, pokazującego się numeru (który nie został spoofowany). Najważniejszą część takiego ataku stanowi socjotechnika wykorzystywana przez przestępców do skłonienia ofiary do postępowania zgodnie z ich poleceniami. Próby ograniczenia CLI-spoofingu na poziomie sieci telekomunikacyjnych można porównać do usuwania jedynie niektórych objawów choroby, bez	

			leczenia samej choroby. Ową chorobą w tym przypadku są przestępcy, którzy dzwonią do ofiar (wykorzystując CLI-spoofing albo nie) i podszywając się pod inną osobę, instytucję publiczną albo firmę skłaniają ofiarę do przekazania danych czy podjęcia czynności, w efekcie których ofiara traci pieniądze albo doznaje szkody w innej postaci. Oznacza to również, że nawet jeśli uda się do pewnego stopnia ograniczyć zjawisko CLI spoofingu, to nie będzie to oznaczało, że przestępcy zaprzestaną swojego przestępczego procederu, gdyż tak długo, jak proceder będzie opłacalny a sprawcy nieuchwytni i bezkarni, przestępcy będą wykonywali przestępcze połączenia albo próbując ominąć zabezpieczenia CLI spoofingowe albo dzwoniąc z dowolnego numeru zastrzeżonego albo widocznego (który nie został spoofowany) i bez CLI spofingu będą próbowali przekonać ofiarę, że są pracownikiem instytucji finansowej albo publicznej.	

ZGŁOSZENIE
ZAINTERESOWANIA PRACAMI NAD PROJEKTEM - ~~ZGŁOSZENIE ZMIANY DANYCH~~*

ustawy o zwalczaniu nadużyć w komunikacji elektronicznej z dnia 15.06.2022 r. (numer wykazu prac legislacyjnych i programowych Rady Ministrów **UD402**)

A. OZNACZENIE PODMIOTU ZAINTERESOWANEGO PRACAMI NAD PROJEKTEM

1. Nazwa/~~imię i nazwisko~~** **HACK&PHACK DEFENCE LTD Piotr Marcin Wierzbicki**

2. Adres siedziby/~~adres miejsca zamieszkania~~**

3. Adres do korespondencji i adres e-mail

B. WSKAZANIE OSÓB UPRAWNIONYCH DO REPREZENTOWANIA PODMIOTU WYMIENIONEGO W CZĘŚCI A W PRACACH NAD PROJEKTEM

Lp.	Imię i nazwisko	Adres
1	Piotr Marcin Wierzbicki	
2		
3		
4		
5		

C. OPIS POSTULOWANEGO ROZWIĄZANIA PRAWNEGO, ZE WSKAZANIEM INTERESU BĘDĄCEGO PRZEDMIOTEM OCHRONY

Opierając się na doświadczeniu wynikającym z praktyki wnoszę o uwzględnienie moich poniższych uwag do projektu UD402:
z art. 2 ustęp 4 usunięcie słów: „celem lub skutkiem„ a w ich miejsce wpisanie słów ”skutkiem wynikającym z celowego działania”, bo znając zasadę rozliczeń między operatorskich IC/CW mogą się często zdarzać sytuacje gdy np. pracownicy jakiej bądź firmy lub nawet osoby prywatne korzystając ze swojego numeru telefonu będą w większości wykonywać połączenia wychodzące do innych sieci (np. kontakt z klientami albo starszą osobą która nie potrafi zbytnio korzystać z telefonu i ogranicza jego użytkowanie do odbierania połączeń do Niej przychodzących) a mając abonament typu No Limit przy określonych dyrektywą UE stawkach MTR/

FTR - zostanie to uznane za działanie na szkodę przedsiębiorcy telekomunikacyjnego i będzie podlegać odpowiedzialności wynikającej z niniejszego projektu ustawy.
Do tego słowa „osiągnięcie nienależytych korzyści" art. 2 ustęp 4 w w/w przypadkach można przypisać operatorowi telekomunikacyjnemu do którego sieci byłyby takie połączenia kierowane i także pociągnąć do odpowiedzialności z mocy niniejszej ustawy dlatego wnoszę o skreślenie słów "lub osiągnięcie nienależytych korzyści".
Dlatego wnoszę o wycofanie się z penalizacji i wszelkich innych form karania za – jak sam Ustawodawca podnosi - otwartą definicję nadużycia w komunikacji elektronicznej przez skreślenie z projektu UD402 zapisów artykułu 3 ustęp 1 pkt 1 - lub dodanie w nim w treści „**ultrakrótkich** połączeń głosowych" zamiast „połączeń głosowych", w przypadku niezmodyfikowania tego artykułu wnoszę o jego skreślenie.
Ponadto wnoszę o skreślenie art. 16 ustęp 1 pkt 1, bo penalizuje standardową procedurę uruchamiania punktu styku sieci operatorów telekomunikacyjnych polegającą na kalibracji systemów rozliczeniowych tych operatorów.
Należy zwrócić uwagę, że istniejące przepisy Kodeksu Karnego skutecznie chronią interes prawny poszkodowanych, w tym przedsiębiorców telekomunikacyjnych oraz abonentów końcowych.

Natomiast skupiłbym się na artykułach dotyczących CLI SPOOFING oraz SMISHING bo nie wzbudzają one większych kontrowersji poza oczywistym faktem , że np. zapoznanie się (nawet automatyczne) z treścią np. SMS wysyłanego przez adwokata narusza tajemnicę adwokacką (art 14 ustęp 2 projektu UD402 oraz art 14 ustęp 3 pkt 1 tego projektu).

D. ZAŁĄCZONE DOKUMENTY

1	Oświadczenie o wpisie do rejestru podmiotów wykonujących zawodową działalność lobbingową
2	Oświadczenie wskazujące podmioty, na rzecz których wykonywana jest zawodowa działalność lobbingowa

E. Niniejsze zgłoszenie dotyczy uzupełnienia braków formalnych/zmiany danych zgłoszenia dokonanego dnia .....**

(podać datę z części F poprzedniego zgłoszenia)

F. OSOBA SKŁADAJĄCA ZGŁOSZENIE

Imię i nazwisko	Data	Podpis
Piotr Marcin Wierzbicki	27.06.2022.	

		HACK & PHACK DEFENCE LTD Piotr Marcin Wierzbicki ul. Pocztowa 12/8A 70-360 Szczecin NIP 8522285856 REGON 811991394

G. KLAUZULA ODPOWIEDZIALNOŚCI KARNEJ ZA SKŁADANIE FAŁSZYWYCH ZEZNAŃ

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia .....

(podpis)

* Jeżeli zgłoszenie nie jest składane w trybie art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, treść: "- Zgłoszenie zmiany danych" skreśla się.

** Niepotrzebne skreślić.

Pouczenie:

1. Jeżeli zgłoszenie ma na celu uwzględnienie zmian zaistniałych po dacie wniesienia urzędowego formularza zgłoszenia (art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa) lub uzupełnienie braków formalnych poprzedniego zgłoszenia (§ 3 rozporządzenia Rady Ministrów z dnia 22 sierpnia 2011 r. w sprawie zgłaszania zainteresowania pracami nad projektami aktów normatywnych oraz projektami założeń projektów ustaw (Dz. U. Nr 181, poz.1080), w nowym urzędowym formularzu zgłoszenia należy wypełnić wszystkie rubryki, powtarzając również dane, które zachowały swoją aktualność.
2. Część B formularza wypełnia się w przypadku zgłoszenia dotyczącego jednostki organizacyjnej oraz w sytuacji, gdy osoba fizyczna, która zgłasza zainteresowanie pracami nad projektem założeń projektu ustawy lub projektem aktu normatywnego, nie będzie uczestniczyła osobiście w tych pracach.
3. W części D formularza, stosownie do okoliczności, uwzględnia się dokumenty, o których mowa w art. 7 ust. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, a także pełnomocnictwa do wniesienia zgłoszenia lub do reprezentowania podmiotu w pracach nad projektem aktu normatywnego lub projektu założeń projektu ustawy.
4. Część E formularza wypełnia się w przypadku uzupełnienia braków formalnych lub zmiany danych dotyczących wniesionego zgłoszenia.

Warszawa, 14.06.2022.

OŚWIADCZENIE

Oświadczam, że podmiot, który reprezentuję – Hack&Phack Defence LTD Piotr Marcin Wierzbicki – wpisany jest do rejestru podmiotów wykonujących zawodową działalność lobbingową (prowadzonego przez Ministerstwo Spraw Wewnętrznych i Administracji) pod numerem 00539.

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.

…….
(podpis Wnioskodawcy)

Warszawa, 14.06.2022.

OŚWIADCZENIE

Oświadczam, że zawodową działalność lobbingową, wykonuję na rzecz następującego podmiotu:

Pika Polska Sp. z o. o. (KRS: 0000636571)

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.

…….
(podpis Wnioskodawcy)

TABELA ZGODNOŚCI				
TYTUŁ PROJEKTU		Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej (UD402)		
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO		Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona)		
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU		Termin wejścia w życie uwzględnia konieczność jak najszybszego wprowadzenia w życie przepisów umożliwiających zwalczanie nadużyć w komunikacji elektronicznej.		
l.p.	**jednostka redakcyjna dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972**	**treść przepisu UE**	**jednostka redakcyjna ustawy**	**treść przepisu/przepisów projektu ustawy**
1.	Art. 1 pkt 5	5) „usługa łączności interpersonalnej” oznacza usługę zazwyczaj świadczoną za wynagrodzeniem, która umożliwia bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci łączności elektronicznej między skończoną liczbą osób, w ramach której osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, natomiast nie obejmuje ona usług, które umożliwiają interpersonalną i interaktywną komunikację	Art. 2 pkt 16	16) usługa komunikacji interpersonalnej – usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej;

		wyłącznie jako podrzędną funkcję dodatkową, która jest nieodłącznie związana z inną usługą;		
2.	Art. 1 pkt 7	7) „usługa łączności interpersonalnej niewykorzystująca numerów” oznacza usługę łączności interpersonalnej, która nie łączy się z publicznie nadanymi zasobami numeracyjnymi, mianowicie numerem lub numerami z krajowych lub międzynarodowych planów numeracji, ani nie umożliwia połączenia z numerem lub numerami z krajowych lub międzynarodowych planów numeracji;	Art. 2 pkt 17	17) usługa komunikacji interpersonalnej niewykorzystująca numerów – usługę komunikacji interpersonalnej, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji;
3.	Art. 1 pkt 31	31) „połączenie” oznacza połączenie, które dochodzi do skutku za pośrednictwem publicznie dostępnej usługi łączności interpersonalnej umożliwiającej dwustronną łączność głosową	Art. 2 pkt 11	11) połączenie głosowe – połączenie ustanowione za pomocą publicznie dostępnej usługi komunikacji interpersonalnej pozwalające na dwukierunkową komunikację głosową;
4.	Art. 29 ust. 1	1. Państwa członkowskie ustanawiają przepisy dotyczące sankcji, w tym, w razie potrzeby, grzywien i innych niż karne określonych z góry lub okresowych sankcji, mających zastosowanie do naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy lub dowolnej wiążącej decyzji przyjętej przez Komisję, krajowy organ regulacyjny lub inny właściwy organ na podstawie niniejszej dyrektywy oraz wprowadzają wszelkie środki niezbędne, by zapewnić ich wykonanie. W granicach określonych przepisami krajowego prawa krajowe organy regulacyjne lub inne właściwe organy mają prawo nakładać takie sankcje. Przewidziane sankcje muszą być odpowiednie, skuteczne, proporcjonalne i odstraszające.	Art. 20 ust. 1-3, 5-9; art. 21 ust. 1-8	**Art. 20.** 1. Przedsiębiorca telekomunikacyjny, który dokonuje następujących nadużyć w komunikacji elektronicznej: 1) generowania sztucznego ruchu, 2) smishingu, 3) CLI spoofingu, 4) nieuprawnionej zmiany informacji adresowej – podlega karze pieniężnej. 2. Jeżeli czyn będący nadużyciem, o którym mowa w ust. 1, wyczerpuje jednocześnie znamiona przestępstwa, w stosunku do przedsiębiorcy telekomunikacyjnego będącego osobą fizyczną stosuje się wyłącznie przepisy o odpowiedzialności karnej.

				3. Na przedsiębiorcę telekomunikacyjnego, który nie wypełnia obowiązków, o których mowa w: 1) art. 5, 2) art. 9, 3) art. 10 ust. 15 lub 16 – może zostać nałożona kara pieniężna, jeżeli przemawia za tym zakres lub charakter naruszenia. 5. Kara pieniężna, o której mowa w ust. 1–4, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia. 6. Niezależnie od kary pieniężnej, o której mowa w ust. 3, Prezes UKE może, w drodze decyzji, nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop wypoczynkowy. 8. Od decyzji Prezesa UKE w sprawie nałożenia kary pieniężnej przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów. 9. Kary pieniężne podlegają egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym. **Art. 21.** 1. Karę pieniężną, o której mowa w art. 20 ust. 1, 3 i 4, nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym.

				Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności. 2. W przypadku gdy podmiot w roku kalendarzowym poprzedzającym rok nałożenia kary pieniężnej nie osiągnął przychodu albo osiągnął przychód w wysokości nieprzekraczającej 500 000 zł, Prezes UKE nakładając karę pieniężną uwzględnia średni przychód osiągnięty przez podmiot w 3 kolejnych latach kalendarzowych poprzedzających rok nałożenia kary pieniężnej. 3. W przypadku gdy podmiot nie osiągnął przychodu w okresie, o którym mowa w ust. 2, albo gdy przychód podmiotu w tym okresie nie przekracza 500 000 zł, Prezes UKE może nałożyć na podmiot karę pieniężną w wysokości nieprzekraczającej 15 000 zł. 4. W przypadku gdy przed wydaniem decyzji o nałożeniu kary pieniężnej podmiot nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary pieniężnej, Prezes UKE nakładając karę pieniężną uwzględnia: 1) przychód osiągnięty przez podmiot w roku kalendarzowym poprzedzającym ten rok; 2) w przypadku, o którym mowa w ust. 2 – średni przychód osiągnięty przez podmiot w 3 kolejnych latach kalendarzowych poprzedzających ten rok; przepis ust. 3 stosuje się odpowiednio. 5. W przypadku gdy podmiot powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu, o którym mowa w ust. 1, Prezes UKE uwzględnia przychód osiągnięty przez te podmioty w roku kalendarzowym poprzedzającym rok nałożenia kary. 6. Ustalając wysokość kary pieniężnej, Prezes UKE uwzględnia zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe.

				7. Podmiot jest obowiązany do dostarczenia Prezesowi UKE, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku niedostarczenia danych lub gdy dostarczone dane uniemożliwiają ustalenie podstawy wymiaru kary, Prezes UKE może ustalić podstawę wymiaru kary pieniężnej w sposób szacunkowy, nie mniejszą jednak niż kwota 500 000 zł. 8. Jeżeli okres działania podmiotu jest krótszy niż rok kalendarzowy, za podstawę wymiaru kary przyjmuje się kwotę 500 000 zł. 9. Kary pieniężne, o których mowa w art. 20 ust. 1, 3 i 4, nakładane przez Prezesa UKE, stanowią dochód budżetu państwa.
5.	Art. 97 ust. 2	Państwa członkowskie zapewniają, aby krajowe organy regulacyjne lub inne właściwe organy mogły wymagać od podmiotów udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej zablokowania w indywidualnych przypadkach dostępu do numerów lub usług, w przypadku gdy jest to uzasadnione ze względu na oszustwo lub nadużycie, oraz wymagać, aby w takich przypadkach dostawcy usług łączności elektronicznej wstrzymali wypłatę dochodów z odpowiednich połączeń wzajemnych lub innych usług	Art. 1; Art. 2 pkt 6; Art. 3; Art. 4; art. 5, Art. 8; Art. 9; Art. 10 ust. 15 I 16; Art. 12; art. 13 Art. 16; Art. 31;	Art. 1 **Art. 1.** Ustawa określa: 1) prawa i obowiązki przedsiębiorców telekomunikacyjnych związane z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich zwalczaniem; 2) kompetencje Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE”, związane z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich zwalczaniem; 3) zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej; 4) zasady wnoszenia sprzeciwu przez podmiot posiadający tytuł prawny do domeny wobec wpisania domeny internetowej na listę ostrzeżeń;

				5) obowiązki dostawcy poczty elektronicznej oraz podmiotu publicznego związane ze świadczeniem i korzystaniem z poczty elektronicznej w celu zapobiegania nadużyciom w komunikacji elektronicznej; 6) szczególne zasady przetwarzania informacji objętych tajemnicą telekomunikacyjną związane z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich zwalczaniem. Art. 2 pkt 6 Określenia użyte w ustawie oznaczają: 6) nadużycie w komunikacji elektronicznej – świadczenie lub korzystanie z usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści dla podmiotu dopuszczającego się nadużycia w komunikacji elektronicznej, innej osoby fizycznej, osoby prawnej lub, jednostki organizacyjnej nieposiadającej osobowości prawnej;Art. 3 **Art. 3.** 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności: 1) wysyłanie lub odbieranie komunikatów lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (generowanie sztucznego ruchu); 2) wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności

				przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania (smishing); 3) nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania (CLI spoofing); 4) nieuprawnione modyfikowanie informacji adresowej uniemożliwiające lub istotnie utrudniające ustalenie przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu informacji adresowej, przy użyciu której nastąpiło wysłanie komunikatu (nieuprawniona zmiana informacji adresowej). 2. Przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Art. 4 i 5 **Art. 4.** 1. CSIRT NASK na podstawie krótkich wiadomości tekstowych (SMS) otrzymanych od odbiorców oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów monitoruje występowanie smishingu.

				2. CSIRT NASK na podstawie wyników monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu, zwany dalej „wzorcem wiadomości”. 3. CSIRT NASK zapewnia funkcjonowanie systemu teleinformatycznego służącego do udostępniania i przekazywania informacji o wystąpieniu smishingu wraz ze wzorcem wiadomości oraz jest administratorem danych przetwarzanych w tym systemie. 4. CSIRT NASK za pośrednictwem systemu teleinformatycznego zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi UKE i przedsiębiorcom telekomunikacyjnym. 5. CSIRT NASK za pośrednictwem systemu teleinformatycznego przekazuje przedsiębiorcy telekomunikacyjnemu informacje o występowaniu smishingu wraz ze wzorcem wiadomości. 6. Podmioty, o których mowa w ust. 4, w celu wymiany informacji są obowiązane do korzystania z systemu. 7. Wzorzec wiadomości, o którym mowa w ust. 2, CSIRT NASK udostępnia na swojej stronie internetowej, nie wcześniej niż 14 dni i nie później niż 21 dni od dnia jego przekazania przedsiębiorcy telekomunikacyjnemu w sposób, o którym mowa w ust. 5. 8. CSIRT NASK, w przypadku gdy uzna, że: 1) treść zawarta we wzorcu wiadomości nie stanowi smishingu, lub 2) niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zgodnych ze wzorcem wiadomości – niezwłocznie informuje o tym podmioty, o których mowa w ust. 4, oraz zamieszcza na swojej stronie internetowej informacje o okresie w jakim wzorzec wiadomości obowiązywał.

				9. CSIRT NASK przetwarza dane pozyskane w związku z monitorowaniem występowania smishingu na zasadach określonych w art. 39 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. **Art. 5.** Przedsiębiorca telekomunikacyjny po otrzymaniu informacji, o której mowa w art. 4 ust. 5 lub 8, niezwłocznie: 1) blokuje krótkie wiadomości tekstowe (SMS) zawierające treści zawarte we wzorcu wiadomości, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (SMS); 2) zaprzestaje blokowania krótkich wiadomości tekstowych (SMS) w przypadku uznania, że treść zawarta we wzorcu wiadomości nie nosi znamion smishingu lub niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zawierających treści wskazane we wzorcu wiadomości. **Art. 8.** 1. Przedsiębiorca telekomunikacyjny może blokować krótkie wiadomości tekstowe (SMS), zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości, o którym mowa w art. 4 ust. 5, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich krótkich wiadomości tekstowych (SMS). 2. Przedsiębiorca telekomunikacyjny może blokować wiadomości multimedialne (MMS) w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego, lub instalacji oprogramowania. Blokowanie odbywa się za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich wiadomości. **Art. 9.** W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo

				ukrywa identyfikację numeru wywołującego dla użytkownika końcowego. Art. 10 ust. 15 i 16 15. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu numeru do wykazu, o którym mowa w ust. 1, blokuje połączenia przychodzące do jego sieci z wykorzystaniem numeru wpisanego do tego wykazu. 16. Przedsiębiorca telekomunikacyjny zaprzestaje blokowania tego numeru w terminie 3 dni od dnia wykreślenia z wykazu. Art. 12 **Art. 12.** 1. W celu realizacji obowiązków, o których mowa w art. 9, przedsiębiorca telekomunikacyjny stosuje środki organizacyjne i techniczne służące monitorowaniu, wykrywaniu oraz wymianie informacji o CLI spoofing, a także blokowaniu połączenia głosowego albo ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego. 2. Dostawca publicznie dostępnych usług telekomunikacyjnych świadczący usługi telekomunikacyjne dla co najmniej 50 000 abonentów, będący jednocześnie operatorem, może zawrzeć z Prezesem UKE porozumienie określające szczegółowe środki organizacyjne i techniczne, które będzie stosował przy realizacji obowiązków, o których mowa w art. 9. 3. Zawarcie porozumienia i jego prawidłowe wykonywanie stanowi spełnienie przez operatora będącego stroną porozumienia obowiązku podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w

				komunikacji elektronicznej i ich zwalczanie w zakresie, o którym mowa w art. 3 ust. 1 pkt 3. 4. Operator prawidłowo wykonujący porozumienie, o którym mowa w ust. 2, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem zastosowanych środków organizacyjnych i technicznych , o których mowa w ust. 1. 5. Prezes UKE kontroluje prawidłowość stosowania środków organizacyjnych i technicznych określonych w porozumieniu, o którym mowa w ust. 2. Do kontroli stosuje się przepisy działu X rozdziału 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. 6. Dla przedsiębiorców telekomunikacyjnych innych, niż określeni w ust. 2, Prezes UKE może wydać rekomendacje określające szczegółowe środki organizacyjne i techniczne służące realizacji obowiązków, o których mowa w art. 9. Rekomendacje są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa UKE. 7. Przedsiębiorca telekomunikacyjny, inny niż określony w ust. 2, prawidłowo stosujący środki organizacyjne i techniczne określone w rekomendacjach, o których mowa w ust. 6, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem wprowadzenia środków. Art. 13 **Art. 13.** 1. W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich mieniem, między Prezesem UKE, ministrem właściwym do spraw informatyzacji, Naukową i Akademicką Siecią Komputerową – Państwowy Instytut Badawczy, oraz przedsiębiorcą telekomunikacyjnym lub przedsiębiorcami telekomunikacyjnymi może

				zostać zawarte porozumienie dotyczące prowadzenia listy ostrzeżeń oraz uniemożliwienia dostępu do tych stron. 2. W przypadku zawarcia porozumienia podmiotem odpowiedzialnym za prowadzenie listy jest CSIRT NASK. 3. Na listę ostrzeżeń wpisywane są domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i doprowadzenie do wyłudzenia ich danych lub niekorzystnego rozporządzenia środkami finansowymi. 4. Każdy może zgłosić domenę internetową mogącą służyć do wyłudzeń danych i środków finansowych do CSIRT NASK. Zgłoszenie domeny internetowej może zawierać uzasadnienie. 5. CSIRT NASK z inicjatywy własnej lub po otrzymaniu zgłoszenia wpisuje domenę internetową na listę ostrzeżeń, jeżeli spełnia ona przesłanki określone w ust. 3. 6. CSIRT NASK publikuje na stronie podmiotowej Biuletynu Informacji Publicznej Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego informację określającą sposób dokonywania zgłoszeń. 7. Porozumienie określa co najmniej zasady współpracy stron porozumienia. 8. Przedsiębiorca telekomunikacyjny będący stroną porozumienia może uniemożliwić użytkownikom internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę ostrzeżeń, przez ich usunięcie z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych służących do zamiany nazw domen internetowych na adresy IP. 9. W przypadku skorzystania z uprawnienia, o którym mowa w ust. 8, przedsiębiorca telekomunikacyjny przekieruje połączenia odwołujące się do nazw domen internetowych wpisanych na listę ostrzeżeń do strony internetowej prowadzonej przez CSIRT NASK zawierającej

				informację skierowaną do użytkowników internetu zawierającą w szczególności informacje o lokalizacji listy ostrzeżeń, wpisaniu szukanej nazwy domeny internetowej na listę ostrzeżeń oraz o możliwej próbie wyłudzenia danych lub środków finansowych. **Art. 16.** 1. Prezes UKE może, gdy jest to uzasadnione ochroną użytkowników końcowych przed nadużyciami w komunikacji elektronicznej, nakazać przedsiębiorcy telekomunikacyjnemu w drodze decyzji, zablokowanie dostępu do numeru lub usługi w terminie nie krótszym niż 6 godzin od momentu jej ogłoszenia oraz nałożyć obowiązek wstrzymania pobierania opłat za połączenia lub usługi zrealizowane po upływie tego terminu. 2. Decyzja, o której mowa w ust. 1, może być ogłoszona ustnie przedsiębiorcy telekomunikacyjnemu. Decyzja ogłoszona ustnie doręczana jest stronie na piśmie w terminie 14 dni od dnia jej ogłoszenia. 3. Decyzji, o której mowa w ust. 1, nadaje się rygor natychmiastowej wykonalności. 4. Do postępowania w sprawie wydania decyzji, o której mowa w ust. 1, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyjątkiem art. 107–113 oraz działu II rozdziału 12 i 13, które stosuje się odpowiednio. **Art. 31.** Przedsiębiorcy telekomunikacyjni są obowiązani do wdrożenia proporcjonalnych środków organizacyjnych i technicznych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie, o których mowa w art. 3 ust. 1: 1) pkt 1 i 2 – w terminie 6 miesięcy od dnia wejścia w życie ustawy; 2) pkt 3 i 4 – w terminie 12 miesięcy od dnia wejścia w życie ustawy.

ODWRÓCONA TABELA ZGODNOŚCI			
projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (UD402)			
l.p.	**jednostka redakcyjna projektu**	**treść przepisu**	**uzasadnienie wprowadzenia przepisu**
1.	Art. 2 pkt 1-5, 7-10, 12-15, 18-20.	**Art. 2.** Określenia użyte w ustawie oznaczają: 1) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, w rozumieniu art. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666); 2) dostawca poczty elektronicznej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadzi, chociażby ubocznie, działalność zarobkową lub zawodową związaną ze świadczeniem poczty elektronicznej; 3) informacja adresowa – numer telefonu lub identyfikator użytkownika wysyłającego komunikat; 4) komunikat – komunikat w rozumieniu art. 2 pkt 17 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581); 5) lista ostrzeżeń – jawna lista ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzenia mieniem użytkowników internetu; 7) operator – operatora w rozumieniu art. 2 pkt 27 lit. b ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 8) poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie	Niniejsza ustawa oprócz implementacji przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej wprowadza również zmiany w zakresie zwalczania nadużyć w komunikacji elektronicznej mające służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania tym nadużyciom przez przedsiębiorców telekomunikacyjnych oraz w dalszej perspektywie przepisy te pozwolą ograniczyć skalę nadużyć. Niniejszy przepis zawiera słowniczek ustawowy w którym wskazano 18 definicji, z czego 14 nie jest powiązane z implementacją Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 i ma charakter pomocniczy przy wyjaśnianiu zakresu zarówno podmiotowego jak i przedmiotowego ustawy.

		komunikatu z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), IMAP4 (Internet Message Access Protocol) lub innego standardu zapewniającego te same funkcje; 9) podmiot publiczny – podmiot, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; 10) przedsiębiorca telekomunikacyjny – przedsiębiorcę w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 12) sieć telekomunikacyjna – sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 13) tajemnica telekomunikacyjna – tajemnicę telekomunikacyjną, o której mowa w art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 14) uprawnione podmioty – uprawnione podmioty, o których mowa w art. 179 ust. 3 pkt 1 lit. a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 15) urządzenie telekomunikacyjne – urządzenie telekomunikacyjne w rozumieniu art. 2 pkt 46 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 18) usługa telekomunikacyjna – usługę telekomunikacyjną w rozumieniu art. 2 pkt 48 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 19) użytkownik – użytkownik w rozumieniu art. 2 pkt 49 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 20) użytkownik końcowy – użytkownik końcowy w rozumieniu art. 2 pkt 50 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.	

2.	Art. 6	**Art. 6.** 1. Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec zablokowania, o którym mowa w art. 5 pkt 1. 2. Sprzeciw zawiera: 1) pełną treść krótkiej wiadomości tekstowej (SMS); 2) uzasadnienie wyjaśniające dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu; 3) wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS); 4) dane identyfikujące nadawcę: a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych, b) nazwę (firmę) podmiotu, adres siedziby, numer z właściwego rejestru - w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej, c) imię i nazwisko osoby uprawnionej do reprezentowania nadawcy wraz z upoważnieniem – jeżeli dotyczy. 3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się na adres do doręczeń elektronicznych Prezesa UKE. 4. Sprzeciw niespełniający wymagań, o których mowa w ust. 2 i 3, pozostawia się bez rozpoznania.	Niniejsza ustawa oprócz implementacji przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej wprowadza również zmiany w zakresie zwalczania nadużyć w komunikacji elektronicznej mające służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania tym nadużyciom przez przedsiębiorców telekomunikacyjnych oraz w dalszej perspektywie przepisy te pozwolą ograniczyć skalę nadużyć. Niniejszy przepis przewiduje dla nadawcy krótkiej wiadomości tekstowej (SMS) możliwość wniesienia sprzeciwu wobec zablokowania krótkiej wiadomości tekstowej (SMS) zawierającej treści zawarte we wzorcu wiadomości smishingowej. Ma to na celu umożliwienie potwierdzenia nadużycia bądź stwierdzenie jego braku, a także czyni zadość interesom oraz prawom nadawcy takiej wiadomości. Pozwoli to również udoskonalić wzorce wiadomości smishingowych, tak aby tylko wiadomości stanowiące nadużycia w komunikacji elektronicznej były blokowane.
3.	Art. 7	**Art. 7.** 1. Prezes UKE: 1) rozpatruje sprzeciw, w terminie 14 dni od dnia jego otrzymania oraz	Przyjęcie niniejszego przepisu jest konieczne z racji powiązania z prawem przysługującym nadawcy krótkiej wiadomości tekstowej (SMS) w przepisie poprzedzającym. Zatem niniejszy przepis zawiera

		2) niezwłocznie informuje nadawcę krótkiej wiadomości tekstowej (SMS) o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył nadawca krótkiej wiadomości tekstowej (SMS), wnosząc sprzeciw. 2. Prezes UKE rozpatrując sprzeciw: 1) uwzględnia sprzeciw, jeżeli treść krótkiej wiadomości tekstowej (SMS) zawierająca treści wskazane we wzorcu wiadomości nie wyczerpuje znamion smishingu, albo 2) nie uwzględnia sprzeciwu, jeżeli treść krótkiej wiadomości tekstowej (SMS) zawierająca treści wskazane we wzorcu wiadomości wyczerpuje znamiona smishingu. 3. W przypadku uwzględnienia sprzeciwu, Prezes UKE nakazuje CSIRT NASK niezwłoczną, nie później niż w terminie 3 dni od dnia uwzględnienia sprzeciwu, zmianę wzorca wiadomości w taki sposób, aby krótka wiadomość tekstowa (SMS), o treści o której mowa w art. 6 ust. 2 pkt 1, nie była blokowana. 4. Prezes UKE może pisemnie upoważnić pracownika Urzędu Komunikacji Elektronicznej do wykonywania czynności, o których mowa w ust. 1–3. 5. Do postępowania w sprawie rozpatrzenia sprzeciwu nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego (Dz. U. z 2022 r. poz. 2000 i 2185).	obowiązki Prezesa UKE oraz CSIRT NASK związane z procedurą odwoławczą dla nadawcy wiadomości uznanej za wyczerpującą znamiona nadużycia w komunikacji elektronicznej. Prezes UKE będzie obowiązany rozpatrzyć sprzeciw co do zasady w terminie 14 dni od dnia jego otrzymania.
4.	Art. 10 ust. 1-14	**Art. 10.** 1. Prezes UKE prowadzi, przy pomocy systemu teleinformatycznego, jawny wykaz numerów służących wyłącznie do odbierania połączeń głosowych i udostępnia ten wykaz w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.	Konieczność wprowadzenia niniejszego przepisu w życie związana jest z podszywaniem się oszustów pod jednostki sektora finansów publicznych czy innych przedsiębiorców za pomocą wykorzystywania numerów infolinii tych podmiotów. Numery te nie są wykorzystywane do wykonywania połączeń do konsumentów czy obywateli, jednakże nieświadomi

		2. Prezes UKE dokonuje wpisu numeru do wykazu, o którym mowa w ust. 1, na wniosek: 1) banku, w rozumieniu art. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2022 r. poz. 2324, 2339, 2640 i 2707 oraz z 2023 r. poz. 180), 2) firmy inwestycyjnej, w rozumieniu art. 3 pkt 33 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2022 r. poz. 1500, 1488, 1933, 2185 i 2640 oraz z 2023 r. poz. 180)), 3) funduszu inwestycyjnego, w rozumieniu art. 3 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (Dz. U. z 2022 r. poz. 1523, 1488, 1933, 2185 i 2640), 4) instytucji płatniczej, w rozumieniu art. 2 pkt 11 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2022 r. poz. 2360 i 2640), 5) jednostki sektora finansów publicznych, o której mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, z późn. zm.[1)]), 6) Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej, 7) oddziału instytucji kredytowej, w rozumieniu art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, 8) spółdzielczej kasy oszczędnościowo-kredytowej, o której mowa w art. 1 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo--kredytowych (Dz. U. z 2022 r. poz. 924, 1358, 1488, 1933, 2339 i 2640),	tego użytkownicy końcowi mogą paść ofiarami takich oszustw. Przepis ten zawiera obowiązek Prezesa Urzędu Komunikacji Elektronicznej prowadzenia jawnego wykazu numerów, które służą wyłącznie do odbierania połączeń głosowych. Rozwiązanie to ograniczy możliwość podszywania się oszustów pod numery infolinii urzędów czy innych podmiotów.

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1692, 1725, 1747, 1768 i 1964 i 2414.

		9) towarzystwa funduszy inwestycyjnych, w rozumieniu art. 38 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, 10) zakładu reasekuracji, o którym mowa w art. 6 ust. 2 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2022 r. poz. 2283 i 2640), 11) zakładu ubezpieczeń, o którym mowa w art. 6 ust. 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej – w zakresie wykorzystywanych przez te podmioty numerów. 3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykazu, o którym mowa w ust. 1, numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego wyłącznie na potrzeby własnego biura obsługi klientów lub infolinii. 4. Wniosek, o którym mowa w ust. 2 i 3, zawiera: 1) dane wnioskodawcy: a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych, b) nazwę (firmę) wnioskodawcy, adres siedziby, numer z właściwego rejestru w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej, c) imię i nazwisko osoby uprawnionej do reprezentowania wnioskodawcy wraz z upoważnieniem; 2) wskazanie numeru, który ma służyć wyłącznie do odbierania połączeń głosowych; 5. Do wniosku, o którym mowa w ust. 2 i 3 dołącza się dokument potwierdzający prawo do dysponowania numerem.	

		6. W przypadku gdy wniosek, o którym mowa w ust. 2 i 3, nie spełnia wymagań, o których mowa w ust. 4, Prezes UKE wzywa wnioskodawcę do uzupełnienia wniosku w terminie 7 dni od dnia otrzymania wezwania pod rygorem pozostawienia wniosku bez rozpoznania. 7. Prezes UKE dokonuje wpisu numeru do wykazu, o którym mowa w ust. 1, w terminie 5 dni od dnia otrzymania wniosku spełniającego wymagania, o których mowa w ust. 4 i 5. 8. Wpis do wykazu, o którym mowa w ust. 1, jest czynnością materialno-techniczną. 9. Prezes UKE pozostawia wniosek o wpis do wykazu, o którym mowa w ust. 1, bez rozpoznania jeżeli wniosek został złożony przez podmiot nieuprawniony albo dotyczy on numeru niewykorzystywanego przez wnioskodawcę. Prezes UKE niezwłocznie informuje wnioskodawcę o pozostawieniu wniosku bez rozpoznania. 10. Wnioskodawca, który złożył wniosek, o którym mowa w ust. 2 i 3, lub podmiot, który aktualnie korzysta z numeru wpisanego do wykazu, o którym mowa w ust. 1, może w każdym czasie złożyć wniosek o wycofanie numeru z wykazu. 11. Do wniosku o wycofanie numeru z wykazu ust. 4 i 5 stosuje się odpowiednio. 12. W przypadku, o którym mowa w ust. 10, Prezes UKE niezwłocznie, jednak nie później niż w terminie 5 dni od dnia otrzymania wniosku o wycofanie numeru z wykazu, o którym mowa w ust. 1, wykreśla go z tego wykazu. 13. Wniosek, o którym mowa w ust. 2, 3 i 10, opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE na adres do doręczeń elektronicznych Prezesa UKE.	

		14. Wniosek nie spełniający wymagań, o których mowa w ust. 13 pozostawia się bez rozpoznania.	
5.	Art. 11	**Art. 11.** Wykaz, o którym mowa w art. 10 ust. 1, obejmuje: 1) wskazanie numeru służącego wyłącznie do odbierania połączeń głosowych; 2) datę wpisania numeru, o którym mowa w pkt 1, do wykazu; 3) datę wykreślenia numeru, o którym mowa w pkt 1, z wykazu.	Przepis niezbędny do wprowadzenia ze względu na związek z przepisem go poprzedzającym. Dookreśla wymogi związane z prowadzeniem przez Prezesa UKE wykazu.
6.	Art. 14	**Art. 14.** 1. Podmiot posiadający tytuł prawny do domeny internetowej wpisanej na listę ostrzeżeń może wnieść do Prezesa UKE sprzeciw wobec wpisania domeny internetowej na listę ostrzeżeń. 2. Sprzeciw zawiera: 1) wskazanie domeny internetowej, której dotyczy; 2) uzasadnienie wyjaśniające dlaczego wpisanie domeny na listę ostrzeżeń było niezasadne; 3) dane identyfikujące podmiot posiadający tytuł prawny do domeny internetowej: a) imię (imiona) i nazwisko, adres zamieszkania – w przypadku osób fizycznych, b) nazwę (firmę) podmiotu, adres siedziby, numer z właściwego rejestru – w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej, c) imię i nazwisko osoby uprawnionej do reprezentowania podmiotu posiadającego tytuł prawny do domeny internetowej wraz z upoważnieniem – jeżeli dotyczy.	Przepis przewiduje możliwość wniesienia sprzeciwu wobec umieszczenia domeny internetowej na liście ostrzeżeń. Ma to na celu umożliwienie potwierdzenia nadużycia bądź stwierdzenie jego braku, a także czyni zadość interesom oraz prawom podmiotu posiadającego tytuł prawny do domeny. Pozwoli to również udoskonalić system ostrzegający przed takimi domenami, tak aby tylko domeny stanowiące nadużycia w komunikacji elektronicznej trafiały na listę ostrzeżeń.

		3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się na adres do doręczeń elektronicznych Prezesa UKE. 4. Sprzeciw niespełniający wymagań, o których mowa w ust. 2 i 3, pozostawia się bez rozpoznania.	
7.	Art. 15	**Art. 15.** 1. Prezes UKE: 1) rozpatruje sprzeciw, w terminie 14 dni od dnia jego otrzymania oraz 2) niezwłocznie informuje podmiot wnosząc sprzeciw o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył podmiot wnosząc sprzeciw. 2. Prezes UKE rozpatrując sprzeciw: 1) uwzględnia sprzeciw, jeżeli domena internetowa nie służy do wyłudzeń danych i środków finansowych użytkowników internetu; 2) nie uwzględnia sprzeciwu, jeżeli domena internetowa służy do wyłudzeń danych i środków finansowych użytkowników internetu. 3. W przypadku uwzględnienia sprzeciwu, Prezes UKE nakazuje CSIRT NASK niezwłoczne, nie później niż w terminie 3 dni od dnia uwzględnienia sprzeciwu, usunięcie domeny internetowej z listy ostrzeżeń. 4. Prezes UKE może pisemnie upoważnić pracownika Urzędu Komunikacji Elektronicznej do wykonywania czynności, o których mowa w ust. 1–3. 5. Do postępowania w sprawie rozpatrzenia sprzeciwu nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego.	Przyjęcie niniejszego przepisu jest konieczne z racji powiązania z prawem przysługującym podmiotowi posiadającego tytuł prawny do domeny internetowej w przepisie poprzedzającym. Zatem niniejszy przepis zawiera obowiązki Prezesa UKE oraz CSIRT NASK związane z procedurą odwoławczą dla właściciela domeny wpisane na listę ostrzeżeń. Prezes UKE będzie obowiązany rozpatrzyć sprzeciw co do zasady w terminie 14 dni od dnia jego otrzymania.

8.	Art. 17	**Art. 17.** 1. Dostawca poczty elektronicznej: 1) dla co najmniej 500 000 użytkowników poczty, lub 2) dla podmiotu publicznego – przy świadczeniu poczty elektronicznej ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail). 2. Podmiot publiczny jest obowiązany do korzystania z poczty elektronicznej wykorzystującej mechanizmy, o których mowa w ust. 1. 3. Prezes UKE może przeprowadzić kontrolę: 1) wykonywania obowiązku, o którym mowa w ust. 1, przez dostawcę poczty elektronicznej oraz 2) wykonywania obowiązku, o którym mowa w ust. 2, przez podmiot publiczny. 4. Do kontroli, o której mowa w ust. 3 stosuje się przepisy działu X rozdziału 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. 5. CSIRT NASK udostępnia 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, o których mowa w ust. 1. 6. Dostawca poczty elektronicznej dla podmiotu publicznego oferuje pocztę elektroniczną umożliwiającą stosowanie metod uwierzytelniania wieloskładnikowego.	Przepis przewiduje dodatkowe obowiązki z zakresu bezpieczeństwa poczty elektronicznej w postaci obowiązku stosowania wyszczególnionych w przepisie mechanizmów uwierzytelniania poczty elektronicznej. Obowiązki te dotyczyć będą dostawców poczty elektronicznej dla co najmniej 500 000 użytkowników lub dla podmiotu publicznego, przy czym sam podmiot publiczny będzie zobowiązany do korzystania z poczty elektronicznej wykorzystującej przedmiotowe mechanizmy uwierzytelniania. Taka regulacja przyczyni się do szerszego i skuteczniejszego zapewnienia bezpieczeństwa w komunikacji elektronicznej na dużą skalę. Równocześnie ograniczenie zakresu podmiotowego tego przepisu sprawia, że nie dojdzie do nałożenia nadmiarowych obowiązków na małych przedsiębiorców.

9.	Art. 18	**Art. 18.** 1. Przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji informacji o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją: 1) obowiązku, o którym mowa w art. 5, 2) uprawnienia, o którym mowa w art. 8 – w zakresie umożliwiającym rozpatrzenie reklamacji, o której mowa w art. 106 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. 2. Przedsiębiorca telekomunikacyjny przechowuje informacje, o których mowa w ust. 1, przez okres 12 miesięcy liczony od dnia w którym usługa miała być wykonana, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu.	Przepis ten nakłada na przedsiębiorców telekomunikacyjnych obowiązek rejestracji danych o niewykonanych usługach w związku z blokowaniem krótkich wiadomości tekstowych (SMS), a także wskazuje przez jaki okres dane te mają być przechowywane ze szczególnym uwzględnieniem potrzeb postępowania reklamacyjnego. Stworzenie takiej bazy danych pozostaje w związku z przeciwdziałaniem oraz zwalczaniem nadużyć w komunikacji elektronicznej. Stanowi też gwarancję, że konsumenci będą mogli dochodzić swoich praw.
10.	Art. 19	**Art. 19.** 1. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej. 2. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać komunikat w celu identyfikacji, zapobiegania i zwalczania smishingu oraz wiadomości multimedialnych (MMS), o których mowa w art. 8 ust. 2. 3. Przedsiębiorca telekomunikacyjny może przetwarzać: 1) treści krótkich wiadomości tekstowych (SMS), 2) treści wiadomości multimedialnych (MMS) oraz 3) informacje o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku, o którym mowa w art. 5 i art. 9 lub uprawnienia, o którym mowa w art. 8	Niniejszy przepis ma na celu wskazanie jakie uprawnienia przysługują przedsiębiorcom telekomunikacyjnym w zakresie przetwarzania i wzajemnego udostępniania informacji, w tym informacji objętych tajemnicą telekomunikacyjną, z wyłączeniem komunikatu, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.

		– w celu realizacji obowiązku, o którym mowa w art. 3 ust. 2, art. 5 i art. 9 oraz realizacji uprawnienia, o którym mowa w art. 8, a także w celach związanych z dochodzeniem roszczeń. 4. Przetwarzanie, o którym mowa w ust. 3 dopuszczalne jest tylko do końca okresu, w którym możliwe jest dochodzenie roszczeń. 5. Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwane dalej „rozporządzeniem 2016/679", nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. 6. Przedsiębiorca telekomunikacyjny może wykonać obowiązek, o którym mowa w art. 14 ust. 1 i 2 rozporządzenia 2016/679, przez udostępnienie informacji, o których mowa w tych przepisach, na swojej stronie internetowej lub przez umieszczenie stosownych informacji w miejscach widocznych w siedzibie lub miejscu działania administratora danych osobowych, w zakresie w jakim dotyczy to danych osobowych pozyskanych w ramach identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.	
11.	Art. 20 ust. 4, 7, 9	4. Na dostawcę poczty elektronicznej, który nie wypełnia obowiązków, o których mowa w art. 17 ust. 1, może zostać nałożona kara pieniężna, jeżeli przemawia za tym zakres lub charakter naruszenia. 7. Prezes UKE może, w drodze decyzji, nałożyć karę pieniężną na kierownika podmiotu publicznego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 17 ust. 2. Kara pieniężna nakładana jest w wysokości do jednokrotności przeciętnego wynagrodzenia w gospodarce narodowej,	Przepis przewiduje fakultatywne kary administracyjne dla podmiotów dokonujących nadużyć w komunikacji elektronicznej. Celem niniejszego uregulowania jest zarówno wywołanie skutku prewencyjnego jak i represyjnego. Ponadto przepis ten pozostaje w związku z ustawą z dnia 2 grudnia 2021 r. o szczególnych zasadach

		ogłaszanego przez Prezesa Głównego Urzędu Statystycznego, w ostatnim komunikacie, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504, 1504 i 2461). 9. Kary pieniężne, o których mowa w art. 20 ust. 1, 3 i 4, nakładane przez Prezesa UKE, stanowią dochód budżetu państwa.	wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, ponieważ wpływy z kar administracyjnych miałyby stanowić przychód Funduszu Cyberbezpieczeństwa, o którym mowa w przytoczonej ustawie. Jest to niezbędne dla zapewnienia skutecznej realizacji celów ustawy.
12.	Art. 22-25	**Art. 22.** 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody wysyła lub odbiera komunikaty lub połączenia głosowe w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe – podlega karze pozbawienia wolności od 3 miesięcy do lat 5. 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. **Art. 23.** 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody wysyła krótką wiadomość tekstową (SMS), wiadomość multimedialną (MMS) lub wiadomość za pośrednictwem innych usług komunikacji interpersonalnej, w której podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego, instalacji oprogramowania, przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji	Wprowadzenie niniejszych przepisów ma na celu penalizację wskazanych w nim nadużyć w komunikacji elektronicznej – m.in. tworzenie sztucznego ruchu, wysyłania smishingu lub dokonywania działań o charakterze CLI spoofingu w celu osiągnięcia korzyści majątkowej, osobistej lub wyrządzenia innej osobie szkody. Ustanowienie takich przepisów ma na celu doprecyzowanie przesłanek ponoszenia odpowiedzialności za działanie niezgodne z ustawą, a tym samym precyzyjne określanie wymiaru kary za dokonane przez sprawcę działania.

		przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej – podlega karze pozbawienia wolności od 3 miesięcy do lat 5. 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. 3. Jeżeli czyn, o którym mowa w ust. 1, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego. **Art. 24.** 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody, przy wywoływaniu połączenia głosowego posługuje się, nie będąc do tego uprawnionym, informacją adresową wskazującą na inną osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, aby podszyć się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania, przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej – podlega karze pozbawienia wolności od 3 miesięcy do lat 5. 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. 3. Jeżeli czyn, o którym mowa w ust. 1, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego. **Art. 25.** 1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody dokonuje nieuprawnionej modyfikacji informacji adresowej uniemożliwiającej lub istotnie utrudniającej ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu,	

		numeru telefonu lub identyfikatora, przy użyciu którego nastąpiło wysłanie komunikatu – podlega karze pozbawienia wolności od 3 miesięcy do lat 5. 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.	
13.	Art. 26	**Art. 26.** 1. Prezes UKE przedstawia sejmowej komisji właściwej w sprawach telekomunikacji oraz ministrowi właściwemu do spraw informatyzacji roczne sprawozdanie z wykonywania swoich obowiązków i uprawnień określonych w niniejszej ustawie. 2. Prezes UKE składa sprawozdanie do dnia 31 marca danego roku kalendarzowego, za rok poprzedni.	Przepis ma na celu nałożenie obowiązku na Prezesa Urzędu Komunikacji Elektronicznej polegającego na przedstawieniu sejmowej komisji właściwej w sprawach nowych technologii oraz ministrowi właściwemu do spraw informatyzacji rocznego sprawozdania z wykonywania zadań określonych w ustawie co stanowi realizację funkcji kontrolnej.
14.	Art. 27	**Art. 27.** W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581) w art. 192 w ust. 1 w pkt 2 w lit. b w tiret czwartym średnik zastępuje się przecinkiem i dodaje się tiret piąte w brzmieniu: „– z dnia …. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. ...);”.	Przepis o charakterze zmieniającym, mający na celu dodanie do ustawy Prawo Telekomunikacyjne kolejny tiret odnoszący do ustawy o zwalczaniu nadużyć w komunikacji elektronicznej – dzięki temu uzupełniony zostanie katalog zadań Prezesa UKE.
15.	Art. 28	**Art. 28.** W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57) w art. 4 po pkt 2 dodaje się pkt 2a w brzmieniu: „2a) obowiązku stosowania, w zakresie korzystania, przy realizacji zadań publicznych, poczty elektronicznej wykorzystującej mechanizmy uwierzytelniania, o których mowa w art. 17 ust. 1	Przepis zmienia ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne – wskazuje w niej, że nie narusza ona obowiązków dot. stosowania przez podmioty publiczne mechanizmów uwierzytelniania poczty elektronicznej.

		z ustawy z dnia… o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. ….).”.	
16.	Art. 29	**Art. 29.** W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666) w art. 26 w ust. 6 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu: „4) monitorowanie występowania smishingu oraz tworzenie wzorca wiadomości wyczerpującej znamiona smishingu, o którym mowa w art. 4 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …).”.	Niniejszy przepis ma na celu wprowadzenie zmiany w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która wynika z dotychczas opisywanych przepisów przedmiotowej ustawy oraz ma związek z monitorowaniem występowania smishingu i tworzeniem wzorca wiadomości wyczerpującej znamiona smishingu. Zmiana ta jest konieczna ze względu na rolę jaką będzie odgrywał NASK w zwalczaniu nadużyć telekomunikacji elektronicznej. W związku z tym te zadania muszą znaleźć odzwierciedlenie w akcie prawnym podstawowym dla funkcjonowania CSIRT NASK.
17.	Art. 30	**Art. 30.** 1. CSIRT NASK w terminie 3 miesiące od dnia wejścia w życie ustawy uruchamia system, o którym mowa w art. 4 ust. 3, i informuje ministra właściwego do spraw informatyzacji o jego uruchomieniu.. 2. Minister właściwy do spraw informatyzacji niezwłocznie po otrzymaniu informacji, o której mowa w ust. 1, udostępnia, w Biuletynie Informacji Publicznej na swojej stronie podmiotowej, informację o uruchomieniu systemu, o którym mowa w art. 4 ust. 3. 3. Komendant Centralnego Biura Zwalczania Cyberprzestępczości, 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.	W przepisie ustanowiono obowiązki związane z uruchomieniem i wdrożeniem przez CSIRT NASK systemu teleinformatycznego do przekazywania informacji o wzorcach wiadomości zawierających smishing. Wprowadzenie niniejszej regulacji jest niezbędne do prawidłowego funkcjonowania systemu teleinformatycznego o którym mowa w ustawie oraz do określenia obowiązków podmiotów, o których przepis stanowi.

18.	Art. 32	**Art. 32.** 1. W terminie miesiąca od dnia wejścia w życie niniejszego przepisu strony porozumienia o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, zawartego w dniu 23 marca 2020 r., zwanego dalej „Porozumieniem z 23 marca 2020 r.", mogą złożyć oświadczenie woli o uznaniu Porozumienia z 23 marca 2020 r. za porozumienie, o którym mowa w art. 13 ust. 1. 2. W przypadku złożenia w terminie, o którym mowa w ust. 1, oświadczeń woli przez wszystkie strony Porozumienia z 23 marca 2020 r. staje się ono porozumieniem, o którym mowa w art. 13 ust. 1, z dniem złożenia oświadczenia woli przez ostatnią ze stron. W takim przypadku postanowienia Porozumienia z 23 marca 2020 r. ograniczające stosowanie tego porozumienia do stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej stają się bezskuteczne. 3. Z dniem uznania Porozumienia z 23 marca 2020 r. za porozumienie, o którym mowa w art. 13 ust. 1, lista ostrzeżeń dotycząca domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu, prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie Porozumienia z 23 marca 2020 r. staje się listą, o której mowa w art. 13 ust. 1.	Niniejszy przepis pełni funkcję dostosowującą. Celem przepisu jest uznanie porozumienia o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczpospolitej Polskiej za porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych.
19.	Art. 33	**Art. 33.** 1. Dostawca poczty elektronicznej, który świadczy pocztę elektroniczną na podstawie umowy, której stroną jest podmiot publiczny, obowiązującej w dniu wejścia w życie ustawy, jest obowiązany w terminie	Niniejszy przepis pełni funkcję dostosowującą. Określa on okres jaki podmioty publiczne będą miały na realizację obowiązków związanych z

		3 miesięcy od dnia wejścia w życie ustawy do spełnienia obowiązku, o których mowa w art. 17 ust. 1. 2. Jeżeli dostawca poczty elektronicznej nie spełni wymagań w terminie, o którym mowa w ust. 1, umowa może zostać jednostronnie rozwiązana przez podmiot publiczny a dostawcy poczty elektronicznej nie przysługują roszczenia z tego tytułu.	zapewnieniem bezpieczeństwa wykorzystywanym przez nich usługom poczty elektronicznej.
20.	Art. 34	**Art. 34.** W terminie 6 miesięcy od dnia wejścia w życie ustawy, dostawca poczty elektronicznej, który zawarł umowę z podmiotem publicznym o świadczenie poczty elektronicznej, przedstawi ofertę poczty elektronicznej umożliwiającej stosowanie metod uwierzytelniania wieloskładnikowego, chyba że świadczona przez tego dostawcę poczta elektroniczna umożliwia stosowanie tych metod.	Przepis ten nakazuje dostawcy poczty elektronicznej dla podmiotu publicznego przedstawienie oferty poczty elektronicznej umożliwiającej stosowanie metod uwierzytelniania wieloskładnikowego w terminie 6 miesięcy od dnia wejścia w życie ustawy.
21.	Art. 35	**Art. 35.** Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem: 1) art. 2 pkt 1, 5 i 10, art. 13-art. 15 oraz art. 32, które wchodzą w życie z dniem następującym po dniu ogłoszenia; 2) art. 20 ust. 3 pkt 1, który wchodzi w życie po upływie 6 miesięcy od dnia wejścia w życie ustawy; 3) art. 20 ust. 3 pkt 2, który wchodzi w życie po upływie 12 miesięcy od dnia wejścia w życie ustawy.	To przepis określający moment wejścia w życie ustawy.