Projekt z 22.11.2022 r.

U S T A W A

z dnia 2022 r.

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

Art. 1. Ustawa określa:

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

Art. 2. Określenia użyte w ustawie oznaczają:

1) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, o którym mowa w art. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863);
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;

---

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 321/36).

2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

4) komunikat – komunikat, o którym mowa w art. 2 pkt 17 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648 i 1933);
5) lista ostrzeżeń – jawna lista ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych 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 siebie lub innej osoby fizycznej, osoby prawnej, jednostki organizacyjnej nieposiadającej osobowości prawnej;
7) operator – operatora, o którym mowa w 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, o którym mowa w 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, o której mowa w art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
13) tajemnica telekomunikacyjna – tajemnicę, o której mowa w art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
14) uprawnione podmioty – podmioty, o których mowa w art. 179 ust. 3 pkt 1 lit. a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
15) 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;

16) usługa komunikacji interpersonalnej niewykorzystująca numerów – usługę komunikacji interpersonalnej, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji;
17) usługa telekomunikacyjna – usługę, o której mowa w art. 2 pkt 48 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
18) użytkownik – użytkownik, o którym mowa w art. 2 pkt 49 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
19) użytkownik końcowy – użytkownik końcowy, o którym mowa w art. 2 pkt 50 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Art. 3. 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności dotyczące:

1) wysyłania lub odbierania 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 (sztuczny ruch);
2) wysłania 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) nieuprawnionego posłużenia się lub korzystania przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, 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 przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania (CLI spoofing);
4) nieuprawnionego modyfikowania informacji adresowej uniemożliwiającego lub istotnie utrudniającego 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 technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.

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

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

3. CSIRT NASK udostępnia, za pomocą systemu teleinformatycznego, informacje o wystąpieniu smishingu wraz ze wzorcem wiadomości i przekazuje te informacje przedsiębiorcom telekomunikacyjnym.

4. Komendant Centralnego Biura Zwalczania Cyberprzestępczości, Prezes UKE i przedsiębiorcy telekomunikacyjni, w celu wymiany informacji o wystąpieniu smishingu, w tym wzorców wiadomości, są obowiązani do korzystania z systemu, o którym mowa w ust. 3.

5. 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. 3.

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

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

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

7. 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.

8. CSIRT NASK odpowiada za funkcjonowanie systemu teleinformatycznego, o którym mowa w art. 4 ust. 3, oraz jest administratorem danych przetwarzanych w tym systemie.

Art. 5. Przedsiębiorca telekomunikacyjny po otrzymaniu informacji, o której mowa w art. 4 ust. 3 lub 6, jest obowiązany do niezwłocznego:

1) blokowania krótkich wiadomości tekstowych (SMS) zawierających treści zawarte we wzorcu wiadomości, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (SMS);
2) zaprzestania blokowania krótkich wiadomości tekstowych (SMS) w przypadku uzyskania informacji, 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, krótkiej wiadomości tekstowej (SMS) zawierającej treści zawarte we wzorcu wiadomości.

2. Sprzeciw zawiera:

1) dokładną treść krótkiej wiadomości tekstowej (SMS) zablokowanej za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (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 jednoznacznie identyfikujące nadawcę, w szczególności:
   a) imię i nazwisko, adres zamieszkania – w przypadku osób fizycznych,
   b) nazwę podmiotu, adres, numer z właściwego rejestru - w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej.

3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE, 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) składając 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. 3, 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 jawny wykaz numerów służących wyłącznie do odbierania połączeń głosowych i udostępnia go 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, o którym mowa w art. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2021 r. poz. 2439, z późn. zm.[3)]),
2) firmy inwestycyjnej, o której mowa w art. 3 pkt 33 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2022 r. poz. 1500, 1488, 1933 i 2185),
3) funduszu inwestycyjnego, o którym mowa w art. 3 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (Dz. U. z 2022 r. poz. 1523, 1488, 1933 i 2185),
4) instytucji płatniczej, o której mowa w art. 2 pkt 11 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2021 r. poz. 1907 i 2140 oraz z 2022 r. poz. 1488),
5) jednostki sektora finansów publicznych, o której mowa w art. 9 z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, 1692, 1725, 1747, 1768 i 1964),
6) Krajowej 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, 1358, 1488 i 1933),
7) oddziału instytucji kredytowej, o którym mowa w 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,
9) towarzystwa funduszy inwestycyjnych, o którym mowa w art. 38 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. 2021 r. poz. 1130, z późn. zm.[4)]),
11) zakładu ubezpieczeń, o którym mowa w art. 6 ust. 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej

---

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 2447 oraz z 2022 r. poz. 830, 872, 1358, 1488, 1692 i 1933.

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 2140 i 2328 oraz z 2022 r. poz. 655, 1488 i 1933.

– w zakresie wykorzystywanych przez te podmioty numerów.

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 własnego biura obsługi klientów lub infolinii.

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

1) wskazanie podmiotu, od którego pochodzi;
2) numer, który ma służyć wyłącznie do odbierania połączeń głosowych;
3) dowód dysponowania prawem do korzystania z numeru.

5. W przypadku gdy wniosek, o którym mowa w ust. 2 i 3, nie zawiera informacji, o których mowa w ust. 4, Prezes UKE wzywa podmiot do ich uzupełnienia w terminie 7 dni od dnia otrzymania wezwania pod rygorem pozostawienia wniosku bez rozpoznania.

6. 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.

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

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

9. Podmiot, który złożył wniosek, o którym mowa w ust. 2 i 3, lub aktualnie korzysta z numeru, który wcześniej został wpisany do wykazu, o którym mowa w ust. 1, może w każdym czasie go wycofać. W takim przypadku 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.

10. Wniosek, o którym mowa w ust. 2 i 3, oraz wniosek o wycofanie numeru z wykazu, o którym mowa w ust. 1, opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE na adres do doręczeń elektronicznych Prezesa UKE.

11. Wniosek niespełniający wymagań, o których mowa w ust. 10, pozostawia się bez rozpoznania.

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

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

Art. 11. 1. Prezes UKE prowadzi wykaz, o którym mowa w art. 10 ust. 1, przy pomocy systemu teleinformatycznego.

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

1) oznaczenie 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 operatorów będących stronami 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 wprowadzonych środków technicznych i organizacyjnych, 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 dziale 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, które będą stosowali ci przedsiębiorcy przy 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 techniczne i organizacyjne określone w rekomendacjach, o których mowa w ust. 6, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem wprowadzonych tych 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, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania listy ostrzeżeń oraz uniemożliwienia dostępu do tych stron.

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

3. Każdy może zgłosić domenę internetową mogącą służyć do wyłudzeń danych i środków finansowych do CSIRT NASK. Zgłoszenie każdej domeny wymaga uzasadnienia.

4. Po otrzymaniu zgłoszenia lub samodzielnie CSIRT NASK wpisuje domenę internetową na listę ostrzeżeń, jeżeli spełnia ona przesłanki określone w ust. 2.

5. CSIRT NASK określi sposób dokonywania zgłoszeń, o których mowa w ust. 3. Komunikat w tej sprawie CSIRT NASK publikuje na stronie podmiotowej Biuletynu Informacji Publicznej Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego.

6. 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.

7. Porozumienie określa co najmniej:

1) CSIRT NASK jako odpowiedzialny za opracowanie, prowadzenie i utrzymanie listy ostrzeżeń oraz udostępnianie jej na stronie internetowej CSIRT NASK;
2) zasady współpracy między stronami, w tym zasady zgłaszania domen internetowych oraz wpisywania na listę ostrzeżeń.

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 wypadku 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 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 środków finansowych.

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 liście ostrzeżeń.

2. Sprzeciw zawiera:

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

3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE, 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 składający sprzeciw o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył podmiot składając 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.

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

2. W decyzji, o której mowa w ust. 1, Prezes UKE określa termin na zablokowanie dostępu do numeru lub usługi lub zaprzestanie świadczenia usługi nie krótszy niż 6 godzin od momentu doręczenia decyzji.

3. 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.

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

5. 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

– 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. Przepisy działu X rozdziału 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stosuje się.

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, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu. Okres przechowywania danych liczony jest od dnia, w którym usługa miała być wykonana.

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 również 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) dane 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 na cele związane z dochodzeniem roszczeń. Przetwarzanie to dopuszczalne jest tylko do końca okresu, w którym możliwe jest dochodzenie roszczeń.

4. 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.

5. 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.

Art. 20. 1. Przedsiębiorca telekomunikacyjny, który dokonuje nadużyć w komunikacji elektronicznej, o których mowa w art. 3 ust.1 pkt 1–4, 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. 12

– 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 niewykonanie obowiązku, o którym mowa w art. 17 ust. 2 przyczyniło się do wystąpienia incydentu w podmiocie publicznym w rozumieniu art. 2 pkt. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 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 i 1504).

8. Od decyzji Prezesa UKE w sprawie nałożenia kary 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 lub osiągnął przychód w wysokości nieprzekraczającej 500

000 zł, Prezes UKE, nakładając karę pieniężną, uwzględnia średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających rok nałożenia kary pieniężnej.

3. 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.

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 trzech 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 tysięcy złotych.

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

9. Wpływy z tytułu kar pieniężnych, o których mowa w art. 20, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 1 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2021 r. poz. 2333 oraz z 2022 r. poz. 655).

10. Prezes UKE przekazuje na rachunek Funduszu Cyberbezpieczeństwa środki pochodzące z kar w terminie 30 dni od dnia ich pobrania.

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, rozporządzenia majątkiem, 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, 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 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 elektronicznego

– 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 nowych technologii oraz ministrowi właściwemu do spraw informatyzacji roczne sprawozdanie z wykonywania swoich obowiązków i uprawnień określonych w niniejszej ustawie.

2. Sprawozdanie składa się 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 i 1933) w art. 192 w ust. 1 w pkt 2 w lit. b w tirecie czwartym średnik zastępuje się przecinkiem i dodaje się tiret piąty w brzmieniu:

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

Art. 27a. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070 i 1641 oraz z 2022 r. poz. 1087) po art. 13b dodaje się art. 13c w brzmieniu:

„Art. 13c. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863), korzysta, przy realizacji zadań publicznych, z 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. 28. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863) 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. 29. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333 oraz z 2022 r. poz. 655) w art. 2 w ust. 4 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) wpływy z kar pieniężnych, o których mowa w art. 19 ust. 1 i 2 oraz 4 i 5 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …);”.

Art. 30. 1. CSIRT NASK uruchomi system, o którym mowa w art. 4 ust. 3, i poinformuje ministra właściwego do spraw informatyzacji, w terminie nie późniejszym niż 3 miesiące od dnia wejścia w życie ustawy.

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

Art. 31. Kary pieniężnej:

1) o której mowa w art. 20 ust. 3 pkt 1, nie nakłada się przed upływem 6 miesięcy od dnia wejścia w życie ustawy;
2) o której mowa w art. 20 ust. 3 pkt 2, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.

Art. 32. Przedsiębiorcy telekomunikacyjni są obowiązani do wdrożenia rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej, o których mowa w:

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

Art. 33. 1. Z dniem wejścia w życie ustawy 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, zawarte w dniu 23 marca 2020 r., staje się porozumieniem, o którym mowa w art. 13 ust. 1.

2. Z dniem wejścia w życie ustawy 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 zawartego w dniu 23 marca 2020 r. 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, staje się listą, o której mowa w art. 13 ust. 1.

3. Postanowienia porozumienia, o którym mowa w ust. 1, ograniczające stosowanie porozumienia do stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej stają się bezskuteczne z dniem wejścia w życie ustawy.

Art. 34. 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 wymagań, 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 ulega może zostać jednostronnie rozwiązania przez podmiot publiczny a dostawcy poczty elektroniczne nie przysługują roszczenia z tego tytułu.

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 poczta elektroniczna już umożliwia stosowanie tych metod.

Art. 36. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
LEGISLACYJNYM I REDAKCYJNYM
Magdalena Witkowska-Krzymowska
Dyrektor Departamentu Regulacji Cyfrowych
Kancelarii Prezesa Rady Ministrów
/podpisano elektronicznie/

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[5]. 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 ono na nieuprawnionym posłużeniu się przez użytkownika (często przestępcę) wywołującego połączenie głosowe 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 poprzez 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. 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. Ustawa wdraża art. 97 ust. 2 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski

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

kodeks łączności elektronicznej, 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, ustawa odwołuje się do Prawa Telekomunikacyjnego, 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, 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

Art. 2 zawiera słowniczek ustawowy. Wskazano w nim 18 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. 2022 r. poz.

1863). 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, 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 i identyfikator użytkownika wysyłającego komunikat. Identyfikatorem mogą być znaki identyfikujące abonenta (z art. 130 Prawa telekomunikacyjnego 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 (Dz. U. 2022 r. poz. 1648). 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 poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację. Takie rozwiązanie zapewnia spójność systemu prawnego.

Kluczową definicją jest także definicja nadużycia w komunikacji elektronicznej. Wpierw opisano czynność będącą nadużyciem. Jest to świadczenie lub korzystanie z usługi telekomunikacyjnej[6] lub korzystanie z urządzeń telekomunikacyjnych[7] niezgodnie z ich 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

[6] Jest to usługa polegająca głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej.
[7] Urządzeniem telekomunikacyjnym jest urządzenie elektryczne lub elektroniczne przeznaczone do zapewniania telekomunikacji.

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 – 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[8]), POP3 (Post Office Protocol[9]), lub IMAP4 (Internet Message Access Protocol) lub innego zapewniającego analogiczna 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 (Dz. U. 2020 r. poz. 344).

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

---

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

[9] 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, poprzez 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 Prawa telekomunikacyjnego 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. sztuczny ruch – 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, 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 modyfikacja 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.

Ad 1 Sztuczny ruch

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 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. Połączenia te często są kierowane na numery o podwyższonej opłacie, należące do osób współpracujących z oszustem. W tej sytuacji tracą przedsiębiorcy telekomunikacyjni, którzy w ramach rozliczeń międzyoperatorskich płacą stawki za zakańczanie połączeń w sieciach stacjonarnych (FTR) oraz mobilnych (MTR). Zjawisko to również negatywnie wpływa na użytkowników końcowych – wskutek działań oszustów zmniejsza się przepustowość sieci telekomunikacyjnych. Z tych powodów zasadne jest wyodrębnienie tego nadużycia.

Ad 2 Smishing

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[10]. 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 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[11].

Opisane wyżej scenariusze nie są jedynymi możliwymi. Oszuści mogą podszywać się pod banki[12], firmy kurierskie[13]. 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.

---

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

[11] 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.

[12] https://cert.pl/posts/2022/04/banki-phishing/.

[13] https://cert.pl/posts/2022/04/flubot-smishing/.

Ad 3 CLI spoofing

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[14] - 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[15], nakłonić do instalacji oprogramowania, które pozwoli na zdobycie danych logowania do bankowości elektronicznej[16] 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[17].

Zjawisko to wywołuje powszechne oburzenie. Wśród społeczeństwa powoduje osłabienie zaufania do usług telekomunikacyjnych. Podmioty, pod które oszuści podszyli się, w niezawiniony przez siebie sposób tracą na wiarygodności. Wizerunkowo tracą również przedsiębiorcy telekomunikacyjni – *CLI spoofing* dokonuje się za pomocą

---

[14] 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.

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

[16] 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.

[17] 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 .

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).

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 poprzez CLI spoofing. Będzie to wywołanie strachu, poczucia zagrożenia lub nakłonienie odbiorcy połączenia do określonego zachowania, zwłaszcza przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania

Nazwa CLI spoofing pochodzi od skrótu *CLI* (*calling line identification*) oraz wyrazu *spoofing*[18].

Ad 4 Nieuprawniona zmiana informacji adresowej

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*

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

połączeń dla właściwego kierowania połączeń[19]. 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 Prawa telekomunikacyjnego, ustalenie sprawcy np. fałszywych alarmów bombowych.

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.

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[20]. 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

---

[19] Dz.U. z 2015 r. poz. 12.

[20] Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" Dz.U. z 2016 r. poz. 283.

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)[21]. 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 technicznych i organizacyjnych. 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 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

Celem zapobiegania oraz zwalczania smishingu proponuje się wprowadzenie zautomatyzowanego blokowania, przez przedsiębiorców telekomunikacyjnych, krótkich wiadomości tekstowych SMS, zawierające 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 SMSa.

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

CSIRT NASK będzie monitorował występowanie zjawiska smishingu na podstawie danych przekazanych mu przez podmioty trzecie – odbiorców SMS czy np. samych przedsiębiorców telekomunikacyjnych. Będzie to się odbywało dokładnie w taki sam sposób jak to się dzieje obecnie – poprzez przekazanie SMS na specjalny numer[22] albo poprzez formularz na stronie internetowej[23]. 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 w celu monitorowania smishingu.

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 ustawy o krajowym systemie cyberbezpieczeństwa do zadań CSIRT NASK należy m. in. monitorowanie zagrożeń cyberbezpieczeństwa na poziomie krajowym. Art. 39 ust. 1 uprawnia CSIRT NASK do przetwarzania danych pozyskanych w związku z zagrożeniami cyberbezpieczeństwa, w tym dane osobowe, w zakresie i w celu niezbędnym do realizacji zadań określonych m. in. w art. 26 ustawy o krajowym systemie cyberbezpieczeństwa. Z tego powodu, aby zapewnić spójność projektowanych przepisów, dodano przepis, zgodnie z którym CSIRT NASK będzie przetwarzał dane pozyskane w związku z monitorowaniem występowania smishingu na zasadach określonych w art. 39 ustawy o krajowym systemie cyberbezpieczeństwa.

Po przeanalizowaniu zgłoszeń wiadomości zawierających smishing CSIRT NASK tworzyłby wzorzec wiadomości wyczerpującej znamiona smishingu. Wzorzec 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.

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.

---

[22] https://www.nask.pl/pl/aktualnosci/4183,Teraz-jeszcze-latwiej-zglosic-incydent-bezpieczenstwa-przez-SMS.html.

[23] https://incydent.cert.pl/#!/lang=pl,entityType=notObligatedEntity,easyIncidentType=email.

Z jednej strony przepis ten zapewnia jawność działania państwa w zakresie zwalczania smishingu. Z drugiej zaś nie jest celowe publikowanie od razu wzorców, 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. Może być też tak, że nie jest celowe dalsze blokowanie takich wiadomości. Może się tak wydarzyć np. jeżeli:

- pomimo przekazania wzorca smishing dociera do użytkowników i wzorzec musi być poprawiony,
- wzorzec jest zbyt szeroki i blokuje także SMS nie mające 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.

Do systemu teleinformatycznego CSIRT NASK będą również podłączeni:

- Komendant 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,
- Prezes Urzędu Komunikacji Elektronicznej – z uwagi na jego zadania przy procedurze sprzeciwu wobec zablokowania krótkiej wiadomości tekstowej.

Komendant Centralnego Biura Zwalczania Cyberprzestępczości , Prezes UKE i przedsiębiorcy telekomunikacyjny 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.

Wprowadza się również przepis wskazujący CSIRT NASK jako odpowiedzialny za funkcjonowanie systemu teleinformatycznego służącego wymianie wzorców. Ponadto CSIRT NASK będzie administratorem danych przetwarzanych w tym systemie. Przepisy te jasno określą kto jest odpowiedzialny za system i przetwarzane w nim dane.

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. Przepis ten umożliwi każdemu kwestionowanie wzorca.

Sprzeciw będzie zawierał:

1. dokładną treść krótkiej wiadomości tekstowej (SMS) zablokowanej za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (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 jednoznacznie identyfikujące nadawcę, w szczególności:
    a. imię i nazwisko, adres zamieszkania - w przypadku osób fizycznych,
    b. nazwę podmiotu, adres, numer z właściwego rejestru - w przypadku osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej.

Informacje te będą niezbędne Prezesowi 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 do Prezesa UKE 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 sprzeciwu.

Sprzeciw niespełniający powyższych wymagań Prezes UKE pozostawi bez rozpoznania.

Art. 7

Przepis zawiera obowiązki Prezesa UKE oraz CSIRT NASK związane z procedurą sprzeciwu dla nadawcy krótkiej wiadomości tekstowej SMS, która została zablokowana. Prezes UKE będzie obowiązany rozpatrzyć sprzeciw w terminie 14 dni od dnia jego 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 2020 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) 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.

Art. 8

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 końcowy będzie mógł skorzystać z procedury reklamacyjnej, jeżeli uzna, że krótka wiadomość tekstowa została niesłusznie zablokowana.

Blokowanie SMS na podstawie projektowanego przepisu ma umożliwić przedsiębiorcom telekomunikacyjnym ochronę adresatów, konsumentów, przed złośliwymi SMSami, które przedsiębiorca telekomunikacyjny wykrył wcześniej, niż CSIRT NASK przygotował wzorzec wiadomości o charakterze smishingu. Przepis ten, wspólnie z art. 4 i 5, realizuje rekomendacje Międzynarodowego Związku Telekomunikacyjnego (ITU), zgodnie z którymi dostawcy usług telefonii komórkowych powinni zapewnić system przeciwdziałania atakom typu smishing[24].

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.

Przepis ustępu drugiego 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

---

[24] 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.

wiadomości MMS, z uwagi na ich charakter (mogą to być 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[25].

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

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

rzeczywiście ktoś dzwoni do niego m.in. z urzędu lub z banku. Oszuści uzyskują wtedy zaufanie ofiary i są w stanie nakłonić do niekorzystnego dla niej działania[26].

Dlatego przepis art. 9 zawiera obowiązek dla Prezesa Urzędu Komunikacji Elektronicznej 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. Wykaz będzie prowadzony w systemie teleinformatycznym Prezesa UKE i udostępniany na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu 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, jak również w przypadku numerów telefonów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii. Wnoszony będzie do Prezesa UKE 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.

Wniosek będzie zawierał wskazanie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych. 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. Wpis do wykazu będzie miał charakter czynności materialno-technicznej. Dokonany będzie w terminie 5 dni od dnia otrzymania wniosku. Prezes UKE będzie mógł pozostawić wniosek bez rozpoznania, jeżeli wniosek

[26] 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.

zostanie złożony przez podmiot nieuprawniony albo wniosek będzie dotyczył numeru niewykorzystywanego przez wnioskodawcę. W takim przypadku wnioskodawca zostanie niezwłocznie poinformowany o pozostawieniu wniosku bez rozpoznania. Wprowadza się również możliwość wycofania wniosku przez podmiot, który go złożył.

Art. 11

W art. 11 określono, że Prezes UKE prowadzi wykaz numerów, które służą wyłącznie do odbierania połączeń głosowych przy pomocy systemu teleinformatycznego. Wykaz zawiera:

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

Wykaz, o którym mowa w art. 10, będzie prowadzony w systemie teleinformatycznym. Dzięki temu przedsiębiorcy telekomunikacyjni będą mieli dogodny dostęp do tego wykazu i będą mogli efektywnie wykorzystać go przy zwalczaniu nadużyć w komunikacji elektronicznej. 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 ustęp 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 Międzynarodowy Związku

Telekomunikacyjnego[27], które dzielą na funkcje wykrywania, monitorowania, mitygacji oszustw oraz wymianie informacji o nadużyciach telekomunikacyjnych. Zrezygnowano przy 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 ustępu pierwszego wprowadza ogólne wymagania co do środków technicznych i organizacyjnych stosowanych przez przedsiębiorców telekomunikacyjnych przy zwalczaniu CLI spoofing. Szczegółowe środki mogą się zmieniać w toku postępu technologicznego. Dlatego 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 poprzez zawarcie tego porozumienia oraz jego prawidłowe wykonywanie operatorzy spełnią obowiązek podejmowania proporcjonalnych działań mających na celu zapobieganie CLI spoofing. Proponowane rozwiązanie ma na celu ułatwienie operatorom telekomunikacyjnym 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.

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 Prawa telekomunikacyjnego.

Dzięki takiemu rozwiązaniu najwięksi operatorzy telekomunikacyjni, przy wsparciu i nadzorze UKE, będą mogli wypracować najlepsze rozwiązania techniczne i organizacyjne, które pozwolą im zwalczać nadużycia w komunikacji elektronicznej. Zwolnienie z

---

[27] 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.

odpowiedzialności w przypadku prawidłowego wykonywania porozumienia będzie stanowiło silny bodziec do dołączenia do porozumienia.

Dla mniejszych operatorów telekomunikacyjnych, którzy mogliby nie być w stanie wypełnić obowiązków, które będą określone w porozumieniu, Prezes UKE będzie wydawał rekomendacje. Prawidłowe wykonywanie rekomendacji Prezesa UKE będzie wyłączało odpowiedzialność tych operatorów za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej.

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 w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu. Obecnie funkcjonuje podobne porozumienie, 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.

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

Z reguły oszust tworzy podobną 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 poprzez pocztę elektroniczną, krótkie wiadomości tekstowe SMS czy inne środki komunikacji elektronicznej[28].

Jako przykład można wskazać domeny internetowe podszywające się pod Pocztę Polską – są podobne wizualnie i stosują podobny adres[29]. Takie fałszywe strony mogą zachęcać do logowania, przelania rzekomej dodatkowej opłaty za dostarczenie paczki czy listu, czy przekazania danych celem uzyskania zysków z rzekomej inwestycji[30]. 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 poprzez fałszywą stronę jak i dostawcy internetu.

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.

Wprowadza się przepis zgodnie z którym każdy będzie mógł zgłosić do CSIRT NASK domenę internetową mogącą służyć do wyłudzeń danych i środków finansowych. Wymagane będzie przy tym uzasadnienie. CSIRT NASK będzie mógł wpisać domenę na listę ostrzeżeń po zweryfikowaniu, że rzeczywiście ma ona na celu wyłudzenia ich danych lub niekorzystnego rozporządzenia środkami finansowymi[31]. Ogólna redakcja przepisu pozwala CSIRT NASK na wpisanie domeny po otrzymaniu zgłoszenia, ale również samodzielnie. Sposób dokonywania

---

[28] 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

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

[30] 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.

[31] Weryfikacja może polegać m. in. na analizie adresu URL podejrzanej strony, jej wyglądu, zawartej treści czy kodu źródłowego. Por. wspomniane wyżej *Recommendation X.1235 (01/22) : Technologies in countering website spoofing for telecommunication organizations* str. 7

zgłoszeń zostanie określony przez CSIRT NASK i opublikowany w BIP NASK-PIB, dzięki czemu każdy będzie mógł się z tym zapoznać.

Jednocześnie zgodnie z ust. 4 pkt. 1 CSIRT NASK będzie odpowiedzialny za prowadzenie jawnej listy ostrzeżeń dotyczącej niebezpiecznych domen internetowych.

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 poprzez usunięcie 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 środków finansowych. Użytkownik internetu uzyska wtedy informację 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[32] 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.

Sprzeciw będzie zawierał:

---

[32] Jedna z projektowanej ustawy, a druga to funkcjonujący na podstawie art. 15f ustawy z 19 listopada 2009 r. *o grach hazardowych* (Dz.U. z 2022 r. poz. 888, z późn. zm.) Rejestr domen służących do oferowania gier hazardowych niezgodnie z ustawą.

1) wskazanie domeny internetowej, której dotyczy,
2) uzasadnienie wyjaśniające, dlaczego wpisanie domeny na listę ostrzeżeń było niezasadne oraz
3) dane jednoznacznie identyfikujące podmiot składający sprzeciw.

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 do Prezesa UKE 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 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 tego Prezes UKE będzie dokonywał oceny, czy dana domena internetowa rzeczywiście służy do wyłudzeń danych i środków finansowych użytkowników internetu. W przypadku gdyby okazało się, że nie, 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.

Art. 16

W artykule tym uregulowana została kwestia ochrony użytkowników końcowych przed nadużyciami z wykorzystaniem sieci telekomunikacyjnej poprzez określenie warunków dla zablokowania dostępu do numeru lub usługi, wstrzymania pobierania opłat za połączenia, zaprzestania świadczenia usługi oraz usunięcia informacji promujących numer lub usługę z dodatkowym świadczeniem. Powyższe obowiązki nakładane są w drodze decyzji Prezesa

UKE, której nadaje się rygor natychmiastowej wykonalności. Przedsiębiorca komunikacji elektronicznej ma obowiązek, zgodnie z decyzją, zablokować dostęp do numeru lub usługi. Podobnie podmiot realizujący dodatkowe świadczenie jest zobowiązany zaprzestać świadczenia usługi. W swojej decyzji Prezes UKE określa termin na zablokowanie dostępu do numeru lub usługi lub zaprzestanie świadczenia usługi nie krótszy niż 6 godzin od momentu doręczenia decyzji. Decyzja w powyższym zakresie może być ogłoszona ustnie przedsiębiorcy komunikacji elektronicznej lub podmiotowi realizującemu dodatkowe świadczenie. 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

68,3% Polaków w przedziale wiekowym 16-74 lata korzysta z poczty elektronicznej[33]. Oprócz korzyści z tego środka komunikacji elektronicznej, na użytkowników poczty czyhają również zagrożenia. Protokół SMTP, używany do wysyłania poczty elektronicznej, pierwotnie nie zakładał możliwości uwierzytelnienia wysyłanych wiadomości. W konsekwencji możliwa jest 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[34].

Mechanizm SPF - Sender Policy Framework[35] 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

---

[33] 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.

[34] 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.

[35] 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.

danej domeny. Serwer pocztowy odbiorcy, odbierając wiadomość, sprawdza, czy adres IP lub 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 mechanizm uwierzytelniania jest DKIM - DomainKeys Identified Mail[36]. 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 klucza prywatnego, którym została podpisana do otrzymana wiadomość, oznacza to jej nieuprawnioną modyfikację[37].

Mechanizm DMARC - *Domain-based Message Authentication Reporting and Conformance*[38] 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[39].

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[40].

---

[36] 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.

[37] Stephen J. Nightingale, *op. cit.*, str. 6-7.

[38] 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.

[39] Stephen J. Nightingale, *op. cit.*, str. 7.

[40] https://www.cisa.gov/sites/default/files/bod-18-01.pdf.

Ponadto brytyjskie[41], australijskie[42] oraz duńskie[43] służby odpowiedzialne za cyberbezpieczeństwo zalecają stosowanie tych mechanizmów.

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

- co najmniej 500 000 użytkowników,
- podmiotów publicznych

obowiązku stosowania mechanizmów SPF, DKIM oraz DMARC (ust. 1).

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 Urzędu Komunikacji Elektronicznej. Kontrola będzie prowadzona zgodnie z przepisami rozdziału 2 działu X Prawa telekomunikacyjnego (ust. 3).

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

[41] https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/configure-anti-spoofing-controls- .
[42] https://www.cyber.gov.au/acsc/view-all-content/publications/how-combat-fake-emails.
[43] https://www.cfcs.dk/da/nyheder/2017/vejledning-dmarc-kan-reducere-antallet-af-falske-mails/.

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 udzielenie 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. 5). 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 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

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.

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.

W tym miejscu należy podkreślić, że 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. 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 SMSa 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 ustawie, 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 wymienione zostały informacje, do przetwarzania których przedsiębiorca telekomunikacyjny jest uprawniony wraz ze wskazaniem celu przetwarzania oraz okresu, do kiedy przetwarzanie danych jest dopuszczalne – jako moment graniczny wskazując koniec terminu, w którym możliwe jest dochodzenie roszczeń. Ust. 4 projektowanego przepisu zawiera wyłączenie stosowania art. 15 rozporządzenia 2016/679 w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.

Przepis ten jest bezpośrednio powiązany z ust. 3 dotyczącym możliwości wymiany informacji pomiędzy przedsiębiorcami i bazuje na podobnych rozwiązaniach z rynku bankowego (art. 106e ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2020 r. poz. 1896)) oraz ubezpieczeń (art. 35a ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2020 r. poz. 895)), które to rozwiązania zostały wprowadzone w ramach tzw. ustawy wdrażającej rozporządzenie 2016/679. Proponowany ustęp wyłącza stosowanie 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.), zwanego dalej „rozporządzeniem 2016/679”.

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 telekomunikacyjne stanowią z perspektywy prawa karnego przestępstwa, z tego względu proponowane wyłączenie jest zgodne z art. 23 ust. 1 lit. d i 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. 15. Zgodnie z tym przepisem akt prawny, który ma wprowadzać ograniczenia w przepisach dotyczących zakresu praw i obowiązków, w tym art. 15 rozporządzenia, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o: celach przetwarzania lub kategorii przetwarzania, kategoriach danych osobowych, zakresie wprowadzonych ograniczeń, zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, określeniu administratora lub kategorii administratorów, okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania, ryzykach naruszenia praw lub wolności osoby, której dane dotyczą, oraz prawie 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 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 celem wykrywania i zwalczania nadużyć, przedsiębiorcy telekomunikacyjni będą przetwarzać dane objęte tajemnicą telekomunikacyjną (których katalog znajduje się w 159 ustawy 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, celem identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. Ust. 4 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 - 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 art. 174^1 ustawy Prawo telekomunikacyjne, zgodnie z którym dostawca usług komunikacji elektronicznej obowiązany jest wdrożyć odpowiednie techniczne i organizacyjne 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 Prawo telekomunikacyjne, a dodatkowo z regulacji art. 18 i 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. 4 wynika zakres i cel ograniczenia prawa do informacji. Ponadto, 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 również naruszać cel tego ograniczenia.

Art. 14 rozporządzenia 2016/679 zawiera katalog informacji podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą. Podczas działań mających na celu zwalczanie i zapobieganie nadużyć w komunikacji elektronicznej przedsiębiorca telekomunikacyjny może pozyskać wiele tego rodzaju danych osobowych. Poinformowanie każdej takiej osoby odrębnie może być niemożliwe do wykonania. Dlatego ust. 5 pozwala przedsiębiorcy telekomunikacyjnemu na podanie informacji wymaganych przez art. 14 rozporządzenia 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

Art. 20 zawiera przepisy związane z administracyjnymi karami pieniężnymi.

Nadużycia w komunikacji elektronicznej powodują szkody po stronie użytkowników końcowych oraz przedsiębiorców telekomunikacyjnych. Dlatego zakaz tych nadużyć, określony w art. 3 ust. 1 in principio 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)[44]. 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 Kodeksu karnego (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[45].

Fakultatywnej administracyjnej karze pieniężnej będą podlegali:

- przedsiębiorca telekomunikacyjny, który nie wypełnia obowiązków wskazanych w art. 5, art. 9 i art. 10 ust. 12 (ust. 3),
- dostawca poczty elektronicznej, który nie wypełnia obowiązków wskazanych w art. 17 ust. 1 (ust. 4),

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 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

[44] Przepis opracowano wzorując się na art. 92a ust. 9 ustawy z 6 września o transporcie drogowym Dz.U. z 2022 r. poz. 2201.

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

wyrządzonej szkody[46]. Charakter naruszenia należy rozumieć jako stopień zawinienia osoby podlegającej odpowiedzialności karnoadministracyjnej, tj. czy czyn został przez nią popełniony z winy umyślnej lub nieumyślnej[47]. 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 Prawa telekomunikacyjnego wprowadzono możliwość nałożenia kary na kierującego przedsiębiorstwem telekomunikacyjnym za nie wykonanie 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 wdrożenie mechanizmów uwierzytelniania poczty elektronicznej SPF/DKIM/DMARC przyczyniło się do wystąpienia incydentu w podmiocie publicznym w rozumieniu art. 2 pkt. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Można sobie wyobrazić sytuację, w której pomimo nałożenia kary na podmiot publiczny, obowiązek nadal nie jest wykonywany. Dlatego powinna być możliwość ukarania kierownika tego podmiotu, co powinno wywołać odpowiedni efekt prewencyjny.

Tak jak w przypadku Prawa telekomunikacyjnego od decyzji Prezesa UKE w sprawie nałożenia kar będzie przysługiwało odwołanie do Sądu Okręgowego w Warszawie - Sądu Ochrony Konkurencji i Konsumentów.

---

[46] 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.

[47] Ibidem, s. 70.

Art. 21

Przepisy artykułu 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 finansowe,
- sposób obliczenia przychodu podmiotu na potrzeby obliczenia wymiaru kary.

Przepisy te nawiązują do art. 210 ustawy – Prawo telekomunikacyjne.

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

Proponuje się, aby wpływy z tych kar stanowiły przychód Funduszu Cyberbezpieczeństwa o którym mowa w art. 1 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2021 r. poz. 2333, z późn. zm.). Z tego też powodu w art. 23 proponuje się odpowiednio zmianę ustawy poprzez uzupełnienie przepisów odnoszących się do przychodów tego Funduszu.

Ustępy 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 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, o którym mowa w 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

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 przestępstwa 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 Kodeksu karnego. Jednocześnie wprowadza się typ uprzywilejowany tego przestępstwa: w wypadku mniejszej wagi[48] – sprawca wtedy podlega grzywnie, karze ograniczenia wolności albo

[48] Za orzecznictwem wskazać należy, że wypadek przestępstwa mniejszej wagi zachodzi wówczas, gdy znamiona przestępstwa, przede wszystkim przedmiotowe, cechują się niewysoką społeczną szkodliwością, zaś jego

pozbawienia wolności do roku. Jeżeli nadużycia w komunikacji elektronicznej dokonano na szkodę osoby najbliższej[49], 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 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 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.

Art. 26

Przepis art. 26 nakłada na Prezesa UKE obowiązek przedstawienia sejmowej komisji właściwej w sprawach nowych technologii 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.

---

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.

[49] Zgodnie z art. 116 Kodeksu karnego 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.

Art. 27

Przepis art. 27 zmienia art. 192 Prawa telekomunikacyjnego, 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

Konsekwencją nałożenia na CSIRT NASK nowych zadań jest wprowadzenie zmian w art. 26 ust. 6 ustawy o krajowym systemie cyberbezpieczeństwa poprzez dodanie do katalogu zadań CSIRT NASK monitorowania występowania smishingu oraz tworzenie wzorca wiadomości wyczerpującej znamiona smishingu. Zmiana ta jest konieczna ze względu na rolę jaką będzie odgrywał CSIRT NASK w zwalczaniu nadużyć w komunikacji elektronicznej.

Art. 29

Przepis art. 29 wprowadza zmiany w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Zmiana polega na dodaniu do przychodów Funduszu Cyberbezpieczeństwa wpływów z kar pieniężnych nakładanych na podstawie art. 20 niniejszej ustawy.

Art. 30

W art. 30 określono trzymiesięczny termin, od dnia wejścia w życie ustawy, w jakim CSIRT NASK ma uruchomić system teleinformatyczny do udostępniania informacji o wzorcach wiadomości zawierających smishing oraz poinformować ministra właściwego do spraw informatyzacji o tym uruchomieniu Niezwłocznie po otrzymaniu informacji minister właściwy do spraw informatyzacji ma udostępnić na swojej stronie podmiotowej w BIP tę informację. 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.

Art. 31

Przepis ma charakter intertemporalny i przewiduje czas niezbędny dla przedsiębiorców telekomunikacyjnych do wdrożenia rozwiązań umożliwiających podejmowanie

proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej w postaci sztucznego ruchu, smishingu i CLI spoofingu, bez ryzyka nałożenia w tym czasie kary przez Prezesa UKE. Jest to rozwiązanie spójne z kolejnym przepisem.

Przepisy zakładają, że kary za niewykonanie obowiązku blokowania wiadomości będzie można nakładać 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 technicznych i organizacyjnych, które umożliwiają przeciwdziałanie odpowiednio smishingowi i spoofingowi. Wprowadzenie kar za okres poprzedzający wprowadzenie obowiązku byłoby sprzeczne z zasadą demokratycznego państwa prawnego.

Art. 32

Przepis art. 32 wprowadza termin dla przedsiębiorców telekomunikacyjnych na wdrożenie rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej.

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. 33

Jest to przepis dostosowujący, który uznaje *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[50] za porozumienie, o którym mowa w art. 12 ust. 1. Również lista ostrzeżeń[51] prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie ww. porozumienia powinna być prawnie uznana za listę, o której mowa w art. 12 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.

Art. 34

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. 30 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, czyli wdrożenia mechanizmów SPF/DKIM/DMARC. W przypadku niespełnienia tych wymagań w tym terminie umowa ulegnie rozwiązaniu.

Art. 35

Zgodnie z 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 poczta elektroniczna już umożliwia stosowanie tych metod.

Art. 36

Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia.

Pozostałe informacje

[50] https://www.uke.gov.pl/akt/uke-przystapil-do-porozumienia-chroniacego-abonentow,300.html.
[51] https://cert.pl/posts/2020/03/ostrzezenia_phishing/.

Projekt nie jest sprzeczny z prawem Unii Europejskiej.

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

Regulacje zawarte w projekcie nie będą miały bezpośredniego wpływu na funkcjonowanie przedsiębiorstw.

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).

Projekt nie podlega procedurze notyfikacji 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** **22.11.2022 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 2018 Nr 321, str. 36 **Nr w wykazie prac** 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[52]. 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 poprzez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu. Od kwietnia 2021 r. do początku czerwca 2022 r. zespół CSIRT NASK zidentyfikował 31 054 krótkich wiadomości tekstowych, mające znamiona smishingu.

W tej sytuacji konieczne jest wprowadzenia odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników.

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

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

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

Przedsiębiorcy telekomunikacyjnie będą obowiązani, w szczególności do:

1) podejmowania proporcjonalnych środków technicznych i organizacyjnych 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.

Prezes Urzędu Komunikacji Elektronicznej 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 poczty elektronicznej.
Na poziomie ustawowym zostanie umocowana lista ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu[53]. Przedsiębiorcy telekomunikacyjni (strony porozumienia) będą mogli blokować dostęp do tych domen internetowych użytkownikom internetu.
Projekt ustawy penalizuje nadużycia w komunikacji elektronicznej – tworzenie 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.

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 roku 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[54].

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

[53] https://cert.pl/posts/2020/03/ostrzezenia_phishing/.
[54] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-scam-calls-and-texts/do-not-originate.

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[55]. Zgodnie z danymi NCSC 14 tysięcy oszustw zostało usuniętych od lipca 2022 r. przy pomocy numeru 7726[56].

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[57].

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[58].

Belgia

W Belgii przyjęto nową ustawę o telekomunikacji, która wprowadza możliwość zastosowania przez operatorów telekomunikacyjnych algorytmów do identyfikowania oraz blokowania podejrzanych wiadomości SMS[59].

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 wyrządzenia 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. Paragraf 2 niniejszego 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

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

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

[57] 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/.

[58] 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.

[59] 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/.

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[60].

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 okres 4 miesięcy 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[61].

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[62].

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[63].

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

---

[60] 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.

[61] 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 .

[62] 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 .

[63] Tamże.

wymagać, aby w takich przypadkach dostawcy usług łączności elektronicznej potrącali przychody z tytułu połączeń wzajemnych[64].

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[65].

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[66].

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[67].

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[68].

Departament Bezpieczeństwa Narodowego USA nakazał także agencjom federalnym stosowanie mechanizmu uwierzytelniania poczty elektronicznej DMARC[69].

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).

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 pochodzącego z tak zwanych „nieprawidłowych numerów" (00-000-0000 lub 111-111-1111 lub te, które przekraczają 15 cyfr)[70].

4. Podmioty, na które oddziałuje projekt			
Grupa	Wielkość	Źródło danych	Oddziaływanie

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

[65] https://www.33700.fr/identifier-et-signaler-un-spam-sms/. .https://www.33700.fr/identifier-et-signaler-un-spam-vocal/.

[66] https://www.fcc.gov/document/mandating-stirshaken-combat-spoofed-robocalls-0.

[67] https://www.fcc.gov/spoofing.

[68] Tamże.

[69] https://www.cisa.gov/sites/default/files/bod-18-01.pdf.

[70] 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/.

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[71]	dane UKNF[72]	Banki będą uprawnione do złożenia wniosku o wpis numeru przez nie wykorzystywane do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Dostawcy poczty elektronicznej	brak danych[73]		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[74]	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[75]	Fundusze inwestycyjne będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
Instytucje płatnicza	40	Dane UKNF[76]	Instytucje płatnicze będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.
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

[71] 30 banków komercyjnych, 1 bank państwowy, 511 banków spółdzielczych.
[72] 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".
[73] 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.
[74] https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_upreg#.
[75] Sprawozdanie KNF 2021 str. 25.
[76] Sprawozdanie KNF 2021 str. 24.

			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[77]	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 • 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 stosowanych przy przeciwdziałania CLI spoofing.

[77] Sprawozdanie KNF 2021, str. 26.

Przedsiębiorcy telekomunikacyjni	3953	Rejestr przedsiębiorców telekomunikacyjnych[78]	Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane z 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[79]	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 nie wykonanie 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. NSA będzie rozpatrywał ewentualne skargi kasacyjne.
Spółdzielcze kasy oszczędnościowo-kredytowe	23	Dane UKNF[80]	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[81]	Towarzystwa funduszy inwestycyjnych będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów

[78] Stan na dzień 31.10.2022 r.

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

[80] 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.

[81] 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.

			służących wyłącznie do odbierania połączeń głosowych.
Użytkownicy internetu w Polsce	29,7 mln	Badania Mediapanel za październik 2022[82]	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[83]	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[84]	Zmniejszenie ryzyka zetknięcia się z CLI spoofing oraz smishingiem.
Zakład reasekuracji	1	Dane UKNF[85]	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[86]	Zakłady ubezpieczeń będą uprawnione do złożenia wniosku o wpis swojego numeru do wykazu numerów służących wyłącznie do odbierania połączeń głosowych.

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

W ramach 14 – dniowych konsultacji i opiniowania projekt został skierowany do zaopiniowania przez:

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;
34) Polska Organizacja Handlu i Dystrybucji;
35) Polska Organizacja Niebankowych Instytuc Płatności;
36) Polska Rada Biznesu;
37) Polska Wytwórnia Papierów Wartościowyc
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;

[82] https://www.gemius.pl/reklamodawcy-aktualnosci/wyniki-badania-mediapanel-za-pazdziernik-2022.html.
[83] https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/maly-rocznik-statystyczny-polski-2022,1,24.html.
[84] 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.
[85] Sprawozdanie KNF 2021 str. 122.

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;
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) Prezesa Urzędu Komunikacji Elektronicznej;
60) Prezesa Urzędu Ochrony Danych Osobowych;
61) Prezesa 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	*Łączn ie (0-10)*
Dochody ogółem												
budżet państwa												
JST												

pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
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	Niemożliwe jest oszacowanie wielkości przychodów Funduszu Cyberbezpieczeństwa o wpływy z kar pieniężnych nakładanych przez Prezesa Urzędu Komunikacji Elektronicznej (zwany dalej „Prezesem UKE) z powodu niewykonania obowiązków wynikających z projektowanych przepisów. Do postępowania w sprawie nałożenia tych kar pieniężnych będą stosowane przepisy *Działu IVA. Administracyjne kary pieniężne* Kodeksu postępowania administracyjnego[87], które to przepisy pozwalają w niektórych sytuacjach na odstąpienie od nałożenia kary pieniężnej. Ponadto konstrukcja przepisów zakłada, że kary będą miały charakter fakultatywny. Z tych powodów każdy szacunek tych wpływów będzie obarczony dużym prawdopodobieństwem błędu i może się nie sprawdzić.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł,	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							

[87] Ustawa z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego Dz.U. z 2022 r. poz. 2000.

ceny stałe z …… r.)	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa sektor mikro-, małych i średnich przedsiębiorstw	**Przedsiębiorcy telekomunikacyjni** Przedsiębiorcy telekomunikacyjni będą obowiązani do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczaniu. Celem dostosowania do projektu ustawy przedsiębiorcy będą musieli • zapoznać się z ustawą, • 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. Konsekwencją dostosowania się do obowiązków wynikających z projektu ustawy może być konieczność zmiany regulaminów świadczenia usług telekomunikacyjnych. Wykonywanie obowiązków z niniejszego projektu ustawy przez przedsiębiorców telekomunikacyjnych zwiększy bezpieczeństwo usług komunikacji elektronicznej. Przełoży się to na zwiększenie zaufania 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[88]; ponadto istnieje wiele poradników						

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

		jak poprawnie skonfigurować te mechanizmy[89]. 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 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.
	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 wyczerpujących znamiona smishingu, inne niż zawarte we wzorcu wiadomości przekazanym przez CSIRT NASK, użytkownik końcowy będzie mógł dochodzić swoich praw poprzez 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 wdrożenie mechanizmów uwierzytelniania poczty elektronicznej SPF/DKIM/DMARC przyczyniło się do wystąpienia incydentu w podmiocie publicznym w rozumieniu art. 2 pkt. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
Niemierzalne		

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

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 popularne i obecnie ich ofiarami stają się tysiące ludzi. Jak zostało wskazane w raporcie CSIRT NASK za 2021 r. cały czas rośnie liczba tego typu ataków[90]. Sam raport opisuje również całą serię różnego rodzaju ataków z wykorzystaniem smsów. Ten trend jest widoczny na całym świecie. Tego typu ataki mają bardzo poważne konsekwencje i często mogą prowadzić do sytuacji w której ludzie tracą dostęp do swoich kont bankowych, nierzadko tracąc oszczędności całego życia. W związku z tym, ustawa ta ma zaadresować bardzo poważny problem społeczny i ochronić kluczowe interesy obywateli. Ograniczenie rozmiarów tego zjawiska jest niemożliwe bez przetwarzania komunikatów 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.	

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 wprowadza następujące obowiązki na przedsiębiorców telekomunikacyjnych:

1. podejmowania proporcjonalnych środków technicznych i organizacyjnych 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;
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.

Prezes Urzędu Komunikacji Elektronicznej będzie

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

- 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 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 nowych technologii,
- kontrolował przedsiębiorców telekomunikacyjnych, dostawców poczty elektronicznej, podmioty publiczne w zakresie wykonywania obowiązków wynikających z ustawy;
- nakładał administracyjne kary pieniężne za niewykonywania 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 techniczne i organizacyjne 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.

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

Ewaluacja efektów projektu nastąpi po roku od momentu wejścia w życie ustawy. 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 ich sposobie załatwienia,
4. Liczba wydanych decyzji nakazujących przedsiębiorcy telekomunikacyjnemu zablokowanie dostępu do numeru lub usługi oraz nakładającą 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 postępowań karnych wszczętych w sprawach przestępstw związanych z nadużyciami w komunikacji elektronicznej.

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

Brak