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 osiągnięcie nienależnych korzyści.

W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych[[1]](#footnote-1). Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć. Oszuści wykorzystywali w ten sposób słabości sieci telekomunikacyjnych, które powodują, że operatorzy sieci mobilnych często nie są w stanie zweryfikować, czy połączenie w ramach którego jest prezentowany numer faktycznie pochodzi z karty SIM, która jest zarejestrowana dla danego numeru. Zjawisko to występuje pod nazwą CLI spoofing.

Innym zagrożeniem dla użytkowników są fałszywe krótkie wiadomości tekstowe SMS. Oszuści podszywając się pod zaufane instytucje próbują nakłonić nieświadome ofiary do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie poprzez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu.

W tej sytuacji konieczne jest wprowadzenia odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników. Kwestia zwalczania nadużyć nie jest regulowana w Europejskim Kodeksie Łączności Elektronicznej oraz nie była dotychczas regulowana w ustawie - Prawo telekomunikacyjne.

Uzasadnienie poszczególnych przepisów materialnych

Art. 1

Przepis art. 1 ustawy określa zakres przedmiotowy ustawy. Przede wszystkim nowe przepisy zawierają prawa i obowiązki przedsiębiorców telekomunikacyjnych związane z zapobieganiem oraz 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 16 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. 2020 r. poz. 1369, z późn. zm.). 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.

Kolejną istotną definicją jest definicja komunikatu elektronicznego. Zgodnie z projektowaną definicją komunikatem elektronicznym jest każda informacja wymieniana lub przekazywana między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej; nie obejmuje on informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację. Definicja ta w zasadniczej mierze powtarza treść definicji komunikatu zawartej w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. 2021 r. poz. 576, z późn. zm.). Rozszerza przy tym to pojęcie o informacje przekazywane za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej, a nie jak dotychczas jedynie publicznie dostępnych usług telekomunikacyjnych.

Kluczową definicją jest także definicja nadużycia w komunikacji elektronicznej. Jest to świadczenie lub korzystanie z usługi telekomunikacyjnej lub urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, którego celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści.

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 podmiotu publicznego odwołuje się z kolei do zbioru podmiotów wskazanych w art. 7–art. 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.

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), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol).

Przy definicji usługi komunikacji interpersonalnej niewykorzystującej numerów wskazano, że jest to usługa, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji oraz umożliwia 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.

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 trzy szczególne (podstawowe) formy nadużyć w komunikacji elektronicznej. Są to:

1. sztuczny ruch – jest to inicjowanie wysyłania lub odbieranie komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe;
2. Smishing – jest to wysyłanie krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę www, żądania kontaktu telefonicznego lub instalacji oprogramowania;
3. CLI spoofing – jest to nieuprawnione posłużenie się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania. Jako przykład CLI spoofing można wskazać nieuprawnione wykorzystywanie numeracji jako informacji adresowej w postaci numeru telefonu lub identyfikatora użytkownika inicjującego połączenie, do wykorzystywania której podmiot nie ma uprawnień.

Użycie w projekcie wyrażeń obcojęzycznych jest uzasadnione, ponieważ nie mają one dokładnego odpowiednika w języku polskim.

Ustęp drugi 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, gdyż wśród przedsiębiorców telekomunikacyjnych znajdują się zarówno duzi przedsiębiorcy dostarczający sieci mobilne, jak i mali i średni przedsiębiorcy. Działania podejmowane przez te podmioty będą więc zależne od wielkości podmiotu, posiadanej infrastruktury czy charakteru świadczonych usług. Przykładowo jako jeden ze środków można wskazać monitorowanie usług telekomunikacyjnych w celu wykrywania przypadków CLI spoofingu.

Art. 4

Projekt zakłada, aby monitorowaniem występowania smishingu zajmował się zespół CSIRT NASK. Po wykryciu smishingu zespół ten informowałby, za pomocą systemu teleinformatycznego, przedsiębiorców telekomunikacyjnych o takim nadużyciu. W systemie przekazywany byłby wzór wiadomości smishingowej. Przedsiębiorca po otrzymaniu takiej informacji blokowałby SMS zgodne ze wzorem przekazanym przez CSIRT NASK. Jednocześnie projektodawca przewidział sytuację, gdy wiadomość uznana za smishing jednak nim nie jest (tzw. *false positive*). Może być też tak, że nie jest celowe dalsze blokowanie takich wiadomości. W tej sytuacji CSIRT NASK poinformuje o *false positive*, a przedsiębiorca przestanie blokować takie wiadomości.

Do systemu teleinformatycznego, przekazującego wzorce wiadomości smishingowej będą również podłączeni:

* Komendant Główny Policji – 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 jego zadania przy ww. procedurze odwoławczej.

Art. 5

Projekt przewiduje procedurę odwoławczą dla nadawcy wiadomości uznanej za wyczerpującą znamiona nadużycia w komunikacji elektronicznej. Nadawca będzie mógł zgłosić sprzeciw do Prezesa UKE. Prezes UKE będzie obowiązany rozpatrzyć sprzeciw co do zasady w terminie 14 dni od dnia jego otrzymania.

Art. 6

Przepis zawiera obowiązki Prezesa UKE oraz CSIRT związane z procedurą odwoławczą dla nadawcy wiadomości uznanej za wyczerpującą znamiona nadużycia w komunikacji elektronicznej.

Art. 7

Art. 7 dotyczy sytuacji, w której przedsiębiorca zidentyfikował 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 identyfikację takich wiadomości.

Art. 8

Przepis nakłada obowiązek na przedsiębiorcę telekomunikacyjnego zablokowania połączenia głosowego albo ukrycia identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia CLI spoofing. 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.

Art. 9

Niektórzy oszuści podszywają się pod jednostki sektora finansów publicznych czy innych 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 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.

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.

Wniosek o wpis do wykazu numeru będzie mógł być złożony przez jednostki sektora finansów publicznych, banki, jak również w przypadku numerów telefonów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii. 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 odmówić wpisu, jeżeli wniosek zostanie złożony przez podmiot nieuprawniony. Odmowa nastąpi w drodze decyzji. Wprowadza się również możliwość wycofania wniosku przez podmiot, który go złożył.

Co najważniejsze, skutek wpisu numeru do wykazu aktualizuje obowiązek po stronie przedsiębiorcy telekomunikacyjnego świadczący usługę połączeń głosowych do blokowania połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu.

Art. 10

Wprowadza możliwość zawarcia przez operatorów telekomunikacyjnych porozumienia z Prezesem UKE, w którym będą określone 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 ułatwić operatorom telekomunikacyjnym skuteczne wykonywanie tych obowiązków oraz 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.

Art. 11

Przepis art. 11 konstytuuje możliwość zawarcia przez: Prezesa Urzędu Komunikacji Elektronicznej, ministra właściwego do spraw informatyzacji, Naukową i Akademicką Sieć Komputerowa – Państwowy Instytut Badawczy, oraz 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. Zasadne jest umożliwienie, aby również poza okresami stanów nadzwyczajnych czy tymi związanymi zepidemią mogło obowiązywać podobne porozumienie.

Art. 12

Proponuje nałożenie na dostawców poczty elektronicznej:

* dla co najmniej 500 000 użytkowników,
* obsługujących 500 000 aktywnych kont pocztowych
* dla podmiotów publicznych

dodatkowych obowiązków z zakresu bezpieczeństwa poczty elektronicznej.

Dostawcy ci będą mieli obowiązek stosować jeden z poniższych mechanizmów uwierzytelnienia poczty elektronicznej:

* DMARC - Domain-based Message Authentication Reporting and Conformance[[2]](#footnote-2),
* DKIM - DomainKeys Identified Mail[[3]](#footnote-3) oraz
* SPF - Sender Policy Framework[[4]](#footnote-4).

Ponadto na podmiot publiczny zostanie nałożony obowiązek korzystania z poczty elektronicznej wykorzystującej jeden z powyższych mechanizmów.

Kontrolę realizacji ww. obowiązków przez dostawców poczty elektronicznej jak i podmiotów publicznych będzie sprawować Prezes Urzędu Komunikacji Elektronicznej.

Art. 13

Art. 13 nakłada na przedsiębiorców telekomunikacyjnych obowiązek rejestracji danych o niewykonanych usługach w związku z blokowaniem krótkich wiadomości tekstowych, wskazując jednocześnie przez jaki okres dane mają być przechowywane, w szczególności na potrzeby postępowania reklamacyjnego.

Art. 14

W art. 14 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. W ust. 2 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. 3 projektowanego przepisu zawiera wyłączenie stosowania art. 14 i 15 rozporządzenia 2016/679 w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.

Art. 15

Art. 15 zawiera przepisy związane z administracyjnymi karami pieniężnymi.

Obligatoryjnie administracyjnej karze pieniężnej będą podlegały podmioty dokonujące nadużyć w komunikacji elektronicznej, wskazane wprost w poszczególnych punktach art. 3 ust. 1.

Fakultatywnej administracyjnej karze pieniężnej będą podlegali:

* przedsiębiorca telekomunikacyjny, który nie wypełnia obowiązków wskazanych w art. w art. 4 ust. 6, art. 8 ust. 2 i art. 9 ust. 12,
* dostawca poczty elektronicznej który nie wypełnia obowiązków wskazanych w art. 12 ust. 1.

Kara będzie mogła być również nałożona na kierownika podmiotu publicznego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 11 ust. 2.

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. 15 proponuje się zmianę tej ustawę stosownie modyfikując przepis o przychodach tego Funduszu.

Art. 16

Przepis art. 16 penalizuje trzy wskazane 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. Sprawca takiego działania będzie podlegał karze pozbawienia wolności od 3 miesięcy do 5 lat. W przypadku mniejszej wagi sprawca będzie podlegał grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jeżeli działania te popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Art. 17

Przepis art. 17 nakłada na Prezesa UKE obowiązek przedstawienia sejmowej komisji właściwej w sprawach nowych technologii półrocznego sprawozdania z wykonywania zadań określonych w ustawie.

Art. 18

Przepis art. 18 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. 15 niniejszej ustawy.

Art. 19

W art. 19 ustanowiono obowiązki związane z uruchomieniem i wdrożeniem przez CSIRT NASK systemu teleinformatycznego do przekazywania informacji o wzorcach wiadomości zawierających smishing. Zgodnie z ust. 3 projektowanego przepisu, Komendant Główny Policji, Prezes UKE i przedsiębiorcy telekomunikacyjny będą obowiązani do dostosowania i podłączenia swoich systemów teleinformatycznych do wskazanego systemu w terminie 3 miesięcy od dnia zamieszczenia przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej informacji o jego uruchomieniu.

Art. 20

Przepis ma charakter intertempolarny 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.

Art. 21

W art. 21 określone zostały obowiązki przedsiębiorców telekomunikacyjnych dotyczące wdrożenia rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej wymienionych w art. 3 ust. 1 pkt 1, 2 i 3 – odpowiednio w terminie 6 i 12 miesięcy od dnia wejścia w życie projektowanej ustawy.

Art. 22

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[[5]](#footnote-5)* za porozumienie, o którym mowa w art. 11 ust.1. Również lista ostrzeżeń[[6]](#footnote-6) prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie ww. porozumienie powinna być prawnie uznana za listę, o której mowa w art. 11 ust. 3.

Pozostałe informacje

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

Wpływ projektu ustawy na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców został omówiony w ocenie skutków regulacji.

Projekt nie będzie miał wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt nie zawiera przepisów technicznych, tym samym nie podlega procedurze notyfikacji.

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 zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

1. Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021, s. 81,

   <https://cert.pl/uploads/docs/Raport_CP_2021.pdf>. [↑](#footnote-ref-1)
2. 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>. [↑](#footnote-ref-2)
3. 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>. [↑](#footnote-ref-3)
4. 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>. [↑](#footnote-ref-4)
5. <https://www.uke.gov.pl/akt/uke-przystapil-do-porozumienia-chroniacego-abonentow,300.html>. [↑](#footnote-ref-5)
6. <https://cert.pl/posts/2020/03/ostrzezenia_phishing/> [↑](#footnote-ref-6)