|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | | Instytucja | Jednostka redakcyjna | Treść uwagi | Odniesienie |
|  | RCL | | Art. 10 | 14) zgodnie z art. 10 ust. 1 projektu operatorzy mogą zawrzeć z Prezesem UKE porozumienie określające środki organizacyjne i techniczne, które będą stosowali przy realizacji obowiązków, o których mowa w art. 8. Zauważenia jednak wymaga, że obowiązek, o którym mowa w art. 8 dotyczy przedsiębiorców telekomunikacyjnych, w tym zakresie wskazany przepis wymaga więc korekty. Odnosząc się jednocześnie do kwestii samych porozumień:  a) projektowaną regulację należy uzupełnić o niezbędne minimalne elementy porozumienia, które miałyby zastosowanie do wszystkich operatorów/przedsiębiorców telekomunikacyjnych zawierających porozumienie,  b) wyjaśnienia wymaga, jakie jeszcze, oprócz blokowania numeru i ukrywania identyfikacji numeru, usługi telekomunikacyjne będące skutkiem wprowadzonych środków  technicznych i organizacyjnych, o których mowa w art. 10 ust. 1 (wskazany przepis odsyła w tym zakresie do art. 8 projektu) będzie świadczyć operator, za których niewykonanie bądź nienależyte wykonanie, w przypadku poprawnego wykonywania porozumienia, nie poniesie on odpowiedzialności; | **Uwaga nieuwzględniona co do doregulowania porozumienia antyspoofing’owego**  Z projektowanych przepisów wynikają m.in.: strony porozumienia, jego przedmiot wraz z celem jego zawarcia, kontrola porozumienia oraz szczególne skutki jest zawarcia i stosowania. Reasumując, minimalne elementy porozumienia są już określone na poziomie ustawowym. Z kolei środki organizacyjne i techniczne jakie będą stosowali przedsiębiorcy są kwestią zbyt szczegółową by została ona uregulowana na poziomie ustawowym. Z tego powodu te kwestie będą ujęte w samym porozumieniu. |
|  | RCL | | Art. 11 | w przypadku projektowanego art. 11 należy podkreślić, że przewidywane jako zawartość projektowanego porozumienia zasady zgłaszania domen, wpisywania i oraz usuwania tych domen z listy ostrzeżeń (o których mowa w ust. 5) stanowią materię rangi ustawowej i powinny zostać określone przepisami ustawy, podobnie jak Projektodawca to uczynił w przypadku art. 4-6 dla nadużycia, o którym mowa w art. 3 ust. 1 pkt 2. Powyższe dotyczy także prowadzenia jawnej listy, o której mowa w art. 11 ust. 1 projektu oraz zadań i kompetencji poszczególnych organów odpowiedzialnych za zwalczanie nadużyć, a wskazanych obecnie jako strony porozumienia w art. 11 ust. 4. Ewentualne doprecyzowania przepisów ustawowych powinny zostać uregulowane w przepisach wykonawczych do ustawy. Takie rozwiązanie pozwoli na rezygnację z regulowania tej materii w drodze porozumienia i rezygnację z regulacji dostosowujących zawartych w art. 22 projektu. Ponadto wskazać należy, że projektowana regulacja nie określa procedury odwoławczej od decyzji o wpisaniu na listę ostrzeżeń, co wymaga uzupełnienia. | **Uwaga nieuwzględniona**  Minimalne elementy porozumienia są już określone w projektowanych przepisach rangi ustawowej.  Porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwienia dostępu do tych stron jako środek o charakterze samoregulacji funkcjonuje bardzo dobrze, z korzyścią dla użytkowników. Praktyka potwierdza to, że to rozwiązanie jest właściwe w stosunku do „oszukańczych” domen. Lista ostrzeżeń jest jawna i spełnia wymogi transparentności. Jednocześnie funkcjonowanie listy wiąże się z uprawnieniem (a nie obowiązkiem) zablokowania dostępu do stron www. wpisanych na listę. |
|  | MON | | Art. 12 | 1. W **art. 12** proponuje się dodać ust. 5 i 6 w brzmieniu:   *„5. Dostawca poczty elektronicznej, o którym mowa w ust. 1, ma obowiązek przechowywania, przez okres nie krótszy niż 90 dni, rejestrów logowań do obsługiwanych przez siebie skrzynek poczty elektronicznej, zawierających co najmniej datę, godzinę uszczegółowioną do 1 sekundy, adres IP oraz port przypisany użytkownikowi w trakcie połączenia przez przedsiębiorcę telekomunikacyjnego.*  *6. Dostawca poczty elektronicznej nieodpłatnie udostępnia dane, o których mowa w ust. 5, organom państwa uprawnionym na podstawie odrębnych przepisów, na potrzeby prowadzonych przez nie postępowań.”.*  4. Jednocześnie, w konsekwencji przyjęcia proponowanych zmian, zasadnym wydaje się rozważenie wprowadzenia regulacji mających na celu wzmocnienie skuteczności pozyskiwania danych, o których mowa w art. 12 ust. 5, przez organ państwowy, np. przez wprowadzenie kontroli Prezesa UKE na zasadach analogicznych jak w art. 12 ust. 3 projektu.  W związku z dynamicznym rozwojem nowych technologii oraz coraz bardziej kreatywnymi sposobami wykorzystywania ich przez osoby popełniające czyny zabronione, organy ścigania muszą niejednokrotnie sięgać po dane związane z użytkowaniem poczty elektronicznej.  Z uwagi na brak obecnie przepisów nakładających na dostawców poczty elektronicznej obowiązek gromadzenia danych na temat adresów IP wraz z portami przypisanymi przez właściwego przedsiębiorcę telekomunikacyjnego w czasie logowań, znacznie utrudnione jest ściganie sprawców przestępstw wykorzystujących pocztę elektroniczną do popełniania czynów zabronionych. Wynika to z faktu wykorzystania przez większość przedsiębiorców telekomunikacyjnych technologii CGNAT i NAT w przypadku przydzielania abonentom adresów IPv4. W praktyce oznacza to przypisanie jednego adresu publicznego bardzo dużej liczbie abonentów w tym samym czasie, co bardzo utrudnia, a często uniemożliwia ustalenie urządzenia końcowego, które korzystało z danego adresu IP. Z uwagi na brak możliwości nakazania przedsiębiorcom telekomunikacyjnym wykorzystywania jedynie adresów IPv6, które rozwiązują ten problem – proponowane zmiany są zasadne. Wprowadzenie wyżej wymienionych przepisów nie spowoduje powstania po stronie dostawców poczty elektronicznej znacznych kosztów, jest również w pełni wykonalne z technicznego punktu widzenia, a przechowywanie wymienionych w proponowanym ust. 5 danych jest niezbędne do sprawnego ścigania sprawców przestępstw. | **Uwaga nieuwzględniona**  Należy wskazać, że celem przepisu jest uregulowanie obowiązków z zakresu bezpieczeństwa poczty elektronicznej, stosowania mechanizmów uwierzytelnienia poczty elektronicznej. Nie jest celem ustawy wprowadzanie obowiązków retencyjnych, które wykraczają poza kwestie walki z nadużyciami w komunikacji elektronicznej. Mają szersze, systemowe skutki dla różnego rodzaju postępowań prowadzonych przez służby.    Dostawcy usług poczty elektronicznej kwalifikują się do kategorii dostawców usług komunikacji interpersonalnej niewykorzystujących numerów („NICS”) (które zostaną uregulowane w PKE) a także usług świadczonych drogą elektroniczną. Należy wskazać, że ta kategoria podmiotów nie jest również w PKE objęta przepisami retencyjnymi. Dyrektywa ustanawiająca Europejski Kodeks Łączności Elektronicznej wyłącza tę kategorię podmiotów (dostawców NICS) z obowiązków związanych z ogólnym zezwoleniem, tj. nie podlegają wpisowi do rejestru przedsiębiorców telekomunikacyjnych. Brak jest zatem oficjalnych danych tych podmiotów. Egzekwowanie stosowania przepisów mogłoby być znacząco utrudnione, gdyż często przedsiębiorcy Ci mają siedziby za granicą. W efekcie zatem wprowadzone obowiązki obciążyły by de facto polskich dostawców takich usług, stawiając ich mniej korzystnej sytuacji niż konkurenci z zagranicy. Naraziłoby to również te podmioty na dodatkowe koszty retencjonowania danych, które nie są im potrzebne. Większy zakres przechowywanych danych wymagałby posiadania pojemniejszych, bezpiecznych serwerów, zakupu bezpiecznego oprogramowania itp.    Podkreślenia wymaga również fakt, że generalny obowiązek retencji danych telekomunikacyjnych został zakwestionowany przez TSUE. Trybunał w licznych wyrokach odnosił się w restrykcyjny sposób do kwestii gromadzenia danych pochodzących z komunikacji elektronicznej i ich udostępniania uprawnionym podmiotom.  Wprowadzanie nowych obowiązków retencyjnych, w odniesieniu do kolejnych grup podmiotów może spotkać się z zarzutem niezgodności z orzecznictwem TSUE.  W ramach UE ciągle trwają prace grupy roboczej ds. współpracy w sprawach karnych COPEN dotyczących wspólnego podejścia do retencji danych w świetle dyrektywy 2002/58/UE o prywatności oraz orzecznictwa TSUE. Grupa rozważa m.in. objęcie obowiązkiem retencyjnym dostawców NICS, poddania retencji adresów IP. Wprowadzanie nowych obowiązków retencyjnych w oderwaniu od prac tej grupy, zapadłych wyroków TSUE jest przedwczesne.  Ponadto, ustawa o świadczeniu usług drogą elektroniczną oraz ustawy kompetencyjne służb zawierają już pewne regulacje dotyczące udostępniania służbom danych zbieranych przez dostawców usług (np. art. 18 uśude). |
|  | MON | | Art. 17a | 1. W następstwie uwzględnienia proponowanego brzmienia art. 12 ust. 5 i 6 niezbędnym jest dodanie w projekcie po art. 17 przepisów zmieniających *ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2021 r. poz. 1214, z późn. zm.),* w brzmieniu:   *„****Art. 17a.****W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2021 r. poz. 1214 oraz z 2022 r. poz. 655) w art. 30 wprowadza się następujące zmiany:*  *1) w ust. 1 po pkt 3 dodaje się pkt 4 w brzmieniu:*  *„4) art. 12 ust. 5 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …);”;*  *2) w ust. 3 po wyrazach „pkt 3” dodaje się wyrazy: „i 4”.* | **Uwaga nieuwzględniona w zw. z nieuwzględnieniem uwagi dot. art. 12 ust. 5 i 6 (pkt 3 tabeli)** |
|  | MS | | OSR | Podkreślenia wymaga, że przedstawiony projekt ustawy nakłada na sądownictwo powszechne **całkowicie nowe obowiązki**. Tym samym oczywistym jest, że ich realizacja musi wiązać się ze wzmocnieniem etatowym. Nowe obowiązki powodują bowiem zwiększenie zadań i tak już znacznie obciążonego sądownictwa, a w związku z tym nie można oczekiwać, że będą one realizowane obecnymi zasobami kadrowymi bez pogorszenia sprawności postępowań.  W OSR wśród podmiotów, na które może oddziaływać projekt ustawy, nie ma SO w Warszawie – SOKiK oraz Sądu Apelacyjnego w Warszawie. Podkreślić trzeba, że takie oddziaływanie może wystąpić, biorąc pod uwagę możliwość odwołania od decyzji Prezesa UKE w przedmiocie kary pieniężnej – określonej w **art. 15** – na podstawie art. 206 ust. 2 pkt 3 *Prawa telekomunikacyjnego*. Konieczność oszacowania wpływu projektowanych rozwiązań na SOKiK, wynika także z rozwiązania przyjętego w art. 10 ust. 4 i art. 12 ust. 4. Przepisy te zawierają odesłanie do przepisów *Prawa telekomunikacyjnego* o kontroli, przy czym zastrzeżenia budzi już sama ogólnikowość takiego odesłania. *Prawo telekomunikacyjne* obejmuje szereg takich przepisów, przy czym w większości znajdują się one w rozdziale 2 *Kontrola i postępowanie kontrolne*. Przepis art. 201 *Prawa telekomunikacyjnego* przewiduje podstawę do wydania przez Prezesa URE decyzji o nałożeniu kary pieniężnej, o której mowa w art. 209, w przypadku stwierdzenia naruszeń obowiązków wynikających z przepisów prawa lub decyzji wydanej przez Prezesa UKE. Zgodnie z art. 206 ust. 2 pkt 3 *Prawa telekomunikacyjnego* decyzja taka podlega zaskarżeniu do SOKiK.  Ponadto **art. 16 ust. 1 i 2** penalizuje trzy nadużycia w komunikacji elektronicznej.  Powoduje to rozszerzenie kognicji wydziałów karnych w sądach powszechnych, zarówno w I, jak też II instancji, co nie zostało wskazane w uzasadnieniu projektu.  Podkreślenia wymaga, że wzrost liczby spraw nie może zostać precyzyjnie oszacowany, albowiem przewidziane projektem ustawy instytucje są nowe i brak jest jakichkolwiek danych umożliwiających oszacowanie tej wartości. Nadto, ani w uzasadnieniu projektu, ani w OSR nie zostały podane jakiekolwiek dane pozwalające na choćby hipotetyczne określenie liczby spraw, które trafią do sądów. Oczywistym jest, że wsparcie etatowe jest konieczne, albowiem komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne i penalizowane czyny mogą występować bardzo często. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych korzysta wiele milionów osób. Usługi te są również coraz szerzej i w sposób bardziej wyszukany wykorzystywane przez przestępców w celu wyrządzenia szkód po stronie przedsiębiorców telekomunikacyjnych, użytkowników końcowych oraz osiągnięcia nienależnych korzyści.  Nowe sprawy – z art. 15 projektu ustawy – trafią do SO w Warszawie – SOKiK, a – z art. 16 projektu ustawy – do sadów rejonowych (pion karny). Zachodzi więc konieczność zapewnienia zwiększenia potencjału kadrowego tych jednostek Znając ograniczenia budżetowe wynikające z sytuacji spowodowanej pandemią COVID-19, Ministerstwo Sprawiedliwości wnosi o przydzielenie nowych etatów do: **SOKiK w liczbie: 1 etat sędziowski, 1 etat asystencki i 2 etaty urzędnicze oraz sądów rejonowych (pion karny) w liczbie: 5 etatów sędziowskich, 5 etatów asystenckich i 10 etatów urzędniczych.**  Zaznaczenia przy tym wymaga, że nie zgłasza się potrzeb na szczeblu sądów okręgowych,choć oczywistym jest, że trafią tam odwołania od orzeczeń wydanych w I instancji. **Etatypowyższe powinny zostać uruchomione od 1 stycznia 2023 r.**  Mając na względzie powyższe, modyfikacji wymaga OSR projektu w punkcie 4  *Podmioty, na które oddziałuje projekt* przez wskazanie SO w Warszawie jako podmiotu rozpoznającego odwołania od decyzji Prezesa UKE oraz sądów powszechnych (sądy okręgowe i sądy rejonowe) jako podmiotów rozpatrujących nowe sprawy karne.  W obu przypadkach nastąpi wzrost wpływu nowych spraw. Skutkiem powyższego konieczne wydaje się także uzupełnienie OSR w punkcie 6 *Wpływ na sektor finansów publicznych* i wskazanie stosownych wydatków związanych z planowanym wsparciem etatowym. | **Uwaga nieuwzględniona**  Przyjęte rozwiązania nie doprowadzą do istotnego wzrostu liczby spraw sądowych. W związku z tym, że dołączenie do porozumienia i jego realizacja będą wiązały się z domniemaniem wypełniania obowiązków wynikających z niniejszej ustawy, najprawdopodobniej nie będzie wielu postępowań karnoadministracyjnych. W związku z tym nie jest konieczne wygospodarowanie nowych wydatków dla SOKIK-u. |