Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 26.06.2020 r.
KIGEiT/1668/06/2020

Sz. P. Agnieszka Krauzowicz
Dyrektor
Departament Telekomunikacji
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dotyczy: pisma z dnia 18 czerwca 2020 r. nr DT-WUKE.441.6.2020

Szanowna Pani Dyrektor,

Działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***"), w odpowiedzi na pismo z dnia 18 czerwca 2020 r. nr DT-WUKE.441.6.2020, Izba dziękując za umożliwienie zaprezentowania stanowiska poniżej przedstawia uwagi do poszczególnych zagadnień w ramach projektu ustawy – Prawo Komunikacji Elektronicznej.

Ad. 1 Wykorzystanie metody wideoidentyfikacji przy rejestracji abonenta

Izba pozytywnie ocenia sam kierunek zmian i rozszerzenie katalogu możliwych sposobów weryfikacji abonentów, w dalszym ciągu postulując dalej idące rozwiązanie, polegające na rezygnacji z tego wymogu. Warto w tym miejscu podkreślić, iż obowiązek rejestracji danych ma na celu ograniczenie zagrożenia wynikającego z ryzyka ataków terrorystycznych, ponieważ takie było uzasadnienie wdrażania tych przepisów. Na dzień dzisiejszy można stwierdzić, iż wdrożone przepisy, które zwiększają koszty działalności po stronie operatorów, spełniły swoje oczekiwania. Dodatkowa bariera w korzystaniu z usług telekomunikacyjnych oraz dodatkowy koszt po stronie operatorów w realizacji procesu, zwiększa bariery do popełniania nadużyć na rynku telekomunikacyjnym, w tym odnoszących się do zagrożeń terrorystycznych. Z tego względu, każde działanie które ma usprawnić obecny proces (a tym samym obniżyć koszty operatorów), przy obecnym poziomie wiarygodności jest jak najbardziej pożądane. Istotne jest również zrozumienie, iż operatorzy mają jedynie potwierdzić dane użytkownika z wiarygodnym źródłem, nie zaś budować tzw. tożsamość elektroniczną użytkownika, zgodnie z regulacją eIDAS.

Przechodząc z kolei do szczegółów proponowanego rozwiązania pragniemy zwrócić uwagę na następujące kwestie.

Po pierwsze, proponowane rozwiązanie ogranicza wideoweryfikację do porównywania danych z dowodem osobistym. Wydaje się, że możliwość ta powinna być jak najbardziej szeroka i obejmować również np. dokumenty takie jak prawo jazdy. Wydaje się zatem, że powiązanie z rejestrem dowodów osobistych jest nadmiarowe. Dodatkowo proces wideoweryfikacji w czasie rzeczywistym jest tylko jedną z wielu metod porównywania danych, jakie mogą zostać wykorzystane. Aktualnie na rynku wykorzystywane są automatyczne mechanizmy

rozpoznawania twarzy użytkownika i porównywanie kluczowych cech twarzy ze zdjęciem znajdującym się w warstwie graficznej dokumentu tożsamości. Mechanizm ten nie wymaga przeprowadzenia wideoweryfikacji poprzez połączenie video pracownika operatora i użytkownika końcowego. Dodatkowo sam dokument tożsamości zawiera coraz więcej funkcji, które powinny być wykorzystywane przez operatorów np. podpis osobisty potwierdzony za pośrednictwem kanału NFC telefonu, czy też możliwość potwierdzania za pośrednictwem innych cech biometrycznych. Te wszystkie obecnie działające rozwiązania powinny być uwzględnione w proponowanej regulacji

Bez uszczerbku dla powyższej uwagi wskazujemy również na zasadnicze wątpliwości związane z koniecznością uzyskania decyzji, o której mowa w art. 68 ust. 3 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (tj. Dz. U. z 2020 r., poz. 332, dalej „Ustawa o dowodach osobistych").

Zgodnie ze wskazanym przepisem, decyzja taka jest wydawana po spełnieniu wymogów w zakresie (i) posiadania i stosowania mechanizmów umożliwiających identyfikację i rejestrację osób uzyskujących dostęp do danych oraz rejestrujących zakres udostępnionych danych i datę udostępnienia danych oraz (ii) posiadania i stosowania zabezpieczeń technicznych i organizacyjnych chroniących przed uzyskaniem dostępu do danych przez inne osoby i podmioty. Jednocześnie przepisy Ustawy o dowodach osobistych ani wydane na jej podstawie przepisy wykonawcze w żaden sposób nie precyzują ww. wymagań, co rodzi ryzyko arbitralnych rozstrzygnięć w tym zakresie. Jest to o tyle istotne, że Ustawa o dowodach osobistych przewiduje w zakresie tych wymagań możliwość kontroli oraz cofnięcia decyzji, a tym samym pozbawienia przedsiębiorcy telekomunikacyjnego możliwości korzystania z tej metody. Wątpliwości budzi również kwestia rejestrowania zakresu udostępnionych danych w kontekście stanowiska Prezesa UODO co do możliwości przetwarzania danych osobowych związanych z dowodem osobistym.

Zdaniem Izby należy zapewnić także odpowiednio szybkie rozstrzygnięcie wniosku o uzyskanie dostępu do rejestru, tak, by przedsiębiorcy mogli zaplanować korzystanie z takiej formy weryfikacji. Jednoczesne utrzymywanie innych form, w szczególności dla podmiotów, które nie mają stacjonarnej sieci sprzedaży, jest rozwiązaniem bardzo kosztownym.

Izba zwraca również uwagę, że zgodnie z Ustawą o dowodach osobistych udostępnienie danych jest nieodpłatne na rzecz podmiotów realizujących na podstawie ustaw szczególnych zadania publiczne. W ocenie Izby weryfikacja jest zadaniem publicznym. W celu uniknięcia jakichkolwiek wątpliwości powinno być to wprost wskazane w projektowanej ustawie (jednorazowe udostępnienie wiąże się z opłatą w wysokości 31 złotych, co może stanowić istotną barierę).

Izba zwraca również uwagę na kwestie związane z możliwością zawieszenia wideoweryfikacji. Zdaniem Izby należy usunąć możliwość zawieszenia w sytuacji niezachowania należytej staranności. Przesłanka ta występuje jako alternatywa wobec przesłanki niezgodności z przepisami. Trudno sobie wyobrazić sytuację, w której praktyka jest co prawda zgodna z przepisami, ale jednocześnie z uwagi na uznaniowe stwierdzenie braku należytej staranności, wobec przedsiębiorcy jest stosowana sankcja.

Ad. 2 Zwalczanie nadużyć telekomunikacyjnych

Izba zwraca uwagę, że proponowana definicja nadużycia telekomunikacyjnego odbiega od standardu wypracowanego przez wszystkie organizacje sektorowe przy okazji porozumień związanych z tzw. ruchem non-EOG.

W ocenie Izby wypracowana definicja trafniej określa istotę nadużycia telekomunikacyjnego. Postulujemy skorzystanie z wypracowanej i stosowanej od kilku lat definicji.

Izba podkreśla, że wprowadzenie mechanizmu nakazującego przedsiębiorcy telekomunikacyjnemu zgłoszenia wystąpienia nadużycia telekomunikacyjnego wraz z proponowanymi środkami zaradczymi **z jednoczesnym obowiązkiem oczekiwania na wydanie decyzji przez Prezesa UKE przez okres 7 dni** przyczyni się znacząco do wzrostu nadużyć na rynku telekomunikacyjnym oraz pozbawi przedsiębiorców telekomunikacyjnych możliwości skutecznej ochrony uczciwych abonentów. Należy zauważyć, iż większość nadużyć telekomunikacyjnych ma charakter krótkotrwały i intensywny, w związku z czym reakcja na nadużycie i podjęcie środków zaradczych dla swej skuteczności wymaga natychmiastowego działania, również w godzinach nocnych oraz w okresie świątecznym.

Przykładem sztucznego ruchu jest jednoczesna aktywacja wielu kart SIM (setek lub tysięcy zarejestrowanych na tzw. słupy) oraz wykonywanie połączeń na określone zakresy krajowe lub międzynarodowe. W celu maksymalizacji korzyści z nadużycia, połączenia te wykonywane są jednocześnie z wielu kart i mają maksymalną możliwą długość.

- W takim przypadku, degradacji podlega jakość połączeń innych użytkowników sieci telekomunikacyjnej, uniemożliwiając w skrajnych przypadkach wykonywanie połączeń;
- koszty sztucznego ruchu obciążają Operatora.

Skuteczną metodą przeciwdziałania tego typu nadużyciom jest szybkie wykrycie i zablokowanie numerów generujących ruch. Po zablokowaniu pierwszej partii kart, dokonujący nadużycia aktywują kolejne karty kontynuując proceder co rodzi konieczność blokowania kolejnych kart.

Informowanie Prezesa UKE o każdym przypadku wystąpienia powyższego naruszenia i oczekiwanie na jego decyzję przez okres 7 dni z jednoczesnym przyzwoleniem na generowanie ruchu przez ten okres, poza spadkiem jakości połączeń dla innych użytkowników sieci, doprowadziłoby do gigantycznych strat finansowych przedsiębiorców telekomunikacyjnych. Tytułem przykładu w przypadku nadużycia, w którym bierze udział 1000 kart, dzwoniących przez 7 dni bez przerwy (7dni*24h*60min= 10080 minut), przy założeniu kosztu w wysokości 1zł, strata wyniesie 10 080 000 zł. W przypadku ruchu międzynarodowego, gdzie koszty za minutę mogą wynosić 1EUR straty te są kilkukrotnie wyższe.

W przypadku wydania przez Prezesa UKE, w terminie 7 dni, decyzji stwierdzającej wystąpienie nadużycia telekomunikacyjnego umożliwiającej blokadę tego ruchu, proceder zostanie przeniesiony na nowe karty SIM, co wywoła konieczność nowego zgłoszenia do Prezesa UKE tworząc tym samym parasol ochronny dla osób żyjących z nadużyć telekomunikacyjnych.

Jedynym sposobem ograniczania skali nadużycia jest zablokowanie kart sim na tyle szybko, żeby koszt pozyskania i aktywacji kart SIM przekraczał korzyści płynące z nadużycia. Sprowadza się to do reakcji w ciągu kilku minut od momentu wykrycia nadużycia telekomunikacyjnego.

Proces występowania z wnioskiem do UKE skutkować będzie znaczącym opóźnieniem w zablokowaniu nadużycia czego konsekwencją będzie promowanie nadużyć i naturalna zachęta do uruchomienia kolejnych kart.

Ponadto warto także zauważyć, że istnieją nadużycia telekomunikacyjne, w których skutkiem oszustwa są wymierne straty finansowe ponoszone przez abonentów (np. Wangiri fraud). Przyjęcie zaproponowanych przez Ministerstwo Cyfryzacji przepisów oznaczałoby, że przedsiębiorca telekomunikacyjny nie może podjąć natychmiastowych działań blokujących działania przestępców i chroniących abonentów przed kosztami, gdyż w pierwszej kolejności musiałby zgłosić zidentyfikowane naruszenie do Prezesa UKE i oczekiwać na decyzję Prezesa UKE co do możliwość podjęcia działań zaradczych. Biorąc pod uwagę, że fraud Wangiri jest

niestety zjawiskiem dosyć powszechny, każdy z największych operatorów musiałby w zasadzie codziennie składać zgłoszenia do Prezesa UKE, a abonenci ponosiliby koszty takich połączeń do czasu zakończenia postępowania administracyjnego przez Prezesa UKE.

Wskazać należy także, że proponowane w art. 152 ust. 2-6 PKE rozwiązanie skutkować będzie także koniecznością zgłaszania do Prezesa UKE każdego przypadku będącego obecnie przedmiotem zawiadomienia Operatora o możliwości popełnienia przestępstwa w szczególności z art. 286 § 1 kk i art. 270 § 1 kk.

Pozostawienie przepisu w obecnym kształcie nie tylko stworzy warunki do masowych nadużyć, ale przede wszystkim, uniemożliwi Operatorom podejmowanie skutecznej i szybkiej reakcji. Ponadto dodatkowo obciąży przedsiębiorcę i Prezesa UKE każdorazowym zgłaszaniem nadużycia.

Dodatkowo zasadnicze wątpliwości budzi propozycja ujęta w art. 292 ust. 3 projektowanej ustawy. Zdaniem Izby istnieje ryzyko poważnych następstw ew. nieprawidłowych decyzji. Zdaniem Izby obecne regulacje, w tym również uprawnienia przewidziane w ramach postępowań kontrolnych, są wystarczające.

Ad. 3 Działania na wypadek upadłości przedsiębiorcy telekomunikacyjnego

Izba zgłasza wątpliwości związane z przesłanką „zagrożenia naruszenia interoperacyjności lub ciągłości świadczenia usług telekomunikacyjnych w sieciach telekomunikacyjnych". Środki zaradcze stosowane w takiej sytuacji są tak daleko idące, że należy zapewnić wysoki standard w zakresie wykazania rzeczywistego ryzyka.

Jednocześnie należy rozważyć ryzyka związane z kryteriami dysponowania zwolnioną numeracją. Przyjęte w projekcie przesłanki (liczba przeniesionych numerów z bloków numerów, dla których Prezes UKE cofnął przydział, liczba abonentów w danej strefie numeracyjnej lub przydział numeracji w bloku sąsiadującym z przydzielanym blokiem numerów) są albo irrelewantne albo promują największych dostawców. Takie działanie będzie zatem sprzeczne z przesłanką promowania skutecznej konkurencji.

Wątpliwości budzi również zasada, zgodnie z którą to nowy dostawca, który otrzymał przydział numeracji, ma obowiązek poinformowania abonentów obecnie korzystających z usług dostawcy, który zgłosił upadłość. Zdaniem Izby obowiązek ten powinien być realizowany przez dotychczasowego dostawcę, zaś abonent powinien podjąć decyzję co do dalszego korzystania z numeru. Izba zgłasza także sprzeciw wobec proponowanego przepisu, nakładającego na przedsiębiorcę telekomunikacyjnego obowiązek świadczenia usług „na dotychczasowych warunkach". Przejmujący przedsiębiorca nie miałby bowiem wiedzy na jakich warunkach dotychczasowa oferta była świadczona, ponadto nawet gdyby taką wiedzę posiadł, musiałby specjalnie tworzyć w swoich systemach liczne odpowiedniki takich „dotychczasowych" ofert. Ponadto konieczna byłaby techniczna implementacja przejętej numeracji i rozgłoszenie jej na rynku, co wymaga czasu. Wszystkie te czynniki powodują, że proponowane w projekcie przepisów rozwiązanie jest kosztowne, czasochłonne i nierealne.

Z tych samych względów wydaje się, że brak jest podstaw do nakładania opłat za numerację przydzieloną na mocy decyzji Prezesa UKE danemu przedsiębiorcy bez jego wniosku o tę numerację, lecz wskutek upadłości innego przedsiębiorcy.

Ad. II Certyfikaty

Podmiot dokonujący audytu bezpieczeństwa przedsiębiorcy telekomunikacyjnego, powinien zatrudniać audytorów posiadających certyfikaty wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U z 2018 poz. 1999), będącym rozporządzeniem wykonawczym

do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 poz. 1560), tj:

1. Certified Internal Auditor (CIA);

2. Certified Information System Auditor (CISA);

3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001, wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;

4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

5. Certified Information Security Manager (CISM);

6. Certified in Risk and Information Systems Control (CRISC);

7. Certified in the Governance of Enterprise IT (CGEIT);

8. Certified Information Systems Security Professional (CISSP);

9. Systems Security Certified Practitioner (SSCP);

10. Certified Reliability Professional;

11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Ponadto Izba zwraca uwagę, że aktualnie Prezes Urzędu Ochrony Danych Osobowych przygotował wymagania dla podmiotów monitorujących kodeksy postępowania RODO, który to dokument został przekazany Europejskiej Radzie Ochrony Danych, dlatego sugerujemy, by Minister Cyfryzacji przy tworzeniu wymagań dla audytorów wykorzystał wskazane tam obowiązki.

Z poważaniem

Prezes Zarządu

Stefan Kamiński