Czy nowa ustawa telekomunikacyjna uderzy w naszą prywatność?

5 lipca 2024

21 maja do Sejmu wpłynął nowy rządowy projekt ustawy „Prawo komunikacji elektronicznej”, który wywołał szeroką debatę w mediach. Wiele osób obawia się, że nowa regulacja, wdrażająca prawo unijne, stworzy przestrzeń do naruszeń prywatności i inwigilacji, tym razem bez konieczności uzyskania zgody sądu czy prokuratury.

Obecnie polski internet jest stosunkowo wolny od biurokratycznych obciążeń dla firm telekomunikacyjnych. Chociaż przedsiębiorcy muszą współpracować z odpowiednimi służbami, nadal chronią dane swoich klientów, a wszelkie procedury są prowadzone manualnie.

Minister cyfryzacji Krzysztof Gawkowski wprowadził wiele inicjatyw na rzecz cyfryzacji i podniesienia prestiżu naszych instytucji, takich jak NASK i CERT Polska, na arenie europejskiej. Nowy projekt ustawy ma na celu pokazanie Unii Europejskiej, że Polska dąży do zwiększenia kompetencji nadzoru cyfrowego. Choć polskie służby często mają ograniczone możliwości działania, projekt ten może wzmocnić ich pozycję, szczególnie w kontekście bezpieczeństwa publicznego.

Zespół „Faktów i Analiz” przeanalizował ustawę i zidentyfikował kilka kluczowych celów:

1. Zwiększenie współpracy i ustalenie procedur między krajowymi i unijnymi operatorami telekomunikacyjnymi.

2. Wdrożenie stopni alarmowych CRP, które będą podlegać prezesowi UKE.

3. Implementacja stanów zagrożenia, nadzwyczajnego i wojennego w polskiej telekomunikacji.

4. Procedury wyłączenia infrastruktury telekomunikacyjnej na określonych obszarach kraju.

5. Blokowanie połączeń i komunikatów elektronicznych przez przedsiębiorców telekomunikacyjnych, jeśli zagrażają bezpieczeństwu państwa.

6. Procedury przechowywania danych z publicznej sieci telekomunikacyjnej.

7. Kary dla przedsiębiorców telekomunikacyjnych za nieprzestrzeganie zasad przewidzianych w ustawie.

8. Przekazywanie informacji o abonentach przez przedsiębiorców telekomunikacyjnych.

9. Tworzenia raportów corocznych przez przedsiębiorców telekomunikacyjnych o stanie swojej infrastruktury.

Nowa ustawa jest kompleksowa i dotyczy wielu aspektów bezpieczeństwa publicznego, podkreślając konieczność dostosowania polskiego prawa do unijnych standardów i wzmacniając współpracę międzynarodową w obszarze telekomunikacji. Niemniej jednak otwiera drogę do naruszeń.

Stopnie alarmowe CRP

Stopień alarmowy CRP jest wprowadzany w przypadku zagrożenia atakiem terrorystycznym na systemy teleinformatyczne organów administracji publicznej lub systemy wchodzące w skład infrastruktury krytycznej, a także w przypadku wystąpienia takiego zdarzenia.

Na podstawie ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, stopnie alarmowe lub stopnie alarmowe CRP wprowadza, zmienia i odwołuje Prezes Rady Ministrów w

drodze zarządzenia, zależnie od rodzaju zagrożenia. Decyzję podejmuje po zasięgnięciu opinii ministra właściwego do spraw wewnętrznych oraz Szefa ABW. W przypadkach wymagających natychmiastowej reakcji minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii Szefa ABW, może wprowadzić stopień alarmowy, informując o tym niezwłocznie Prezesa Rady Ministrów.

Zgodnie z art. 40 ust. 2 projektu nowej ustawy, Prezes UKE, w przypadku ogłoszenia jednego ze stopni alarmowych CRP, może nałożyć na przedsiębiorców telekomunikacyjnych obowiązek minimalizowania szkód powstałych w wyniku zakłóceń radiowych i współpracy w celu wyeliminowania zagrożenia. W sytuacjach wymagających pilnych działań decyzje te mogą być przekazywane ustnie.

Stan wojenny, nadzwyczajny i podwyższonej gotowości obronnej państwa

W przypadku ogłoszenia stanu wojennego, nadzwyczajnego lub podwyższonej gotowości obronnej państwa, Prezes UKE wydaje przedsiębiorcom telekomunikacyjnym odpowiednie polecenia, nakładając na nich obowiązek współpracy w celu eliminacji zagrożenia.

Wyłączenie telekomunikacji z danego obszaru

Artykuł 42 projektu ustawy wprowadza kontrowersyjną możliwość wyłączenia telekomunikacji na określonym obszarze. W uzasadnionych przypadkach ściśle określonych w przepisach odrębnych minister właściwy do spraw wewnętrznych oraz służby wymienione w projekcie (m.in. CBA, ABW, Policja, Żandarmeria Wojskowa, SOP, kontrwywiad wojskowy) mogą zarządzić użycie

urządzeń zakłócających działanie sieci telekomunikacyjnych na danym terenie.

Zagrożenia i wątpliwości

Wprowadzenie tego przepisu budzi wiele obaw i zastrzeżeń. Możliwość wyłączenia komunikacji telekomunikacyjnej w sytuacjach kryzysowych, choć zrozumiała z punktu widzenia bezpieczeństwa publicznego, może nieść ze sobą szereg zagrożeń:

1. Nadmierna ingerencja w prawa obywatelskie: Dostęp do komunikacji jest fundamentalnym prawem człowieka, a jego ograniczenie, nawet czasowe i lokalne, powinno być ściśle uzasadnione i proporcjonalne do zagrożenia. Istnieje ryzyko nadużywania tych uprawnień przez służby, co może prowadzić do ograniczania wolności słowa i prawa do protestu.

2. Utrudnienie działań ratunkowych i medycznych: W przypadku katastrof lub awarii, sprawne działanie służb ratunkowych i medycznych jest kluczowe. Wyłączenie sieci telekomunikacyjnych może utrudnić lub uniemożliwić im koordynację działań i dotarcie do potrzebujących.

3. Destabilizacja życia społecznego: Nawet krótkotrwałe wyłączenie komunikacji może mieć negatywny wpływ na funkcjonowanie społeczeństwa, dezorganizując m.in. transport, systemy płatnicze i codzienne kontakty międzyludzkie.

Konieczne jest doprecyzowanie pojęcia „naruszenia porządku publicznego”, aby uniknąć nadmiernie szerokiej interpretacji, która mogłaby uzasadniać wyłączenie komunikacji w przypadku każdego większego protestu lub demonstracji antyrządowej.

W przypadku wyłączenia telekomunikacji na danym obszarze, krótkofalowcy i radioamatorzy mogą odegrać kluczową rolę jako łącznicy między ludźmi. Hobbyści ci od dawna podkreślają, że ich pasja zapewnia niezależność od rządów i korporacji, co

czyni ich idealnymi kandydatami do utrzymywania komunikacji w sytuacjach kryzysowych.

W przypadku wprowadzenia stanu wojennego reakcja Urzędu Komunikacji Elektronicznej (UKE) w kwestii wydawania licencji krótkofalarskich pozostaje niepewna. Doświadczenia historyczne wskazują, że podczas stanu wojennego w latach 1981-1983 wstrzymywano wydawanie większości zezwoleń amatorskich, a także blokowano możliwość składania nowych wniosków.

Blokowanie połączeń i komunikatów elektronicznych na wniosek prezesa UKE

Blokada musi być wprowadzona w ciągu 6 godzin od otrzymania decyzji. Prezes UKE może przekazać tę decyzję ustnie, a następnie, w ciągu 14 dni, dostarczyć ją na piśmie. Firmy telekomunikacyjne muszą niezwłocznie wykonać tę decyzję.

Art. 53 projektu ustawy przewiduje możliwość blokowania połączeń i komunikatów elektronicznych. Prezes UKE, na wniosek uprawnionego podmiotu, może nałożyć na firmę telekomunikacyjną obowiązek blokowania połączeń lub wiadomości elektronicznych, które mogą zagrażać bezpieczeństwu państwa lub porządkowi publicznemu.

Oznacza to, że dowolny abonent może zostać zablokowany, jeśli jego działania stanowią zagrożenie dla bezpieczeństwa państwa lub porządku publicznego.

Przekazywanie informacji o abonentach do polskich służb

Art. 43 projektu ustawy budzi największe kontrowersje. Na podstawie wniosku służb wymienionych w projekcie ustawy, takich jak Policja, ABW, CBA, KAS, Kontrwywiad Wojskowy i

inne, przedsiębiorca telekomunikacyjny ma obowiązek udostępnić informacje o abonentach.

Informacje te obejmują komunikaty elektroniczne przesyłane przez abonenta oraz dane dotyczące nadawcy komunikatu. W skład tych danych wchodzą: przydzielony numer telefonu (jeśli taki istnieje), adres korespondencyjny, data i godzina nadania komunikatu, dane lokalizacyjne abonenta oraz lokalizacja jego urządzenia.

Warto rozróżnić dwie kwestie. W przypadku dostawcy Internetu nie jest przydzielany numer telefonu. Natomiast jeśli korzystamy z Internetu mobilnego lub usług telekomunikacyjnych (np. SMS, starsze wersje RCS, połączenia telefoniczne), numer telefonu jest przydzielony. Obowiązek telekomunikacyjny dotyczy obu tych przypadków.

Definicja komunikatu elektronicznego w projekcie ustawy budzi szczególne zainteresowanie. Zgodnie z ustawą, komunikat elektroniczny to każda informacja wymieniana między użytkownikami. W kontekście Internetu komunikaty te obejmują transmisję pakietów danych. W większości przypadków protokoły komunikacyjne wykorzystują kryptografię, co oznacza, że transmisja jest szyfrowana.

Mimo szyfrowania operatorzy mogą przekazywać adres IP docelowy oraz nazwę domeny, jeśli abonent korzysta z dedykowanego serwera DNS. Pozwoliłoby to służbom określić, kiedy abonent połączył się z konkretnym serwerem, np. Telegrama. Jednak szczegółowe informacje zawarte w komunikacie byłyby niedostępne z powodu szyfrowania, co przypomina sytuacje związane z atakami typu Man in The Middle (MITM).

W przypadku SMS-ów i połączeń telefonicznych sytuacja jest prostsza, ponieważ wiadomości w tej transmisji najczęściej nie są szyfrowane i mogą być pozyskane przez operatora.

Źródło: FaktyiAnalizy.info