Szanowni Państwo,

piszę w związku z projektem ustawy o działaniach antyterrorystycznych uchwalonym przez Sejm 10 czerwca br., który ma być rozpatrywany przez Senat.

Mam do tego projektu następujące uwagi:

1. W art. 5 ust. 1 i 2 mowa o katalogu incydentów o charakterze terrorystycznym, określanym w drodze rozporządzenia przez ministra właściwego do spraw wewnętrznych w porozumieniu z ministrem właściwym do spraw finansów publicznych i Ministrem Obrony Narodowej oraz po zasięgnięciu opinii Szefa ABW. Katalog ten ma być używany do klasyfikacji informacji służących realizacji działań antyterrorystycznych, przekazywanych do ABW. Pojęcie „incydentu o charakterze terrorystycznym” nie jest zdefiniowane. Nie jest to to samo, co „zdarzenie o charakterze terrorystycznym” zdefiniowane w art. 2 pkt. 7 (sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub zagrożenie zaistnienia takiego przestępstwa) i za zapobieganie któremu, zgodnie z art. 3, odpowiedzialny jest Szef ABW. W załączonym do projektu ustawy projekcie rozporządzenia określającego ten katalog wymienione zostały m. in. takie zdarzenia, jak np.:

*"sygnały o podjęciu pracy przez cudzoziemców z krajów podwyższonego ryzyka, prowadzeniu przez nich działalności gospodarczej oraz powierzanie im wykonywania zleceń na terytorium RP"*

*"opublikowanie i zapowiedzi opublikowania w mediach materiałów audiowizualnych mogących wywołać protesty poszczególnych grup wyznaniowych lub etnicznych"*

*"próby uruchomienia lub uruchomienie internetowych portali, blogów, forów o charakterze ekstremistycznym, w szczególności funkcjonujących na serwerach zlokalizowanych na terenie RP"*

*"kolportaż literatury i periodyków propagujących ideologie ekstremistyczne"*

*"odnotowanie przesyłu środków finansowych z pominięciem międzynarodowych systemów bankowych, np. z zastosowaniem alternatywnych systemów przekazów pieniężnych typu hawala".*

Jest oczywiste, że tego typu zdarzenia nie muszą wyczerpywać znamion „zdarzenia o charakterze terrorystycznym” określonego zgodnie z definicją w art. 2 pkt. 7 ustawy, mogą nie naruszać prawa i nie musi zachodzić potrzeba zapobiegania im. Są to zdarzenia, które jedynie potencjalnie mogą mieć związek ze zdarzeniami o charakterze terrorystycznym. Dlatego też słusznie rozróżniono je od „zdarzeń o charakterze terrorystycznym” nadając im inną nazwę (w pierwotnym projekcie tego rozróżnienia nie było, co prowadziło do absurdalnej sytuacji, w której Szef ABW byłby odpowiedzialny za zapobieganie np. podejmowaniu pracy przez cudzoziemca z kraju podwyższonego ryzyka). Jednak pozostawienie nazwy bardzo zbliżonej, przy jednoczesnym braku zdefiniowania, czym jest „incydent o charakterze terrorystycznym” może potencjalnie grozić nadużyciami:

Po pierwsze, minister może legalnie umieścić w katalogu dowolny typ zdarzenia, niekoniecznie mający nawet potencjalny związek z terroryzmem (przykładowo „przynależność do partii politycznej mającej związek z nacjonalizmem” lub „aktywność grup kibiców”), co będzie skutkowało przekazywaniem do ABW informacji o osobach z terroryzmem niezwiązanych, za to związanych z np. opozycją polityczną.

Po drugie, podobieństwo nazwy „incydent o charakterze terrorystycznym” do nazwy „zdarzenie o charakterze terrorystycznym” może prowadzić do prób utożsamiania obu typów zdarzeń, a w rezultacie np. nakazy blokowania stron internetowych, na których zamieszczono „materiały audiowizualne mogące wywołać protesty poszczególnych grup wyznaniowych lub etnicznych” (np. krytykę islamu lub karykatury Mahometa).

Aby uniknąć tych nadużyć, wystarczy wprowadzić definicję „incydentu o charakterze terrorystycznym”. Wskazana byłaby też zmiana nazwy, ponieważ np. podjęcie pracy przez cudzoziemca z kraju podwyższonego ryzyka, choć w szczególnym przypadku może mieć związek z terroryzmem, to jednak samo w sobie charakteru terrorystycznego nie ma.

**W związku z tym proponuję:**

1. **W art. 5 ust. 2 i 3 zmienić sformułowanie „incydentów o charakterze terrorystycznym” na „incydentów mogących mieć związek z terroryzmem”;**
2. **W art. 2 dodać punkt 8 o treści: „incydencie mogącym mieć związek z terroryzmem – należy przez to rozumieć zdarzenie o charakterze terrorystycznym lub mogące mieć związek z takim zdarzeniem”.**
3. W art. 37 znajduje się fragment: *„Art. 32c. 1. W celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia, może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym, zwane dalej „blokadą dostępności””*. Jakkolwiek w sposób oczywisty chodzi tutaj o zablokowanie np. dostępności strony internetowej (z treściami mającymi związek z terroryzmem) przez właściciela hostingu, określonych treści na portalu lub forum internetowym przez właściciela tego portalu lub forum, bądź dostępności skrzynki mailowej wykorzystywanej przez terrorystów przez właściciela serwera poczty, to jednak w przypadku tych przedsiębiorców świadczących usługi drogą elektroniczną, którzy są jednocześnie przedsiębiorcami telekomunikacyjnymi oferującymi usługę dostępu do Internetu może zostać to wykorzystane do nakazania blokady dostępu do zasobów znajdujących się w światowym Internecie, a więc potencjalnego cenzurowania światowej sieci. Furtką jest tu brak dookreślenia, o jaki system teleinformatyczny chodzi. Obarczyłoby to tych przedsiębiorców problemem technicznego rozwiązania takiej blokady (zwłaszcza, jeżeli dane, do których dostęp ma być zablokowany znajdują się w tzw. darknecie czy „deep web” – <https://pl.wikipedia.org/wiki/Ukryta_sie%C4%87>) oraz ewentualnymi kosztami, które w związku z tym musieliby ponieść.

Pragnę zwrócić uwagę, że precyzyjne zablokowanie dostępu do określonego adresu internetowego (URL), w szczególności wskazującego na protokół SSL (rozpoczynającego się od https://) wymaga ponadstandardowych środków (oprogramowania lub dedykowanego sprzętu obsługującego analizę i filtrowanie pakietów w wyższych warstwach modelu OSI – np. lokalnego serwera proxy - <https://pl.wikipedia.org/wiki/Serwer_po%C5%9Brednicz%C4%85cy>), którymi przedsiębiorcy telekomunikacyjni, zwłaszcza mali, nie zawsze dysponują. W przypadku, jeżeli przedsiębiorcy nie dysponują odpowiednimi środkami technicznymi, żądanie zablokowania dostępu do określonego adresu internetowego mogą oni zrealizować jedynie przez zablokowanie dostępu do całego serwera, na którym te dane się znajdują (blokowanie po adresie IP) lub zablokowanie dostępu do całej domeny (np. facebook.com), co może spowodować zablokowanie dostępu do wielu innych zasobów, które nie powinny być blokowane. Ponadto blokada bezpośredniego dostępu do danego adresu jest mało skuteczna, gdyż można to łatwo obejść korzystając z takich usług jak np. serwery anonimizujące (<https://pl.wikipedia.org/wiki/Serwer_anonimizuj%C4%85cy>), open proxy (<https://pl.wikipedia.org/wiki/Open_proxy>), VPN (<https://pl.wikipedia.org/wiki/Virtual_Private_Network>) czy sieć TOR (<https://pl.wikipedia.org/wiki/Tor_%28sie%C4%87_anonimowa%29>), które pozwalają na dostęp pośredni. Blokowanie skuteczniejsze (choć i tak nie do końca stuprocentowo skuteczne) wymaga poniesienia sporych kosztów na urządzenia filtrujące. Kosztów tych nie oszacowano.

Proszę postawić się w sytuacji przedsiębiorcy telekomunikacyjnego dostarczającego dostęp do Internetu (providera), który otrzyma żądanie zablokowania dostępu do konkretnego adresu internetowego. Jeżeli zablokuje za dużo (np. cały adres IP), może liczyć się ze skargami na niedotrzymanie warunków umowy. Jeśli nie zablokuje sposobów obejścia, takich jak serwery anonimizujące, open proxy, VPN, TOR itd. (a przynajmniej nie spróbuje tego zrobić - nie wykaże "dołożenia należytej staranności"), może obawiać się odpowiedzialności za niewykonanie nakazu. W efekcie będzie zmuszony zainwestować w oprogramowanie / dedykowane urządzenia filtrujące i próbować zablokować wszystkie znane adresy serwerów anonimizujących, open proxy, VPN, protokół TOR itd. A co, jeżeli żądanie blokady dostępu będzie dotyczyło danych dostępnych jedynie przez TOR (np. w domenie .onion - <https://pl.wikipedia.org/wiki/.onion>)?

W pierwotnym projekcie ustawy żądanie blokowania miało być kierowane do „administratora systemu teleinformatycznego”. Jako, że to ostatnie pojęcie zostało zmienione na „usługodawcę świadczącego usługi drogą elektroniczną” świadczy o tym, że intencją autorów ustawy nie jest umożliwianie blokowania dostępu do zasobów światowego Internetu i możliwość zarządzenia zablokowania dostępu ma być kierowana jedynie do właścicieli hostingów, portali, for, serwerów pocztowych itd., w odniesieniu do danych znajdujących się w zarządzanych przez nich systemach. Aby ostatecznie zamknąć furtkę do wykorzystywania tego zapisu do prób cenzury Internetu wystarczy dookreślić, o jaki system teleinformatyczny chodzi.

**Proponuję więc zmienić w tym fragmencie słowa „dostępności w systemie teleinformatycznym” na „dostępności w zarządzanym przez siebie systemie teleinformatycznym”.**

1. Art. 21 proponowanej ustawy przewiduje możliwość zarządzenia przez ministra właściwego do spraw wewnętrznych zakazu odbywania zgromadzeń publicznych na obszarze objętym trzecim lub czwartym stopniem alarmowym. Stwarza to możliwość wprowadzenia takiego zakazu faktycznie z przyczyn politycznych (np. w celu zapobieżenia manifestacjom organizowanym przez opozycję), jedynie pod pretekstem wystąpienia „zdarzenia o charakterze terrorystycznym” (zgodnie z art. 2 ustawy takim zdarzeniem jest również samo zagrożenie zaistnienia czynu stanowiącego przestępstwo o charakterze terrorystycznym). Nawet, jeżeli obecny rząd ma dobre intencje, to za kilka lat do władzy mogą dojść inni.

Należy zwrócić uwagę, że zgodnie z obowiązującą ustawą zgromadzeniem jest „zgrupowanie osób na otwartej przestrzeni dostępnej dla nieokreślonych imiennie osób w określonym miejscu w celu odbycia wspólnych obrad lub w celu wspólnego wyrażenia stanowiska w sprawach publicznych” – bez określenia liczby tych osób, więc zgromadzeniem są już np. trzy osoby rozdające ulotki lub zbierające podpisy pod wnioskiem o referendum. Zakaz obejmie więc praktycznie wszystkie publiczne przejawy aktywności społecznej. Nie wydaje się to racjonalne – dlaczego osoby aktywne społecznie przebywające w miejscu publicznym miałyby stanowić większe zagrożenie dla życia i zdrowia ludzi lub bezpieczeństwa publicznego niż inne grupy osób przebywające w miejscu publicznym? Nawet, jeśli takie zagrożenie może wiązać się z konkretnym zgromadzeniem, to Prawo o zgromadzeniach przewiduje już możliwość zakazania konkretnego planowanego zgromadzenia przez organ gminy, jeżeli „jego odbycie może zagrażać życiu lub zdrowiu ludzi albo mieniu w znacznych rozmiarach”. Dodatkowy zakaz jest tu więc niecelowy.

**W związku z tym, proponuję ograniczyć możliwość wprowadzenia zakazu przewidzianą w art. 21 jedynie do imprez masowych.**

1. Art. 9 daje możliwość zarządzenia przez Szefa ABW, bez potrzeby uzyskiwania zgody sądu, na okres do 3 miesięcy, niejawnego prowadzenia czynności odpowiadających faktycznie czynnościom z zakresu kontroli operacyjnej, określonych w art. 27, ust. 6 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. W tym czasie czynności te nie stanowią formalnie kontroli operacyjnej, a zatem nie stosują się do nich ustępy 15f-18 art. 27 wspomnianej wyżej ustawy, regulujące postępowanie z uzyskanymi w ten sposób materiałami. Postępowanie to nie podlega jakiejkolwiek kontroli sądowej. Jakkolwiek ustawa zobowiązuje Prokuratora Generalnego do zarządzenia zniszczenia materiałów, które nie zawierają dowodów popełnienia przestępstwa albo nie są istotne dla bezpieczeństwa państwa, a Szefa ABW do ich niezwłocznego komisyjnego i protokolarnego zniszczenia, to jednak oceny, co jest istotne dla bezpieczeństwa państwa dokonuje tu urzędnik z nadania politycznego (Prokurator Generalny), a nie sąd. W dodatku nie ma obowiązku prowadzenia rejestru zarządzeń o zniszczeniu materiałów zgromadzonych w wyniku tych czynności (jako, że brak odpowiednika art. 27 ust. 16c ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu), a także rejestru postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących tych czynności (jako, że brak odpowiednika art. 27 ust. 16b ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu).

Grozi to nadużyciami. Mimo iż takie czynności mogą być zarządzone jedynie „wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej”, to np. pod pretekstem możliwości pojawienia się takiej osoby w danym pomieszczeniu (restauracji, klubie, biurze, mieszkaniu prywatnym) będzie można zarządzić tam podsłuch (czynności polegające na „uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne”), a pod pretekstem, że mogła lub może ona skorzystać z danego komputera (należącego do innej osoby lub instytucji) skopiować znajdujące się na nim dane lub zainstalować tam oprogramowanie szpiegujące (czynności polegające na „uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych”). Przy braku kontroli sądowej można sobie wyobrazić sytuację, że materiały uzyskiwane w ten sposób przez okres 3 miesięcy, mogące dotyczyć obywateli polskich, a nawet stanowić np. tajemnicę obrończą, mediatorską, adwokacką, lekarską czy dziennikarską, mogą nie zostać zniszczone, a następnie być wykorzystywane do innych celów.

**W związku z tym, proponuję skreślić w art. 9 ust. 7-10, a zamiast nich dodać ust. 7 o treści: „Przepisy art. 27 ust. 15f-18 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu stosują się odpowiednio”.**

1. Art. 43 ustawy wprowadza zmiany do ustawy Prawo telekomunikacyjne, skutkujące obowiązkiem identyfikacji tożsamości osoby chcącej korzystać z usług telekomunikacyjnych. W praktyce oznacza to obowiązek identyfikacji osoby chcącej zakupić kartę pre-paid (umożliwiającą skorzystanie z przedpłaconych usług telefonicznych). W uzasadnieniu stwierdzono, że „anonimowość tzw. przedpłaconych kart telefonicznych (pre-paid) dostarcza – jak pokazują przypadki krajowe i zagraniczne – przestępcom, w tym osobom zaangażowanym w działalność terrorystyczną, dogodnego narzędzia do komunikowania się i kamuflażu”. Nie przytoczono jednak żadnych dowodów świadczących o tym, że obowiązek identyfikacji osób utrudnia działanie terrorystom. Osoba zaangażowana w działalność terrorystyczną lub przestępczą zawsze będzie mogła skorzystać z karty zakupionej w innym kraju (w kilkunastu krajach europejskich – m. in. w Czechach, Wielkiej Brytanii, Irlandii, Austrii, Belgii, Finlandii, Szwecji, Estonii, na Litwie i Łotwie – a także w USA nie ma obowiązku identyfikacji abonentów takich usług), będzie mogła też zakupić kartę przy pomocy innej osoby (tzw. „słupa”), np. bezdomnego posiadającego dowód tożsamości. Z wypowiedzi komisarza UE Cecilii Malmström (<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2012-006014&language=EN>) oraz przedstawiciela rządu Wielkiej Brytanii (<http://www.publications.parliament.uk/pa/ld200607/ldhansrd/text/70716w0001.htm#07071618000042>) wynika, że nie stwierdzono żadnych korzyści z takiego rozwiązania.

Z drugiej strony, obowiązek identyfikacji osób chcących korzystać z kart pre-paid uderzy w osoby, dla których ważne jest zachowanie anonimowości w kontaktach – informatorzy dziennikarscy, osoby korzystające z porad prawnych, osoby ujawniające nieprawidłowości w funkcjonowaniu państwa. Służby państwowe będą mogły łatwiej identyfikować, a co za tym idzie np. podsłuchiwać, telefony osób, które z jakichś powodów narażą się władzy.

Obowiązek identyfikacji wiąże się też z dodatkowymi kosztami dla przedsiębiorców telekomunikacyjnych (ewidencjonowanie wszystkich abonentów, sprawdzanie ich tożsamości przy zwieraniu umowy). Może zostać ograniczona liczba punktów sprzedaży kart pre-paid, bo choć ustawa dopuszcza potwierdzanie tożsamości przez osoby trzecie działające w imieniu dostawcy usług, to dokonywanie tego przez np. sprzedawców w kioskach może okazać się zbyt czasochłonne.

Fakt braku obowiązku identyfikacji osób korzystających z usług telekomunikacyjnych w wielu krajach, zarówno tych silnie zagrożonych terroryzmem, jak i tych zagrożonych w małym stopniu dowodzi, że obowiązek taki nie jest powszechnie postrzegany jako narzędzie walki z terroryzmem i przestępczością. Doświadczenia np. Meksyku (gdzie przestępczość po wprowadzeniu takiego obowiązku w 2009 r. wzrosła i gdzie ostatecznie wycofano się z tego pomysłu – patrz <http://eleconomista.com.mx/sociedad/2011/04/29/senado-cancela-renaut>) pokazują, że regulacje takie nie powodują zmniejszenia zagrożeń, a nawet powodują wzrost przestępczości związanej z posługiwaniem się cudzą tożsamością.

**W związku z tym, proponuję wykreślić art. 43.**