Szanowni Państwo,

piszę w związku z projektem ustawy o działaniach antyterrorystycznych skierowanym do Sejmu 16 maja br. (druk nr 516), który 20 maja br. został skierowany do Komisji Administracji i Spraw Wewnętrznych.

Mam do tego projektu następujące uwagi:

1) Pod wspólną nazwą „zdarzenie o charakterze terrorystycznym" łączone są zdarzenia, którym należy zapobiegać (zgodnie z art. 2 „należy przez to rozumieć sytuację, 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 (Dz. U. poz. 553, z późn. zm.2)), lub zagrożenie zaistnienia takiego czynu") i obowiązek takiego zapobiegania ciąży na Szefie ABW (art. 3) oraz zdarzenia, informacja o których ma być przekazywana do ABW w celu realizacji działań antyterrorystycznych (zgodnie z art. 5 ust. 3), ale niekoniecznie takie, którym należy zapobiegać . Załączony do projektu ustawy projekt rozporządzenia o katalogu zdarzeń o charakterze terrorystycznym zawiera jedne i drugie – w tym m. in. zdarzenia takie, jak:
   "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"
   W rezultacie dochodzi do sytuacji, w której np. samo w sobie podjęcie pracy przez cudzoziemca z kraju podwyższonego ryzyka czy przesył środków finansowych z pominięciem międzynarodowych systemów bankowych (np. transfer bitcoinów) stanowią (zgodnie z art. 3 ustawy, jako „zdarzenia o charakterze terrorystycznym") zdarzenia, którym Szef ABW ma obowiązek zapobiegać, a nie jedynie zdarzenia, informacja o których może okazać się potencjalnie przydatna w realizacji działań antyterrorystycznych. Przypuszczam, że nie było to intencją autorów ustawy.
   Dodatkowo, w związku z art. 36 ustawy, pojawia się podstawa do zablokowania dostępu do całkowicie zgodnych z prawem (i niezwiązanych z faktycznym terroryzmem) materiałów zamieszczanych w Internecie - tylko na tej podstawie, że mogą one wywołać protesty jakiejś grupy wyznaniowej lub etnicznej (przykład: rysunki Mahometa) lub zostaną uznane za „ekstremistyczne" (ten termin nie jest zdefiniowany – w naukach politycznych do ideologii ekstremistycznych zalicza się zwyczajowo np. anarchizm, nacjonalizm, Nową Lewicę, czasami też libertarianizm: ideologie, których propagowanie nie jest zabronione). Mają one bowiem wówczas związek ze „zdarzeniem o charakterze terrorystycznym" wymienionym w katalogu.

W związku z tym wydaje się celowe zdefiniowane nowej kategorii „zdarzenia mogącego wiązać się ze zdarzeniami o charakterze terrorystycznym" lub „zdarzenia podwyższonego ryzyka" i użyć jej w art. 5 ustawy zamiast „zdarzenia o charakterze terrorystycznym". Katalog powinien zawierać właśnie zdarzenia z tej nowej kategorii.

2) Art. 36 projektu ustawy wprowadza do ustawy o Agencji Bezpieczeństwa Wewnętrznego poprawkę umożliwiającą sądowi w drodze postanowienia (na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego), lub, „w wypadkach nie cierpiących zwłoki" Szefowi ABW po uzyskaniu pisemnej zgody Prokuratora Generalnego, zażądania od „administratora systemu teleinformatycznego" zablokowania „dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym". Jako że pojęcie "systemu teleinformatycznego" nie jest zdefiniowane w tym projekcie, nie ma przeszkód w interpretowaniu tego zapisu tak, że zezwala on również na zarządzenie zablokowania dostępu do danych znajdujących się w Internecie na serwerach poza granicami Polski i zażądanie tego od przedsiębiorców telekomunikacyjnych świadczących usługi dostępu do Internetu (dostawców Internetu) lub zarządzających sieciami szkieletowymi (operatorów). Taka interpretacja zgodna jest z definicją systemu teleinformatycznego znajdującą się w ustawie o świadczeniu usług drogą elektroniczną ("zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)") - zgodnie z tą definicją zarówno całą ogólnoświatową sieć Internet, jak i jej fragment zarządzany przez danego przedsiębiorcę telekomunikacyjnego można uznać za system teleinformatyczny.

   Oznacza to, że projektowana ustawa daje możliwość nakazania zablokowania dostępu do dowolnych danych znajdujących się w Internecie, czyli cenzury całego Internetu, i to nawet, w przypadkach „nie cierpiących zwłoki", z dopiero następczą kontrolą ze strony sądu (w dodatku właścicielowi danych, do których dostęp został zablokowany, ani też ich użytkownikom, nie przysługuje zażalenie – takowe przysługuje jedynie Szefowi ABW i Prokuratorowi Generalnemu) . Koresponduje to z pomysłem Rejestru Stron i Usług Niedozwolonych z lat 2009-2010 (z którego rząd Donalda Tuska wycofał się pod wpływem protestów internautów i organizacji społecznych). Obarcza to przedsiębiorców telekomunikacyjnych 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 telekomunikacyjni 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)?

Albo blokowanie pozostanie fikcją (połączoną jednak z dodatkowymi obowiązkami dla przedsiębiorców telekomunikacyjnych), albo będzie wymagało poniesienia sporych wydatków (choć i tak nie będzie stuprocentowo skuteczne i zaawansowani użytkownicy będą mogli nadal omijać blokady). W tym drugim przypadku istnieje niebezpieczeństwo, że część, zwłaszcza małych, przedsiębiorców telekomunikacyjnych nie będzie mogła sprostać wymogom zapewnienia możliwości wystarczająco skutecznego blokowania danych internetowych i wypadnie z rynku, a pozostali zrekompensują koszty podwyższeniem cen. W dodatku powstanie wówczas w całej Polsce techniczna infrastruktura pozwalająca na w miarę skuteczne (z punktu widzenia przeciętnego użytkownika) blokowanie dowolnych zasobów internetowych - narzędzie, które może być wykorzystane w bardzo złych celach przez polityków. **Nawet, jeżeli obecny rząd ma dobre intencje, to za kilka lat do władzy mogą dojść inni.**

Nie zostało przedstawione przekonywujące uzasadnienie, dla którego możliwość blokowania dostępu do zasobów światowego Internetu jest konieczna dla zwalczania terroryzmu. W uzasadnieniu projektu ustawy napisano jedynie: *„Projektowane rozwiązanie ma szczególne znaczenie w kontekście przeciwdziałania działalności organizacji terrorystycznych, które wykorzystują Internet do promowania swojej ideologii, zamieszczania instruktarzu w zakresie sposobu przeprowadzania zamachów terrorystycznych oraz komunikowania się ze swoimi zwolennikami”*. Należy zwrócić jednak uwagę, że główne kanały promowania ideologii działalności organizacji terrorystycznych to albo powszechnie używane portale społecznościowe (np. Facebook, Twitter, Youtube), zablokowanie dostępu do których

oznaczałoby w praktyce zablokowanie dostępu do najpowszechniej używanych usług internetowych, albo „darknet", którego zablokowanie jest bardzo trudne, jeżeli nie niemożliwe.

W związku z tym, proponuję skreślić w projekcie ustawy zapisy w art. 36 odnoszące się do wprowadzenia w ustawie o ABW art. 32c.

Alternatywnie, proponuję zastąpić tam „administratora systemu teleinformatycznego" „przedsiębiorcą świadczącym usługi drogą elektroniczną". W ten sposób żądania blokady ograniczą się jedynie do przedsiębiorców świadczących usługi drogą elektroniczną, czyli np. udostępniających na swoich miejsce na strony internetowe (hosting), pocztę elektroniczną, usługi komunikatora (np. Gadu-Gadu) czy właścicieli stron, forów i portali. Nie będą zaś obejmowały przedsiębiorców telekomunikacyjnych. Dodatkowo proponuję wprowadzić dla owych przedsiębiorców możliwość zażalenia na postanowienie o zarządzeniu zablokowania dostępności danych czy usług.

3) Projekt ustawy w art. 30 (pkt. 1) wprowadza poprawkę do kodeksu karnego, zmieniając definicję przestępstwa o charakterze terrorystycznym - górna granica trwania kary pozbawienia wolności czynu za takie przestępstwo uznawanego zostaje obniżona z 5 do 3 lat. Oznacza to, że wiele czynów, dotychczas nie uznawanych za przestępstwa o charakterze terrorystycznym, stanie się takimi przestępstwami. Zgodnie z nową definicją, będzie można uznać za takie przestępstwo np. czynny udział w zbiegowisku publicznym (art. 254 § 1 kk), jeżeli uzna się, iż jego celem było zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej do podjęcia lub zaniechania określonych czynności – można pod to podciągnąć udział w antyrządowej manifestacji, podczas której dojdzie do np. starć z policją, obrzucenia ważnego polityka jajami czy spalenia samochodu telewizji. Przestępstwem o charakterze terrorystycznym stanie się też ujawnienie informacji zastrzeżonej przez funkcjonariusza publicznego (art. 266 § 2 kk), jeżeli uzna się, iż jego celem było zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej do podjęcia lub zaniechania określonych czynności – przykładem mogłoby być ujawnienie zastrzeżonych szczegółów negocjacji umowy TTIP przez europosła (tak jak uczynił to irlandzki europoseł Luke Flanagan).

   Jako, że przez „zdarzenie o charakterze terrorystycznym" należy zgodnie z art. 2 projektowanej ustawy rozumieć sytuację, „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 (Dz. U. poz. 553, z późn. zm.2)), lub zagrożenie zaistnienia takiego czynu", zarówno wymienioną wyżej manifestację lub ujawnienie zastrzeżonych danych, jak i nawet np. możliwość, że zapowiadana antyrządowa manifestacja będzie skutkować zamieszkami, będzie można uznać za zdarzenie o charakterze terrorystycznym (oceny nie dokonuje tu sąd, ale urzędnik) i sięgnąć po specjalne środki przewidziane tą ustawą – wprowadzić trzeci lub czwarty stopień alarmowy, zakazać zgromadzeń, skierować do pomocy Policji (np. przeciwko demonstrantom) oddziały Sił Zbrojnych itd. Możliwy (miejmy nadzieję, że przesadzony) scenariusz tutaj: http://sierp.libertarianizm.pl/?p=1380.

   W uzasadnieniu projektu ustawy napisano: *„W obecnym stanie prawnym część czynów zabronionych ściśle związanych z działalnością terrorystyczną z uwagi na swoje niskie zagrożenie karą pozbawienia wolności nie spełniały kryteriów art. 115 § 20 Kodeksu karnego"*. Nie zostało jednak wskazane, jakie to czyny. Wobec tego, argument ten należy uznać za bezzasadny.

W związku z tym, proponuję skreślić punkt 1 w art. 30 projektu ustawy, zostawiając dotychczasową definicję przestępstwa o charakterze terrorystycznym.

4) Art. 20 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). Ponownie - **nawet, jeżeli obecny rząd ma dobre intencje, to za kilka lat do władzy mogą dojść inni**.

   Jakkolwiek w uzasadnieniu ustawy znajduje się zastrzeżenie, że taki zakaz może być zarządzony, *„jeżeli jest to konieczne dla ochrony życia i zdrowia ludzi lub bezpieczeństwa publicznego"*, to w samym tekście przepisu takiego zastrzeżenia nie ma. 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. 20 jedynie do imprez masowych.