FUNDACJA PANOPTYKON

Warszawa, 10 maja 2016 r.

Stanowisko Fundacji Panoptykon[1] w sprawie projektu ustawy o działaniach antyterrorystycznych[2]

Deklarowanym celem projektowanej ustawy o działaniach antyterrorystycznych (**dalej: projekt**) jest podniesienie efektywności polskiego systemu antyterrorystycznego poprzez wzmocnienie mechanizmów koordynacji działań, doprecyzowanie zadań poszczególnych służb oraz zasad współpracy między nimi, zapewnienie możliwości skutecznych działań, zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń oraz dostosowanie przepisów karnych do nowych typów zagrożeń o charakterze terrorystycznym. W naszej opinii nie odnosimy się do propozycji dotyczących koordynacji między służbami – zwracamy jednak uwagę na te, które zwiększają uprawnienia policji i służb specjalnych – zwłaszcza Agencji Bezpieczeństwa Wewnętrznego.

Zdaniem Fundacji Panoptykon wiele spośród proponowanych rozwiązań narusza Konstytucję RP. Podstawowym problemem jest szeroka definicja przestępstwa o charakterze terrorystycznym, co umożliwi ABW stosowanie zawartych w ustawie uprawnień nie tylko w sprawach dotyczących najpoważniejszych przestępstw. Projekt zakłada także, niedopuszczalne w demokratycznym państwie prawa, odbieranie prawa do ochrony prywatności osobom nieposiadającym polskiego obywatelstwa. Zwracamy także uwagę na umożliwienie ABW zdalnego, w praktyce nieograniczonego i niekontrolowanego dostępu do publicznych baz danych, a także systemów monitoringu wizyjnego. Rosnący zakres danych na temat obywateli, jakie może pozyskiwać ABW, uwypukla konieczność powołania organu, który będzie kontrolował przetwarzanie przez nią danych osobowych. Projekt ogranicza także wolność słowa i dostęp do informacji w Internecie, przyznając ABW możliwość blokowania dostępu do (bliżej nieokreślonych) danych informatycznych. Wreszcie, zwracamy uwagę na nieuzasadnione ograniczenie prawa do anonimowej komunikacji za pomocą tzw. przedpłaconych kart telefonicznych, a także niejasności związane z prowadzeniem przez ABW wykazu osób stwarzających zagrożenie terrorystyczne.

1. Tryb prac

Przed przejściem do omówienia najbardziej kontrowersyjnych rozwiązań zawartych w projekcie, zwracamy uwagę na tryb prac. Zgodnie z oceną skutków regulacji ze względu na konieczność zapewnienia bezpieczeństwa planowanych w lipcu 2016 r. wydarzeń o międzynarodowym charakterze: Światowych Dni Młodzieży i Wizyty w Polsce Ojca Świętego Franciszka oraz Szczytu Organizacji Traktatu Północnoatlantyckiego, przyjęto szczególny tryb procedowania projektu. W praktyce oznacza to, że projekt nie został poddany konsultacjom publicznym:

[1] Stanowisko przygotowane przez Wojciecha Klickiego.
[2] Projekt ustawy o działaniach antyterrorystycznych w wersji z 5 maja 2016 r.

nie umożliwiono obywatelom ani organizacjom społecznym, a także instytucjom takim jak Rzecznik Praw Obywatelskich czy Generalny Inspektor Ochrony Danych Osobowych, przedstawienia opinii na etapie rządowego procesu legislacyjnego. Negatywnie wpływa to na jakość stanowionego prawa. Jednocześnie, uzasadnienie projektu nie wyjaśnia, dlaczego opracowanie potrzebnych (ze względu na ww. wydarzenia) szczegółowych procedur działania służb w reakcji na zdarzenia o charakterze terrorystycznym nie było możliwe w oparciu o dotychczasowe przepisy.

W przypadku tej materii, ze względu na szczególnie wysoki stopień ingerencji w prawa jednostki, bardzo ważnie jest tworzenie przepisów w sposób przemyślany i angażujący jak najszerszą liczbę obywateli i ekspertów.

Zwracamy również uwagę na tempo prac nad projektem i zakładany termin wejścia w życie ustawy. Wiele proponowanych rozwiązań (np. dotyczących nowego trybu uzyskiwania przez ABW dostępu do rejestrów publicznych) wymaga wdrożenia technicznego. Z kolei przyznanie ABW wiodącej i koordynacyjnej roli w zwalczaniu terroryzmu wymusza stworzenie nowych procedur współpracy między nią a pozostałymi służbami. W tym kontekście rodzi się pytanie, czy nowe rozwiązania będą w pełni funkcjonalne już w lipcu podczas wydarzeń, które wykorzystywane są do uzasadnienia konieczności przyjęcia przepisów w pilnym trybie.

Tryb prac – tj. brak konsultacji publicznych czy konferencji uzgodnieniowej – utrudnia także ocenę konkretnych rozwiązań zawartych w projekcie. Uzasadnienie projektu w wielu punktach sprowadza się do przedstawienia proponowanego rozwiązania, natomiast nie odpowiada na pytanie o jego niezbędność, a także nie wskazuje, czy były rozważane inne możliwości, mniej ingerujące w prawa jednostki. Niektóre propozycje zawarte w projekcie (np. w zakresie przyznania ABW możliwości pozyskiwania danych ze zbiorów publicznych w drodze teletransmisji[3]) nie są nawet wspomniane w uzasadnieniu. Możliwość zgłoszenia merytorycznych uwag autorom projektu i uzyskania od nich niezbędnych wyjaśnień z pewnością wpłynęłaby pozytywnie na poziom i kierunki debaty publicznej.

2. Definicja przestępstw o charakterze terrorystycznym

Kluczowe znaczenie dla oceny zakresu, celu i skutków projektu ma definicja przestępstwa i zdarzenia o charakterze terrorystycznym. Zgodnie z projektem[4], przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, popełniony w jednym z celów wskazanych w Kodeksie karnym, np. w celu poważnego zastraszenia wielu osób lub zmuszenia organu władzy publicznej do podjęcia lub zaniechania określonych czynności.

W takim ujęciu – pod warunkiem spełnienia wymogu dotyczącego celu – przestępstwami o charakterze terrorystycznym mogą być np.:

- znieważenie Prezydenta Rzeczypospolitej Polskiej (art. 135 § 2 Kodeksu karnego);
- naruszenie nietykalności cielesnej funkcjonariusza publicznego (art. 222 § 1 Kodeksu karnego);
- utrudnienie dostępu do danych informatycznych (art. 268a Kodeksu karnego).

[3] Por. art. 32 projektu – zmiany w ustawie o ABW – pkt 7.
[4] Por. art. 28 projektu – zmiany w Kodeksie karnym – pkt 1.

W naszej ocenie projekt umożliwia uznanie za przestępstwo o charakterze terrorystycznym wiele czynów zabronionych, których społeczna szkodliwość jest znacznie niższa od faktycznych zamachów terrorystycznych. Za taki czyn mogłoby zostać uznane np. przestępstwo naruszenia nietykalności cielesnej funkcjonariusza popełnione w celu zmuszenia go do zaniechania określonych czynności.

Niezwykle szeroka definicja przestępstwa o charakterze terrorystycznym rodzi następujące wątpliwości:

a. Szczególne uprawnienia służb nie tylko w najpoważniejszych sprawach

Definicja zdarzenia[5] oraz przestępstwa o charakterze terrorystycznym ma kluczowe znaczenie przy możliwości stosowania przez ABW nowych uprawnień, o których mowa niżej (np. żądanie zablokowania danych informatycznych, możliwość stosowania podsłuchu). Jest to istotne dla oceny zgodności proponowanych rozwiązań z zasadą proporcjonalności (art. 31 ust. 3 Konstytucji).

Przepisy nie gwarantują, że zwiększone uprawnienia ABW będą wykorzystywane w absolutnie wyjątkowych sytuacjach. Drastyczne ograniczenie praw i wolności będzie możliwe również w przypadkach, w których nie jest to konieczne i proporcjonalne do stopnia zagrożenia. Przykładowo możliwe będzie zastosowanie tymczasowego aresztowania – do którego **samoistną przesłanką** będzie przygotowanie do popełnienia przestępstwa o charakterze terrorystycznym – wobec sprawcy przestępstwa znieważenia Prezydenta RP[6].

Jeszcze w kontekście dotychczasowej definicji przestępstwa o charakterze terrorystycznym zwracano uwagę[7], że w przypadku pojedynczego sprawcy cele, jakimi kieruje się w swoich działaniach, często możliwe są do rozpoznania dopiero *ex post*. Oznacza to, że organy ścigania skazane są na „dość intuicyjne i uznaniowe określanie, czy dany czyn zabroniony posiada rys terrorystyczny, czy też w konkretnym przypadku go brak”[8]. A zatem ABW będzie samodzielnie i arbitralnie oceniać, czy doszło (lub może dojść) do przestępstwa o charakterze terrorystycznym.

b. Ryzyko ograniczenia wolności zgromadzeń

Zgodnie z projektem w przypadku zagrożenia przestępstwem o charakterze terrorystycznym można wprowadzić jeden z czterech stopni alarmowych[9]. Wprowadzenie trzeciego lub czwartego stopnia alarmowego wiąże się z możliwością zarządzenia przez ministra właściwego do spraw wewnętrznych zakazu odbywania zgromadzeń publicznych lub imprez masowych na wskazanym obszarze.

Wprowadzenie trzeciego stopnia możliwe jest m.in. w przypadku pozyskania informacji o planowanym zdarzeniu o charakterze terrorystycznym, którego skutki mogą dotyczyć obywateli polskich przebywających za granicą albo uzyskania informacji o planowanym zdarzeniu o charakterze terrorystycznym na terenie RP.

---

[5] Zgodnie z art. 2 pkt 7 projektu przez zdarzenie o charakterze terrorystycznym należy rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym lub zagrożenie zaistnienia takiego czynu.

[6] Por. art. 24 ust. 2 projektu.

[7] Przesławski, Tomasz, *Cel w konstrukcji przestępstwa terrorystycznego*, Prokuratura i Prawo 5/2009.

[8] Brzezińska, Joanna, *Z rozważań o terrorystycznym charakterze przestępstwa*, NKPK 2008/22.

[9] Por. art. 14 projektu, zgodnie z którym wprowadzone mogą być cztery stopnie alarmowe, a także cztery stopnie alarmowe CRP.

Nie kwestionując możliwości ograniczenia wolności zgromadzeń w niektórych sytuacjach, zwracamy uwagę, że zaproponowane rozwiązania nie gwarantują wyjątkowości zastosowania takiego środka i dają ministrowi właściwemu do spraw wewnętrznych ogromną, dyskrecjonalną władzę. Wiąże się to z, omawianą już, szeroką definicją przestępstwa o charakterze terrorystycznym.

3. Cudzoziemcy – brak ochrony prywatności

Projekt umożliwia[10] „w celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym" zarządzenie wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, niejawnych czynności, takich jak uzyskiwanie i utrwalanie treści rozmów. Są to czynności tożsame ze znaną już polskiemu prawodawstwu kontrolą operacyjną. Zasadniczą różnicą jest jednak tryb ich podjęcia: w przypadku osób nieposiadających polskiego obywatelstwa Szef ABW będzie mógł samodzielnie zarządzić takie czynności, informując jedynie Ministra Koordynatora Służb Specjalnych oraz Prokuratora Generalnego. Nie będzie natomiast konieczności uzyskania zgody sądu na prowadzenie tych czynności.

Propozycja ta rodzi fundamentalne wątpliwości.

a. Bezzasadne odebranie prawa do prywatności osobom nieposiadającym polskiego obywatelstwa

Projektodawcy podnoszą w uzasadnieniu projektu, że Trybunał Konstytucyjny[11] dopuszcza odmienne określenie przesłanek pozyskiwania danych i postępowania z nimi w stosunku do osób niepodlegających polskiemu prawu. Należy jednak pamiętać, że przepisy dotyczące cudzoziemców także muszą spełniać wymóg proporcjonalności, o którym mowa w art. 31 ust. 3 Konstytucji RP.

Kontrola operacyjna jest najdalej ingerującym w prywatność jednostki uprawnieniem ABW i – jak wynika z bogatego orzecznictwa zarówno Trybunału Konstytucyjnego[12], jak i Europejskiego Trybunału Praw Człowieka – musi podlegać ścisłej kontroli sądu. Jak bowiem zwrócił uwagę ETPC w wyroku w sprawie Zakharow przeciwko Rosji[13], w przypadku tego typu uprawnień służb niezbędna jest kontrola zewnętrzna względem służb i administracji rządowej.

W naszej opinii wynikająca z przytoczonego w uzasadnieniu projektu orzeczenia Trybunału Konstytucyjnego dopuszczalność różnego traktowania ze względu na obywatelstwo nie oznacza możliwości prowadzenia kontroli operacyjnej względem cudzoziemców bez jakiejkolwiek zewnętrznej kontroli. Wprowadzenie takiego rozwiązania de facto oznaczałoby pozbawienie ich jakiejkolwiek ochrony przed nadmierną i nieuzasadnioną ingerencją w prywatność, a nie tylko obniżenie obowiązującego w stosunku do nich standardu ochrony.

Dodatkowo, w przeciwieństwie do przepisów umożliwiających prowadzenie kontroli operacyjnej wobec osób posiadających polskie obywatelstwo, projekt umożliwia prowadzenie wspomnianych czynności w każdej sytuacji, a nie tylko wówczas „gdy inne środki okazały się

[10] Por. art. 8 projektu.
[11] Por. wyrok TK z 30 lipca 2014 r., sygn. K 23/11.
[12] Por. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04.
[13] Por. wyrok z 4 grudnia 2015 r. w sprawie Roman Zacharow przeciwko Rosji (skarga nr 47143/06).

bezskuteczne albo będą nieprzydatne”[14]. Zasada subsydiarności, zgodnie z którą należy stosować środki możliwie najmniej ingerujące w prawa jednostki, jest jednym z podstawowych wymogów, które powinny być spełnione w przypadku wkraczania w prawa jednostki: stosowanie głębiej ingerujących środków dopuszczalne jedynie wówczas, gdy inne – mniej uciążliwe – okazały się nieprzydatne.

Konstytucja przyznaje każdemu – bez względu na posiadane obywatelstwo – prawo do ochrony prywatności. Ze względu na brak kontroli sądowej nad stosowaniem wobec cudzoziemców kontroli operacyjnej, a także brak zasady subsydiarności, rozwiązanie zawarte w projekcie ustawy jest niezgodne z Konstytucją RP, a także Konwencją o ochronie praw człowieka i podstawowych wolności.

b. Nieuzasadnione wyeliminowanie nadzoru sądowego

Zwracamy uwagę, że w obecnym stanie prawnym istnieje możliwość zastosowania kontroli operacyjnej wobec cudzoziemców. Wymagana obecnie zgoda sądu w sytuacjach niecierpiących zwłoki może być wyrażona już po rozpoczęciu kontroli operacyjnej. Jest to kluczowy mechanizm pozwalający uprawnionym podmiotom reagować na dynamicznie zmieniającą się sytuację – bez względu na fakt, czy osoba podejrzana ma polskie obywatelstwo. W tym kontekście **rażący jest brak jakiekolwiek uzasadnienia dla zróżnicowania poziomu ochrony ze względu na posiadane obywatelstwo, w szczególności wyeliminowania nadzoru sądu nad stosowaniem kontroli operacyjnej**.

c. Fikcyjność zróżnicowania poziomu ochrony – ryzyko nadużyć również w stosunku do obywateli RP

Zgodnie z projektem ABW będzie mogła prowadzić kontrolę operacyjną bez konieczności uzyskania zgody sądu m.in. „w celu rozpoznawania” przestępstw o charakterze terrorystycznym. Zwracamy uwagę, że kontrola operacyjna może być prowadzona wobec osoby, której tożsamość – a tym samym obywatelstwo – nie jest znana. Rodzi to ryzyko obniżenia standardu ochrony także względem polskich obywateli. Dotyczy to m.in. sytuacji, w której obywatel polski jest jedynie rozmówcą cudzoziemca.

Jak zwrócił uwagę w analogicznej sytuacji Europejski Trybunał Praw Człowieka[15], system pozwalający np. na przechwytywanie połączeń bez konieczności przedstawienia dostawcy usług telekomunikacyjnych zezwolenia, jest szczególnie **podatny na nadużycia**. Sprawia on bowiem, że tajne służby posiadają możliwość obejścia procedury wydawania zezwoleń i przechwytywania połączeń komunikacyjnych bez uzyskania zgody sądu. Zdaniem ETPC, konieczność zabezpieczenia przed samowolą i nadużyciami w tym obszarze jest szczególnie istotna.

Zgodnie z projektem[16] przedłużanie kontroli operacyjnej zarządzonej bez uzyskania zgody sądu następuje na „zasadach ogólnych” (czyli za zgodą sądu). Niemniej projekt nie zawiera gwarancji wykluczających ominięcie tego wymogu poprzez ponowne rozpoczęcie kontroli operacyjnej na podstawie tych samych przesłanek, względem tej samej osoby, zamiast uzyskania zgody sądu na przedłużenie czynności.

[14] Por. art. 19 ustawy o policji.
[15] Por. wyrok z 4 grudnia 2015 r. w sprawie Roman Zacharow przeciwko Rosji (skarga nr 47143/06).
[16] Por. art. 8 ust. 5 projektu.

4. Dostęp do rejestrów publicznych i obrazu z monitoringu wizyjnego

Zgodnie z projektem[17], ABW w celu zapobiegania zdarzeniom o charakterze terrorystycznym może nieodpłatnie uzyskać dostęp do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach. Ich lista (katalog ma charakter otwarty) obejmuje m.in. Zakład Ubezpieczeń Społecznych czy podległe Ministrowi Finansów urzędy skarbowe. ABW uzyska także dostęp do obrazu zdarzeń rejestrowanego przez kamery umieszczone w obiektach użyteczności publicznej, przy drogach publicznych i innych miejscach publicznych „z uwzględnieniem zasad i trybu określonych w art. 34 ustawy o ABW". Z kolei do wspomnianego art. 34 ustawy o ABW projekt dodaje ust. 2a, zgodnie z którym udostępnianie danych następuje w drodze teletransmisji, bez konieczności każdorazowego przedstawiania imiennego upoważnienia. ABW musi jedynie zagwarantować możliwość odnotowania w systemie: kto, kiedy, w jakim celu oraz jakie dane uzyskał, a także zagwarantować zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania.

ABW uzyskuje nieograniczony, niekontrolowany dostęp do wszystkich publicznych baz danych.

W naszej ocenie już na podstawie obowiązujących przepisów ABW miało możliwość uzyskania dostępu do wszystkich publicznych baz danych. Wydaje się zatem, że istotą zmiany jest **tryb** i **zakres** pozyskiwania informacji. Projekt umożliwia ABW szybkie i zdalne pobieranie nieograniczonych ilości danych o dowolnej liczbie osób, co w praktyce może się przekładać na tworzenie rozbudowanych profili osobowych nie tylko w stosunku do podejrzanych. Pozyskiwanie tak szerokiego zakresu informacji przez ABW nie podlega żadnej kontroli, w szczególności Generalnego Inspektora Ochrony Danych Osobowych.

Wyłączenie kompetencji GIODO do kontroli zgodności przetwarzania przez służbę specjalną danych osobowych było przedmiotem kontroli Trybunału Konstytucyjnego w sprawie o sygn. K 54/07[18] (dotyczącej ustawy o CBA). Zdaniem Trybunału „ściśle określone ustawowo zastosowanie w demokratycznym państwie prawnym innych niż powszechnie obowiązujące, szczególnych reguł postępowania ze zbiorami danych przetwarzanych przez służby specjalne nie budzi – co do zasady – istotnych wątpliwości konstytucyjnych". Oznacza to, że nie ma przeszkód, by kontrola przetwarzania danych przez służby specjalne była sprawowana przez inny organ, niż GIODO. W związku z tym uważamy, że niezbędne jest stworzenie niezależnego organu o kompetencjach zbliżonych do GIODO, sprawującego **zewnętrzną kontrolę** nad przetwarzaniem danych osobowych przez wszystkie służby specjalne, bądź przyznanie tej kompetencji samemu GIODO.

Wobec perspektywy zdalnego dostępu ABW do publicznych baz danych i systemów monitoringu, wprowadzenie mechanizmu kontroli przetwarzania przez tę służbę danych osobowych staje się bardzo pilnym wyzwaniem.

[17] Por. art. 10 projektu.
[18] Por. wyrok Trybunału Konstytucyjnego z 23 czerwca 2009 r., sygn. K 54/07.

5. Obowiązkowa rejestracja tzw. przedpłaconych kart telefonicznych

Zgodnie z projektem[19] abonenci korzystający z usług telefonicznych zobowiązani będą do podania operatorowi telekomunikacyjnemu imienia i nazwiska, a także numeru PESEL. Dostawca będzie mógł rozpocząć świadczenie usług telekomunikacyjnych nie wcześniej, niż po potwierdzeniu zgodności podanych danych z danymi zawartymi w dokumencie poświadczającym tożsamość. Inną możliwością weryfikacji tożsamości będzie uwierzytelnienie w bankowym systemie teleinformatycznym lub za pomocą bezpiecznego podpisu elektronicznego.

Zwracamy uwagę przede wszystkim na to, że skuteczność proponowanego mechanizmu w walce z poważną przestępczością jest kontrowersyjna. ABW, policja i inne służby uprawnione są do pozyskiwania danych telekomunikacyjnych, w tym danych o lokalizacji i wykazu połączeń telefonicznych, na podstawie których można ustalić nie tylko tożsamość użytkownika telefonu, ale także skonstruować jego szczegółowy profil i ustalić z dużym prawdopodobieństwem, z jakich urządzeń i kart SIM korzysta ta sama osoba (lub osoby kontaktujące się w ramach siatki przestępczej). Należy w tym kontekście zwrócić uwagę na wypowiedź unijnej komisarz do spraw handlu Cecilii Malmström, która wskazała, że nie ma obecnie żadnych dowodów na zwiększenie skuteczności organów ścigania w związku z wprowadzeniem obowiązku rejestracji przedpłaconych kart telefonicznych[20].

Podczas gdy korzyści płynące z nałożenia obowiązku rejestracji przedpłaconych kart telefonicznych wydają się wątpliwe, z pewnością wpłynie on na ograniczenie prawa do anonimowej komunikacji, szczególnie ważnego np. dla adwokatów i dziennikarzy. Z perspektywy przedstawicieli zawodów zaufania publicznego niezarejestrowane karty telefoniczne pełnią ważną funkcję, wspierając ochronę danych osobowych ich klientów lub źródeł (dziennikarskich).

6. Blokowanie danych informatycznych

Projekt przewiduje[21] rozszerzenie kompetencji Szefa ABW o możliwość zarządzenia – albo zażądania od administratora systemu teleinformatycznego – zablokowania danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym. Wniosek Szefa ABW wymaga jedynie pisemnej zgody Prokuratora Generalnego. Projekt przewiduje kontrolę sądu dopiero w terminie 5 dni od faktycznego zablokowania treści.

Korzystanie z Internetu stało się w społeczeństwie informacyjnym kluczową formą realizowania wolności słowa, gwarantowanej zarówno przez Konstytucję RP, jak i Konwencji o ochronie praw człowieka i podstawowych wolności. Ewentualne ograniczenia tego konstytucyjnego prawa muszą spełniać zasady proporcjonalności. Naszym zdaniem **proponowany mechanizm** narusza te standardy i powinien zostać wykreślony z projektu.

Poniżej przedstawiamy najistotniejsze zarzuty:

[19] Por. art. 38 projektu.
[20] Por. P-006014/2012 Answer given by Ms Malmström on behalf of the Commission (17.7.2012).
[21] Art. 34 ustawy – dodany do ustawy o ABW art. 32c.

a. Brak jasności co do tego, jakie treści można zablokować

Pojęcie „dane informatyczne" może dotyczyć zarówno konkretnych treści, jak i całych portali internetowych, w tym również społecznościowych. Oznacza to, że zablokowane mogą być zarówno komunikatory (Facebook, Twitter), jak i sieci anonimowej wymiany danych. Wydaje się to szczególnie prawdopodobne w sytuacji, gdy ze względów technicznych niezwłoczne zablokowanie wybranych, kontrowersyjnych komunikatów przez Szefa ABW nie będzie możliwe (np. wobec odmowy współpracy przez administratora konkretnego portalu lub braku możliwości nawiązania szybkiego kontaktu).

Niejasne pozostaje także, jak powinno być rozumiane kryterium „związku ze zdarzeniem o charakterze terrorystycznym". Zgodnie z projektem wystarczającą podstawą do zablokowania danych informatycznych jest ich związek ze zdarzeniem, które powstało na skutek przestępstwa o charakterze terrorystycznym. W tym kontekście należy przypomnieć uwagi dotyczące szerokiego zakresu tego pojęcia (por. punkt 2 stanowiska). Ponadto niejasne jest, na ile bezpośredni powinien być **związek** pomiędzy przestępstwem a danymi informatycznymi i czy blokowanie może objąć np. przekazy medialne dotyczące zdarzenia o charakterze terrorystycznym. W naszej opinii otwiera to pole do arbitralnych działań Szefa ABW.

b. Brak związku z ochroną infrastruktury krytycznej

Uzasadnienie projektu, w części dotyczącej nowych uprawnień Szefa ABW, odnosi się do potrzeby lepszej ochrony systemów teleinformatycznych, będących elementami krytycznej infrastruktury państwa. Nie kwestionując tej potrzeby, nie dostrzegamy związku pomiędzy ochroną infrastruktury krytycznej z zaproponowanym mechanizmem blokowania danych informatycznych, które – jak wykazujemy powyżej – mogą być rozumiane bardzo szeroko, w szczególności jako informacje publikowane przez obywateli na komercyjnych portalach internetowych lub własnych blogach.

c. Brak skutecznej i adekwatnej kontroli sądowej

Projekt umożliwia Szefowi ABW za zgodą Prokuratora Generalnego arbitralne zablokowanie każdej treści dostępnej w Internecie, bez względu na jej charakter czy dostępność. Ze względu na ogromne ryzyko dla wolności słowa i dostępu do informacji w sieci, kontrola sądu nad realizacją tego uprawnienia powinna mieć realny i niezwłoczny charakter. Tymczasem blokada dostępności danych informatycznych miałaby być znoszona dopiero w przypadku nieudzielenia przez sąd zgody na zarządzenie zablokowania określonych danych informatycznych w terminie 5 dni. Biorąc pod uwagę dynamikę wymiany informacji we współczesnym świecie, 5 dni oczekiwania na następczą kontrolę sądową nie stanowi realnej gwarancji ochrony wolności słowa.

d. Nieprzyjęcie zasady subsydiarności

Ustawa za wystarczającą przesłankę do zablokowania dostępu do danych uznaje „związek ze zdarzeniem o charakterze terrorystycznym" – bez wprowadzenia tzw. zasady subsydiarności, która wymusiłaby zastosowanie blokady tylko w sytuacjach, w których inne środki okazały się lub byłyby nieskuteczne. W tym kontekście oznacza to przede wszystkim obowiązek podjęcia próby doprowadzenia do usunięcia treści u źródła. Kryterium subsydiarności powinno być także kluczowe na etapie podejmowania przez Sąd Okręgowy decyzji co do dopuszczalności blokowania (lub jego przedłużenia).

e. Brak skutecznych mechanizmów odwoławczych dla zainteresowanych stron

Przepisy stawiają Szefa ABW w wyraźnie uprzywilejowanej pozycji względem innych podmiotów zainteresowanym postępowaniem w sprawie zablokowania dostępu do danych: postanowienie Sądu Okręgowego w Warszawie, dotyczące zarówno zatwierdzenia żądania Szefa ABW, jak i przedłużenia blokowania danych informatycznych, może być zaskarżone wyłącznie przez Szefa ABW. Projekt ustawy nie przewiduje nawet dostarczenia postanowienia sądu innym podmiotom (por. ust. 6, zgodnie z którym „Szef ABW niezwłocznie informuje administratora systemu teleinformatycznego o treści prawomocnego postanowienia sądu"). Należy zwrócić uwagę na konieczność zapewnienia pozycji równej Szefowi ABW zarówno administratorowi systemu teleinformatycznego, jak i osobie, której dane miałyby być blokowane.

f. Brak przejrzystości

Ustawa nie przewiduje żadnych mechanizmów gwarantujących przejrzystość działań Szefa ABW. Osoba, której dane zostaną zablokowane, nie zostanie o tym nawet poinformowana. Poza iluzoryczną, następczą kontrolą sądową, nie przewidziano żadnych mechanizmów społecznej kontroli np. w postaci publikowania zbiorczych danych nt. adresów, które podlegały blokowaniu na wniosek Szefa ABW.

g. Niebezpieczny precedens

Mechanizm blokowania danych informatycznych nie polega na usunięciu treści u źródła, ale na utrudnieniu dostępu do nich, najczęściej poprzez filtrowanie zapytań o dostęp do danego adresu internetowego na poziomie operatora telekomunikacyjnego. W praktyce może to oznaczać konieczność stworzenia i utrzymywania (przez operatorów telekomunikacyjnych) infrastruktury filtrującej wszystkie zapytania użytkowników Internetu w Polsce. Ponadto, wprowadzenie takiego mechanizmu na potrzeby realizacji opisywanych uprawnień Szefa ABW, dodatkowo bez efektywnej kontroli sądowej, może otworzyć drzwi do blokowania innych rodzajów treści, np. pornograficznych czy hazardowych.

h. Możliwość czasowego zablokowania danych informatycznych jako ryzyko biznesowe

Samo wprowadzenie rozwiązań przewidzianych w projekcie (nawet zakładając, że Szef ABW nie skorzysta ze swoich uprawnień) może mieć poważne skutki dla finansowania i prowadzenia działalności gospodarczej w Internecie. Z perspektywy przedsiębiorcy, prawna możliwość zablokowania przez organ państwa dostępu do jego danych informatycznych na okres 5 dni (lub dłuższy) oznacza ryzyko sparaliżowania biznesu i poważnych strat. Kalkulacja tego ryzyka i związanych z nim strat finansowych może, w niektórych przypadkach, uniemożliwić lub utrudnić zdobycie finansowania na rozpoczęcie lub rozwinięcie tego typu działalności w Polsce.

7. Wykaz osób niebezpiecznych

Zgodnie z projektem[22] Szef ABW w celu zapobiegania zdarzeniom o charakterze terrorystycznym prowadzi wykaz, który ma zawierać informacje m.in. o osobach podejrzewanych o popełnienie przestępstw o charakterze terrorystycznym lub osobach, „wobec których istnieje uzasadnione podejrzenie, że mogą prowadzić działania zmierzające do popełnienia przestępstwa

[22] Por. art. 6 projektu.

o charakterze terrorystycznym". Informacje z wykazu mogą być przekazywane innym służbom, a także innym organom administracji publicznej.

Naszym zdaniem przywołana charakterystyka osób, które mogą znaleźć się w prowadzonym przez ABW wykazie, ma zbyt ogólny i uznaniowy charakter. W praktyce da ona ABW możliwość podjęcia arbitralnej decyzji, czyje nazwisko zostanie tam umieszczone. Uznaniowość powyższej decyzji pogłębia fakt, że proponowane przepisy regulujące sposób działania wykazu nie przewidują mechanizmu gwarantującego poszanowanie praw jednostki. Projekt nie precyzuje również, czy wpis do wykazu wywołuje jakieś konsekwencje dla jednostki.

Cel i charakter projektowanego wykazu osób niebezpiecznych upodobniają go do tzw. czarnych list osób i organizacji podejrzewanych o terroryzm lub współpracę z organizacjami terrorystycznymi opracowanych przez Organizację Narodów Zjednoczonych[23] i Unię Europejską. Listy te były przedmiotem krytyki Rady Europy, która w 2008 r. przygotowała raport w tej sprawie[24]. Zgromadzenie Parlamentarne Rady Europy wydało rekomendację[25], w której wskazało, że nawet przy implementacji sankcji ONZ i Unii Europejskiej związanych ze zwalczaniem terroryzmu niezbędne jest przestrzeganie minimalnego standardu ochrony praw człowieka wynikającego z Konwencji o ochronie praw człowieka i podstawowych wolności.

Uwagi te powinny znaleźć zastosowanie również do projektowanego wykazu. W związku z tym konieczne jest **doprecyzowanie kryteriów umieszczania w nim danych konkretnych** osób, jak również określenie okoliczności, w których osoba, której dotyczy wpis, może uzyskać informacje o tym fakcie. Niezbędne jest ponadto zagwarantowanie środków prawnych pozwalających na weryfikację słuszności dokonanego wpisu oraz doprecyzowanie okresu, przez który przetwarzane będą dane umieszczonych w nim osób. Te kwestie powinny zostać uregulowane w dokumencie o randze ustawowej, a nie w zarządzeniu Szefa ABW, ponieważ mają one istotne znaczenie dla zapewnienia przestrzegania praw jednostki.

***

Ze względu na tempo prac nad projektem, brak konsultacji publicznych, a także misję Fundacji Panoptykon przedstawiona opinia nie omawia szczegółowo wszystkich zastrzeżeń i problemów związanych z projektem.

[23] Rezolucje Rady Bezpieczeństwa nr 1267/1999 z 15 października 1999 r., nr 1333/2000 z 19 grudnia 2000 r. oraz 1390/2002 z 16 stycznia 2002 r.
[24] http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=11749&Language=en.
[25] http://assembly.coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=17618&lang=EN.