



RADA FUNDACJI

Halina Bortnowska-Dąbrowska Marek Antoni Nowicki
Jerzy Ciemniowski Teresa Romer
Janusz Grzelak Mirosław Wyrzykowski
Michał Nawrocki

ZARZĄD FUNDACJI

Prezes: Danuta Przywara
Wiceprezes: Maciej Nowicki
Sekretarz: Piotr Kładoczny
Skarbnik: Elżbieta Czyż
Członek Zarządu: Janina A. Kłosowska

Warszawa, dnia 18 maja 2016 r.

987/2016/MPL

Szanowny Pan
Marek Kuchciński
Marszałek Sejmu

Uwagi Helsińskiej Fundacji Praw Człowieka
do projektu ustawy o działaniach antyterrorystycznych
(druk sejmowy nr 516)

Helsińska Fundacja Praw Człowieka (dalej: HFPC) pragnie przedstawić opinię w przedmiocie projektu ustawy o działaniach antyterrorystycznych (druk sejmowy nr 516), przyjętego przez Radę Ministrów w dniu 10 maja 2016 r. i skierowanego do Sejmu w dniu 16 maja 2016 r. Z uwagi na niezwykle pospieszny tryb procedowania nad projektem ustawy, niniejsza opinia ograniczy się do najważniejszych zagadnień zawartych w projekcie.

1. Uwagi ogólne

Podstawowe założenia ustawy antyterrorystycznej zostały zaprezentowane podczas konferencji prasowej Ministra Spraw Wewnętrznych i Administracji oraz Ministra Koordynatora ds. służb specjalnych w dniu 24 marca 2016 r. Konferencja ta miała charakter informacyjny, zaś same założenia projektu ustawy – których opracowanie jest wymagane na gruncie Regulaminu pracy Rady Ministrów¹ – nie były przedmiotem jakichkolwiek konsultacji społecznych. Również sam projekt ustawy nie został poddany rzeczowym konsultacjom społecznym. Co więcej, projekt został wpisany do wykazu prac legislacyjnych i programowych Rady Ministrów dopiero 21 kwietnia 2016 r. (projekt nr UD 60), mimo że informacje o prowadzonych pracach dostępne były od kilku miesięcy².

¹ Rozdział 5. uchwały z 29 października 2013 r. - Regulamin pracy Rady Ministrów (M.P. poz. 979, ze zm.).

² M.in. komunikat „Posiedzenie Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych” zamieszczony na stronie internetowej MSWiA (komunikat z 27 stycznia 2016 r., dostępny: <https://mswia.gov.pl/pl/aktualnosci/14120,Posiedzenie-Miedzyresortowego-Zespołu-ds-Zagrozen->

Już w styczniu 2016 r. podczas spotkania Rady ds. Cyfryzacji, minister Maciej Wąsik, Sekretarz Kolegium ds. Służb Specjalnych zapowiadał, że projekt ustawy o działaniach antyterrorystycznych, nad którymi wówczas pracowała Rada Ministrów, zostanie poddany szerokim konsultacjom społecznym³.

Taki tryb procedowania jest nieadekwatny do powagi celu projektowanej ustawy, tj. próby zapewnienia bezpieczeństwa publicznego. Zagwarantowanie tak fundamentalnej wartości, jaką jest bezpieczeństwo publiczne, powinno wiązać się z szeroką dyskusją publiczną na temat kierunków zmian prawa, które mają doprowadzić do jego realizacji. Ignorowanie przez władzę publiczną obowiązku prowadzenia takiej dyskusji może mieć negatywnie konsekwencje dla zapewnieniu tego bezpieczeństwa. Z kolei termin wejścia w życie ustawy określony jako dzień następujący po dniu ogłoszenia ustawy w Dzienniku Ustaw, narusza zasadę przewidywalności i pewności prawa. Odpowiednio zakreślone *vacatio legis* jest niezbędne dla zagwarantowania sprawnych działań realizowanych przez organy publiczne. Zabezpiecza również obywateli przed nagłymi zmianami w ich sytuacji prawnej, do której nie mogli się wcześniej przygotować. W ocenie Helsińskiej Fundacji Praw Człowieka, zarówno tryb prac nad projektem ustawy, jak również brak adekwatnego *vacatio legis* powoduje, że tak uchwalone prawo narusza zasadę demokratycznego państwa prawnego.

2. Cel ustawy

Cele, które mają być zrealizowane dzięki przyjęciu ustawy o działaniach antyterrorystycznych zostały zakreślone szeroko, m.in.: podniesienie skuteczności polskiego systemu antyterrorystycznego oraz zwiększenie bezpieczeństwa wszystkich obywateli RP poprzez:

1. doprecyzowanie mechanizmów koordynacji działań;
2. doprecyzowanie zadań poszczególnych służb i organów oraz zasad współpracy między nimi;
3. zapewnienie możliwości skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego;
4. zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń;
5. dostosowanie przepisów karnych do nowych typów zagrożeń o charakterze terrorystycznym.

Jednocześnie projektodawca wskazał, że obecne przepisy dotyczące przeciwdziałania terroryzmowi mają charakter rozproszony, natomiast projektowana regulacja ma

[Terrorystycznych.html](#)) wskazywał, że „w trakcie posiedzenia odbyła się dyskusja dotycząca rozwiązań, które znajdują się w ustawie o działaniach antyterrorystycznych”.

³ Informacja ta została następnie potwierdzona w sprostowaniu M. Wąsika do artykułu: E. Siedlecka, *Poselski projekt ustawy "inwigilacyjnej" będzie wycofany?*, Gazeta.pl [artykuł z 4 stycznia 2016 r., dostępny na stronie: <http://wyborcza.pl/1,75398,19427955,poselski-projekt-ustawy-inwigilacyjnej-bedzie-wycofany.html>].

charakter integrujący. W uzasadnieniu wyraźnie wskazano, że czynnikiem, który zdecydował o przyjęciu projektu ustawy (a z pewnością przyspieszeniu prac nad projektem) był zamach terrorystyczny w Brukseli w marcu 2016 r. W komentarzach medialnych wskazywano również na potrzebę zabezpieczenia Światowych Dni Młodzieży odbywających się w lipcu 2016 r. w Krakowie. Prawdopodobnie z tego względu termin wejścia w życie ustawy został pierwotnie określony na 1 czerwca 2016 r.

Pozostaje jednak wątpliwe, czy w tak krótkim czasie – tj. na ok. 2 miesiące przed Światowymi Dniami Młodzieży – możliwe jest zrealizowanie celu stawianego przed ustawą, tj. wzmocnienia koordynacji działań służb na zasadach przewidzianych w ustawie. Tym bardziej, że w marcu uchwalona została tzw. spec-ustawa dotycząca przygotowania i organizacji Światowych Dni Młodzieży.

Jak powszechnie wiadomo terroryzm jest zjawiskiem niezwykle skomplikowanym. Dlatego też doświadczenia i przyczyny zamachów w Brukseli oraz w Paryżu powinny zostać przeanalizowane wieloaspektowo i nie mogą sprowadzać się do konkluzji o potrzebie przyznania służbom nowych uprawnień, które będą realizowane bez żadnego zewnętrznego nadzoru.

3. Zakres ustawy

Projekt ustawy określa zasady prowadzenia działań antyterrorystycznych (art. 1), tj. działań organów administracji publicznej, polegające na:

1. zapobieganiu zdarzeniom o charakterze terrorystycznym,
2. przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć,
3. reagowaniu w przypadku wystąpienia takich zdarzeń,
4. usuwaniu ich skutków,
5. odtwarzaniu zasobów przeznaczonych do reagowania na nie (art. 2 pkt 1).

Podstawowe znaczenie dla określenia zakresu ustawy, tj. m.in. nowych kompetencji przyznanych służbom, jest pojęcie „zdarzenia o charakterze terrorystycznym”, które zostało określone w bardzo szeroki sposób jako „sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym lub zagrożenie zaistnienia takiego czynu”. Dodatkowo ustawa poszerza również dotychczasową definicję „przestępstwa o charakterze terrorystycznym” (art. 115 § 20 k.k.).

Nieprecyzyjna jest również granica między działaniami antyterrorystycznymi a kontrterrorystycznymi zdefiniowanymi w art. 2 projektu. Nie jest jasne, jaki jest dokładny zakres „infrastruktury administracji publicznej” i czy np. obejmuje on również obiekty, w których siedziby mają podmioty realizujące zadania publiczne dla administracji. Tym samym działania określone w ustawie, w tym nowe uprawnienia ABW, będą mogły zostać zastosowane po spełnieniu tych niezwykle szerokich przesłanek.

Co więcej, projekt posługuje się szerokimi i nieprecyzyjnymi definicjami, pozostając jednocześnie (docelowo) aktem prawnym koncentrującym się na ściganiu określonej kategorii przestępstw. Rodzi poważne wątpliwości, czy z punktu widzenia spójności systemu prawa, takie rozwiązanie jest prawidłowe.

4. Poszerzenie kompetencji ABW

Podstawowym środkiem do osiągnięcia założonych celów projektu jest wyraźne przypisanie Szefowi ABW odpowiedzialności za zapobieganie zdarzeniom o charakterze terrorystycznym (art. 3 ust. 1) zaś Ministrowi Spraw Wewnętrznych – za „przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym” (ust. 2). Istnieje ryzyko, że taki podział kompetencji (ABW nie podlega MSW) może rodzić konflikty kompetencyjne.

Projekt przewiduje, że podmioty wymienione w art. 4 ust. 1 projektu, tj.: organy administracji publicznej, właściciele, posiadacze obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej, mają obowiązek współpracy z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych. Ponadto podmioty te są zobowiązane przekazywać Szefowi ABW informacje dotyczące zagrożeń o charakterze terrorystycznym (art. 4 ust. 2). Z kolei Szef ABW jest uprawniony na gruncie ustawy do wydawania poleceń podmiotom określonym w art. 4 ust. 1 projektu.

4.1. Wykazy zdarzeń i osób

Szefowi ABW przyznano kompetencję do koordynacji czynności analityczno-informacyjnych podejmowanych przez służby oraz wymianę informacji między służbami dotyczących zagrożeń o charakterze terrorystycznym. W świetle projektu, na „informacyjne działań antyterrorystyczne” składają się, m.in.:

- kompetencja Ministra Spraw Wewnętrznych do określenia w drodze rozporządzenia (w porozumieniu z ministrem właściwym ds. finansów publicznych, Ministrem Obrony Narodowej i po zasięgnięciu opinii Szefa ABW) katalogu zdarzeń o charakterze terrorystycznym (art. 5 ust. 2 projektu);
- kompetencja Szefa ABW do prowadzenia wykazu osób „podejrzanych o terroryzm”, tj. podejmujących działalność na rzecz organizacji terrorystycznych, poszukiwanych osobach prowadzących działalność terrorystyczną lub podejrzewanych o popełnienie przestępstw o charakterze terrorystycznym czy osobach uczestniczących w szkoleniach terrorystycznych.

Wystąpienie zdarzeń określonych w katalogu zdarzeń o charakterze terrorystycznym będzie pozwalało na podjęcie przez uprawnione służby kompetencji przewidzianych w projekcie ustawy. Katalog będzie określany przez władzę wykonawczą. Projekt rozporządzenia określającego zdarzenia o charakterze terrorystycznym został załączony

do projektu ustawy przyjętego przez Radę Ministrów w dniu 10 maja 2016 r. Wśród zdarzeń o charakterze terrorystycznym wskazano, m.in.:

- kontakty obywateli RP z przedstawicielami organizacji fundamentalistycznych;
- informacje o utracie bądź kradzieży polskich dokumentów tożsamości;
- konstruowanie ładunków wybuchowych;
- użycie „zielonego lasera”;
- wystąpienie przedstawicieli struktur muzułmańskich w Polsce, w trakcie których głoszone były fundamentalistyczne hasła;
- informacja o zamiarze odbycia przez cudzoziemca z kraju podwyższonego ryzyka stażu naukowego, podjęcia studiów;
- informacje na temat planów utworzenia w naszym kraju uczelni islamskich;
- wizyty w polskich zakładach penitencjarnych islamskich duchownych bądź przedstawicieli organizacji zrzeszających osoby tego wyznania;
- kolportaż literatury i periodyków propagujących ideologie ekstremistyczne;
- sygnały o nieprawidłowościach odnotowywanych przez organy kontroli skarbowej w podmiotach kierowanych przez osoby pochodzące z państw podwyższonego ryzyka;
- informacje o zagranicznych dotacjach przekazanych osobom i organizacjom funkcjonującym na terytorium RP podejrzewanym o związki lub sympatyzowanie z ugrupowaniami ekstremistycznymi;
- nabycie w Polsce nieruchomości i lokowanie kapitału pochodzącego z nieujawnionych źródeł przez osoby pochodzące z państw podwyższonego ryzyka;
- rozpowszechnianie treści nawołujących do aktów przemocy i łamania prawa na tle rasowym, religijnym, narodowościowym, etnicznym, politycznym (np. hasła antysemityczne).

Istotnym elementem konstrukcji tych zdarzeń jest ich powiązanie z islamem. O ile jeszcze próba powiązania tych zdarzeń z działalnością ekstremistyczną, może mieć przełożenie na przeciwdziałanie zjawiskom terrorystycznym, o tyle postrzeganie w tych kategoriach samego faktu planowanego utworzenia uczelni islamskiej czy wizyty w więzieniu islamskich duchownych nosi znamiona dyskryminacji ze względu na religię. To samo wydarzenie, jednak związane religią inną niż islam, nie będzie bowiem analizowane w kategoriach zagrożeń terrorystycznych.

Odnosnie zaś wykazu osób „niebezpiecznych”, który będzie prowadzony na podstawie projektowanego art. 6, wskazać trzeba, że przesłanki decydujące o umieszczeniu w tym wykazie są ocenne i nieostre i nie spełniają kryterium precyzyjności przepisów ingerujących w prawa i wolności. Po drugie, nie ma żadnej zewnętrznej kontroli nad tym, kto zostanie umieszczony na takiej liście (nie jest przewidziana rzetelna procedura weryfikacji umieszczenia na tej liście). Po trzecie, z ustawy nie wynika, jakie skutki wiążą się z umieszczeniem na liście (np. czy umieszczenie na liście będzie miało wpływ na prowadzenie wobec tych osób czynności, o których mowa w art. 8 projektu albo na jakiegokolwiek postępowanie administracyjne dotyczące tej osoby, np. w zakresie kwestii imigracyjnych). Po czwarte, zakres gromadzonych informacji, które zostaną zawarte w wykazie, zostanie uregulowany w formie zarządzenia Szefa ABW. A zatem to z aktu

prawa wewnętrznego wynikać będzie zakres ingerencji w prawa i wolności konstytucyjnie chronione. Narusza to konstytucyjny wymóg, aby ograniczenie praw następowało w formie ustawy.

W uzasadnieniu projektu wskazano w sposób blankietowy, że „utworzenie takiej bazy stanowi naturalną konsekwencję wzrostu zagrożenia zdarzeniami o charakterze terrorystycznym” oraz że „umożliwi to wymianę informacji ze służbami państw trzecich”.

Informacje zawarte w „wykazie osób”, jak również w katalogu zdarzeń o charakterze terrorystycznym, będą następnie przekazywane przez Szefa ABW właściwym organom. Ponadto projekt przewiduje, że Szef ABW – w celu zapobiegania zdarzeniom o charakterze terrorystycznym – będzie koordynował czynności operacyjno-rozpoznawcze oraz czynności obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych (art. 7 ust. 1). Szef ABW będzie mógł również wydawać służbom prowadzącym te czynności operacyjno-rozpoznawcze „zalecenia mające na celu usunięcie bądź minimalizację zaistniałego zagrożenia terrorystycznego”. Przepis ten częściowo powiela regulację z art. 40 ustawy o ABW, zgodnie z którą *Szef ABW koordynuje podejmowane przez służby specjalne czynności operacyjno-rozpoznawcze mogące mieć wpływ na bezpieczeństwo państwa*. Jest to zatem przepis szczegółowy odnoszący się do jednej z kategorii zagrożeń dla bezpieczeństwa publicznego.

4.2. Prowadzenie kontroli operacyjnej bez zgody sądu

Jednym z narzędzi, które mają umożliwić lepsze zapewnienie bezpieczeństwa publicznego, jest zawarta w projekcie propozycja przyznania Szefowi ABW kompetencji do prowadzenia wobec cudzoziemców kontroli operacyjnej. Mimo, iż przedmiot kompetencji określony w art. 8 projektu pokrywa się w pełni z regulacjami dotyczącymi kontroli operacyjnej funkcjonującymi (np. na podstawie ustawy o Policji czy ustawy o ABW), projekt ustawy nie posługuje się jednak określeniem „kontroli operacyjnej”. Uzasadnienie projektu wskazuje na tę analogię podkreślając jednak, że najważniejsza różnica ma polegać na tym, że kontrolę nad tymi czynnościami ma prowadzić Prokurator Generalny, a nie sąd. W dalszym ciągu cudzoziemcy będą mogli być objęci kontrolą operacyjną na gruncie ustawy o Policji czy ustawy o ABW. Ten sam stan faktyczny został uregulowany odmiennie na gruncie dwóch rodzajów aktów prawnych – tzw. ustaw resortowych oraz ustawy antyterrorystycznej.

Działania określone w art. 8 projektu mają być realizowane „w celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym” i mają dotyczyć jedynie cudzoziemców, w stosunku do których „istnieje obawa” co do możliwości prowadzenia przez nich działalności terrorystycznej. Tym samym, z jednej strony projektodawca używa bardzo szerokiej przesłanki przedmiotowej (zwalczanie przestępstw o charakterze terrorystycznym). Z drugiej, zakreślając stronę podmiotową kompetencji przyznanej Szefowi ABW, projektodawca posługuje się arbitralną przesłanką – tj. faktem posiadania obywatelstwa polskiego. Ponadto, sformułowanie

„istnieje obawa” sugeruje niezwykle niski poziom „przekonania” o związku danej osoby z prowadzeniem działalności terrorystycznej.

Decyzję o prowadzeniu tych czynności będzie podejmował Szef ABW, który następnie zawiadomi o tym Ministra Koordynatora Służb Specjalnych oraz Prokuratora Generalnego. Nie będzie wymagana zgoda sądu przez 3 miesiące prowadzenia działań na podstawie art. 8 projektu. Dopiero po tym czasie przedłużanie prowadzonych czynności będzie wymagało zgody sądu uzyskanej na podstawie art. 27 ustawy o ABW. Przy braku zgody sądu na początku prowadzenia tych działań, pojawienie się obowiązku uzyskania takiej zgody na dalszym etapie będzie rodziło nadużycia, np. przerwanie prowadzonych działań na kilka dni, a następnie prowadzenie ich od początku, co nie będzie formalnie przedłużeniem, a zainicjowaniem na nowo.

Projektodawca w uzasadnieniu wskazuje, że w świetle wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. dopuszczalne jest wprowadzenie regulacji przewidujących odmienne traktowanie cudzoziemców i obywateli polskich⁴. Trybunał wskazał, że „różnicowanie poziomu ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się może także nastąpić z uwagi na to, czy niejawne pozyskiwanie informacji dotyczy obywateli, czy osób niemających polskiego obywatelstwa”.

Standard taki wynika m.in. z wykładni art. 51 ust. 2 Konstytucji, który wskazuje na zakaz pozyskiwania informacji o obywatelach. Trybunał wyraźnie odrzucił jednak interpretację, która pozwalałaby na gromadzenie o cudzoziemcach „informacji niekoniecznych w demokratycznym państwie”. O ile Trybunał nie wykluczył różnicowania poziomu ochrony różnych praw konstytucyjnych ze względu na obywatelstwo, o tyle określił wyraźną granicę takiego różnicowania: „nie może [ona] prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności oraz praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich”. Dlatego Trybunał przyjął „jako założenie wyjściowe – jednakowy standard ingerencji w konstytucyjne wolności oraz prawa, bez względu na to, czy ich podmiot ma obywatelstwo polskie”. Trybunał wskazał dalej, że „każdy znajdujący się pod władzą Rzeczypospolitej (...) niezależnie od statusu obywatelskiego – może zatem zasadnie oczekiwać ochrony przed nieuzasadnioną ingerencją w przysługujące mu wolności i prawa” oraz stwierdził, że standardem konstytucyjnym nałożonym na ustawodawcę jest „konieczność ustanowienia takich samych standardów dotyczących pozyskiwania, gromadzenia czy przechowywania danych zgromadzonych przez władze publiczne w toku czynności operacyjno-rozpoznawczych w stosunku do wszystkich podmiotów, które znajdują się pod władzą Rzeczypospolitej Polskiej”.

Od tak zakreślonych zasad ogólnych dopuszczalne są jednak wyjątki, które muszą spełniać wymogi zasady proporcjonalności z art. 31 ust. 3 Konstytucji. Trybunał odrzucił tym samym tezę, jakoby art. 37 ust. 2 stanowił *lex specialis* wyłączający zastosowanie art. 31 ust. 3 Konstytucji. Odmienne stanowisko skutkowałoby tym, że „cudzoziemcy nie

⁴ Sygn. K 23/11

mieliby faktycznie żadnych gwarantowanych konstytucyjnie praw”. Ograniczenie praw nie może naruszać ani przekreślać ich istoty⁵.

Tymczasem projektowane przepisy przewidują, że jedynym organem decydującym o prowadzeniu *de facto* kontroli operacyjnej jest Szef ABW. Nie ma tym samym gwarancji zabezpieczających przed nadużyciami. Zabezpieczeniem takim nie jest wymóg uzyskania zgody po 3 miesiącach prowadzenia działań na podstawie art. 8 projektu. Jak wskazano powyżej, bez zewnętrznej kontroli, niezwykle łatwo będzie dopuścić się nadużyć również w tym zakresie.

Również na gruncie orzecznictwa Europejskiego Trybunału Praw Człowieka (dalej: ETPC) wkroczenie w tajemnicę korespondencji wymaga, aby działanie to było proporcjonalne. Niezbędnym elementem proporcjonalności jest istnienie gwarancji, które zabezpieczą przed nadużywaniem uprawnień w zakresie tajnego pozyskiwania informacji przez służby⁶. Procedura przewidziana w art. 8 projektu nie zawiera praktycznie żadnych takich gwarancji.

Co więcej, fakt, że służby będą gromadzić na podstawie art. 8 jeszcze więcej informacji, które następnie będą musiały zostać przeanalizowane, nie gwarantuje, że zapewniony zostanie wyższy poziom bezpieczeństwa. Ponadto korespondencja cudzoziemca zawsze będzie prowadzona z jakąś drugą stroną, która z dużym prawdopodobieństwem może się okazać obywatelem polskim. Tym samym bardzo prawdopodobne jest to, że taką pozasądową kontrolą operacyjną objęta zostanie duża grupa obywateli polskich. Rozwiązanie takie narusza m.in. art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych gwarantujący każdemu (nie jedynie obywatelom danego państwa) prawo do ochrony przed ingerencją w tajemnicę korespondencji⁷.

W polskim prawie nawet procedura przekazywania prokuraturze i sądom materiałów tajnych i ściśle tajnych poddana jest kontroli ze strony Pierwszego Prezesa Sądu Najwyższego (art. 39 ustawy o ABW). W uzasadnieniu nie wskazano dlaczego dotychczasowe rozwiązania dotyczące prowadzenia kontroli operacyjnej, wymagającej zgody (choćby „następczo” w wypadkach niecierpiących zwłoki) były niewystarczające dla ścigania najpoważniejszych przestępstw, w tym o charakterze terrorystycznym.

Procedura przewidziana w art. 8 nie zawiera jakichkolwiek gwarancji ochrony tajemnicy spowiedzi, tajemnicy obrończej czy innych tajemnic zawodowych, przykładowo

⁵ Konsekwencją obowiązywania art. 37 ust. 2 Konstytucji jest natomiast możliwość dokonania bardziej elastycznej interpretacji poszczególnych przesłanek składających się na zasadę proporcjonalności, uzasadniającej większy poziom ingerencji w wolności i prawa cudzoziemców niż obywateli.

⁶ Wyrok Europejskiego Trybunału Praw Człowieka z 4 grudnia 2015 r. w sprawie *Zakharov v. Rosja*, skarga nr 47143/06.

⁷ Artykuł 17. 1. Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. 2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami.

dziennikarskiej. Co więcej, może ona mieć również wpływ na bezpieczeństwo korespondencji dyplomatycznej prowadzonej w Polsce przez cudzoziemców.

Procedura niszczenia materiałów zgromadzonych w wyniku prowadzenia *quasi*-kontroli operacyjnej jest również niejasna. Z jednej strony Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych materiałów, z drugiej projekt przewiduje odpowiednie stosowanie art. 238 § 3-5 k.p.k., który przyznaje odpowiednie kompetencje sądowi w zakresie niszczenia danych zgromadzonych podczas utrwalania rozmów. Z takiego brzmienia art. 8 ust. 7-9 nie wynika, żeby nad procesem niszczenia danych – który co do zasady pozostaje w kompetencji Prokuratora Generalnego – kontrolę sprawował sąd. Należy wprowadzić takie rozwiązania, które będą gwarantowały możliwość niezależnej weryfikacji prawidłowości i legalności procedury niszczenia danych zgromadzonych na podstawie art. 8 projektu.

4.3. Blokowanie stron internetowych

Kolejnym zagadnieniem, które budzi poważne wątpliwości z punktu widzenia ochrony praw i wolności obywatelskich jest możliwość blokowania treści dostępnych w internecie na mocy zaproponowanego w projekcie art. 32c ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Projektowany przepis wprowadza rozwiązanie, które może powodować istotne ograniczenie swobody wypowiedzi gwarantowanej m.in. w art. 54 Konstytucji, art. 10 Europejskiej Konwencji Praw Człowieka (dalej: EKPC) oraz art. 11 Karty Praw Podstawowych UE.

Przed dokonaniem szczegółowej analizy zaproponowanej regulacji warto zaznaczyć, że zgodnie z orzecznictwem ETPC gwarancje chroniące swobodę wypowiedzi znajdują zastosowanie zarówno do tradycyjnych środków przekazu, jak i do komunikacji internetowej (zob. np. wyroki ws. *Times Newspapers p. Zjednoczonemu Królestwu*⁸, *Węgrzynowski i Smolczewski p. Polsce*⁹, *Editorial Board of Pravoye Delo and Shtetel p. Ukrainie*¹⁰). Trybunał wielokrotnie wskazywał, że internet odgrywa dziś kluczową rolę nie tylko w zapewnianiu dostępu społeczeństwa do informacji, ale także przyczynia się do realizacji prawa do wyrażania oraz rozpowszechniania poglądów. Dzieje się tak w szczególności za sprawą rozwoju tzw. Sieci 2.0. (Web 2.0.), której cechą jest współtworzenie treści dostępnych w internecie przez jego użytkowników. W konsekwencji internet stał się podstawową platformą współczesnej komunikacji pomiędzy jednostkami, a także ważnym medium, za pośrednictwem którego prowadzona jest obecnie obywatelska debata o sprawach mających publiczne znaczenie, w tym debata o kwestiach politycznych (*Yildirim p. Turcji*¹¹).

⁸ Wyrok ETPC z 10 marca 2009 r., skargi nr . 3002/03, 23676/03.

⁹ Wyrok ETPC z 16 lipca 2013, skarga nr 33846/07.

¹⁰ Wyrok ETPC z 5 maja 2011 r., skarga nr 33014/05.

¹¹ Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10.

Analiza dotychczasowego orzecznictwa ETPC wskazuje, że Trybunał uznaje blokowanie treści dostępnych w internecie, a tym bardziej całych witryn lub domen internetowych, za środek, który głęboko ingeruje w wartości chronione przez art. 10 EKPC, ograniczając prawo do swobodnego otrzymywania oraz przekazywania informacji (*Yildirim p. Turcji, Cengiz i inni p. Turcji*¹²). Dlatego też ETPC przykłada szczególną wagę do tego, aby środek ten był stosowany z dużą rozważą, jedynie gdy jest niezbędny i proporcjonalny dla osiągnięcia uprawnionego celu oraz wyłącznie na podstawie dostatecznie precyzyjnych regulacji prawnych, które będą chronić przed jego arbitralnym wykorzystywaniem przez organy państwa. Na konieczność wprowadzenia odpowiednich zabezpieczeń chroniących swobodę wypowiedzi w kontekście nakazu blokowania treści w sieci zwracają uwagę także inne międzynarodowe instytucje zajmujące się ochroną praw człowieka, takie jak m.in. Komitet Ministrów Rady Europy w Rekomendacji z 2016 r. w sprawie wolności w internecie¹³ czy Specjalny Sprawozdawca ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi w swoim raporcie z 2011 r.¹⁴.

Przesłanki określone w art. 32 c, w oparciu o które, będzie można zarządzić zablokowanie dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych (lub zażądać ich zablokowania od administratora systemu teleinformatycznego) mają bardzo ogólny, nieostry charakter. Projekt zakłada bowiem, że ww. czynności mogą być zarządzone przez Sąd (postanowieniem) na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego na określony czas, nie dłuższy niż 30 dni „w celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców”, gdy podlegające zablokowaniu dane „mają związek ze zdarzeniem o charakterze terrorystycznym”. W ocenie HFPC tak ujęte przesłanki blokowania pozostawiają uprawnionym organom państwa **zbyt szerokie pole do arbitralnego stosowaniu tego środka** oraz do nadużywania go do celów wykraczających poza deklarowane założenia projektu ustawy. Co więcej, proponowane regulacje nie określają precyzyjnie możliwego zakresu blokowania danych. Nie jest jasne, czy nakaz blokowania wydany na podstawie projektowanej ustawy może dotyczyć tylko uniemożliwienia dostępu do określonych informacji na konkretnej stronie

¹² Wyrok ETPC z 1 grudnia 2015 r., skargi nr 48226/10 i nr 14027/11.

¹³ CM/Rec(2016)5

¹⁴ Raport nr A/HRC/17/27, 16 maja 2011 r.: “States’ use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression, as the criteria mentioned under chapter III are not met. Firstly, the specific conditions that justify blocking are not established in law, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body.” (par. 31).

internetowej, blokowania całej witryny czy też całej domeny internetowej, w ramach której prowadzona jest dana strona, a nawet blokowania całych aplikacji internetowych (projekt ustawy umożliwia bowiem blokowanie zarówno „danych informatycznych”, jak i „usług teleinformatycznych”).

Brak dostatecznie szczegółowego określenia przesłanek umożliwiających blokowanie treści w internecie oraz brak uregulowania możliwego zakresu stosowania tego środka jest sprzeczny z wytycznymi wynikającymi zarówno z orzecznictwa ETPC, jak i z ww. raportu Specjalnego Sprawozdawcy ONZ. W szczególności warto w tym kontekście przytoczyć wyrok ETPC ws. *Yildirim p. Turcji*, w którym Trybunał wyraźnie zaznaczył, że blokowanie może być uznane za dopuszczalne tylko, gdy odbywa się na podstawie maksymalnie precyzyjnych przepisów prawa krajowego oraz jest stosowane w możliwie wąskim zakresie, niewykraczającym poza niezbędne minimum. W omawianej sprawie Trybunał ocenił, że turecki sąd niesłusznie zdecydował o blokadzie całej domeny internetowej na podstawie wniosku krajowego Urzędu Telekomunikacji (TIB), nie weryfikując w należyty sposób, czy jest to środek rzeczywiście konieczny oraz proporcjonalny dla osiągnięcia uprawnionego celu (w tym przypadku walki z treścią obrażającą Atatürka). Trybunał zwrócił ponadto uwagę na to, że w tureckim prawie nie było wyraźnych przepisów przewidujących możliwość blokowania całej domeny internetowej (przepisy odnosiły się jedynie do możliwości zablokowania konkretnych bezprawnych treści), przez co decyzja sądów krajowych nie miała wystarczającej podstawy prawnej. W efekcie ETPC stwierdził, iż doszło w tym przypadku do naruszenia swobody wypowiedzi.

Kolejnym elementem omawianej regulacji, który budzi poważne wątpliwości, jest kwestia zapewnienia **efektywnej kontroli sądu** nad blokowaniem treści w internecie. Na konieczność istnienia takiej kontroli zwrócono uwagę zarówno w orzecznictwie ETPC (*Yildirim p. Turcji*, *Cengiz i inni p. Turcji*), jak i w ww. Rekomendacji Komitetu Ministrów RE oraz Raporcie Specjalnego Sprawozdawcy ONZ. Niestety, w ocenie HFPC, przedstawiona przez projektodawcę propozycja przepisów nie gwarantuje spełnienia tego wymogu. Po pierwsze efektywna kontrola sądu w świetle wskazanych standardów międzynarodowych powinna obejmować zarówno ocenę wystąpienia przesłanek blokowania (które – jak wspomniano wyżej – mają niedostatecznie precyzyjny charakter w projekcie ustawy), jak i ocenę zakresu zastosowanego środka pod kątem jego proporcjonalności i adekwatności w konkretnych okolicznościach sprawy (czego w projekcie ustawy w ogóle nie przewidziano). Tymczasem kontrola sądu nie może ograniczać się do stwierdzenia, czy istnieją podstawy do zastosowania środka przewidzianego w art. 32c, ale powinna również uwzględniać dokonanie oceny, czy zarządzony środek nie ma nadmiernego charakteru w stosunku do celu, który ma realizować w danej sprawie (np. sąd nie powinien zaakceptować nakazu zablokowania całej strony internetowej w sytuacji, gdy wystarczy nakaz zablokowania jedynie określonej treści, która się na niej znajduje).

Po drugie wątpliwości wzbudza zaproponowana przez projektodawcę procedura blokowania. Należy zauważyć, że przedłożony w Sejmie projekt ustawy zawiera w tym zakresie lepsze rozwiązanie w stosunku to pierwotnego projektu ustawy przedstawionego

przez MSWiA, tj. wprowadza co do zasady wymóg uzyskania uprzedniej zgody sądu na blokowanie. Procedura blokowania wymagająca jedynie następczej zgody sądu została natomiast ograniczona do „przypadków niecierpiących zwłoki”. W takich sytuacjach będzie o tym decydował Szef ABW za pisemną zgodą Prokuratora Generalnego. Jednocześnie z zablokowaniem danych lub zażądaniem od administratora danych ich zablokowania, Szef ABW będzie zobowiązany do zwrócenia się do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wydanie postanowienia w tej sprawie. Sąd będzie musiał wydać takie postanowienie w ciągu pięciu dni (jeśli w tym czasie sąd nie „zatwierdzi” blokady, Szef ABW ma obowiązek ją wstrzymać). Choć obecnie zaproponowane rozwiązanie stwarza silniejsze gwarancje chroniące przed nieuzasadnioną ingerencją w wolność słowa, to jednak projektodawca powinien w większym stopniu zadbać o to, aby procedura wymagająca jedynie następczej zgody sądu nie była nadużywana. W szczególności projektodawca powinien w sposób bardziej precyzyjny wskazać, w jakich okolicznościach odstępstwo od standardowej procedury wymagającej uzyskania uprzedniej zgody sądu byłoby możliwe, gwarantując przy tym w przepisach, że jej stosowanie będzie rzeczywiście ograniczone do wyjątkowych przypadków.

Po trzecie na krytyczną ocenę zasługuje również zaproponowane przez projektodawcę rozwiązanie, zgodnie z którym możliwość zaskarżenia postanowienia sądu będzie przysługiwać tylko Szefowi ABW oraz Prokuratorowi Generalnemu. Projektodawca nie przewidział natomiast takiego uprawnienia np. dla administratora zablokowanej strony internetowej, który w efekcie nie będzie miał żadnej możliwości odniesienia się do zarzutów Szefa ABW, przedstawienia swojego stanowiska w sprawie w postępowaniu przed sądem (w posiedzeniu będzie mógł wziąć udział tylko „prokurator i Szef ABW”), czy wreszcie zakwestionowania postanowienia sądu w ramach kontroli instancyjnej. Co więcej, projektodawca na żadnym etapie nie wprowadził nawet obowiązku poinformowania administratora zablokowanej strony o zastosowaniu wobec niego tego środka (na podstawie art. 32 c ust. 1 pkt 1), chociaż taki wymóg wynika wprost z rekomendacji zawartej w ww. raporcie Specjalnego Sprawozdawcy ONZ. Takie rozwiązanie powoduje znaczącą, nieuzasadnioną nierównowagę pomiędzy pozycją organów państwa a pozycją obywateli, przyczyniając się do zwiększenia ryzyka arbitralności podejmowanych decyzji.

Po czwarte wątpliwości budzi dodatkowo rola w tym procesie Prokuratora Generalnego, którym obecnie jest osoba sprawująca jednocześnie funkcję polityczną - Ministra Sprawiedliwości. Jest to rozwiązanie, które osłabia efektywność kontroli sądowej (sąd, który nie wydałby postanowienia uwzględniającego wniosek Szefa ABW za zgodą Prokuratora Generalnego, lub następnie zażalenia Prokuratora Generalnego na postanowienie sądu orzekającego w I instancji, *de facto* kwestionowałby decyzję osoby pełniącej funkcję Ministra sprawującego nadzór nad funkcjonowaniem wymiaru sprawiedliwości). To z kolei, w połączeniu z innymi, wskazanymi wyżej mankamentami art. 32c (nieostrość przesłanek blokowania), rodzi obawę, że przewidziany w nim środek może być wykorzystywany do celów politycznych, tj. nie tylko do walki z treściami faktycznie mającymi związek z działaniami terrorystycznymi, ale także treściami, które są krytyczne wobec władzy lub z innych względów nie odpowiadają jej poglądom.

Podsumowując, należy zaznaczyć, że potrzeba przeciwdziałania terroryzmowi może w określonych sytuacjach usprawiedliwiać ingerencję w wolność słowa (zob. np. wyrok ETPC ws. *Leroy p. Francji*¹⁵). Deklarowany przez projektodawcę cel omawianego przepisu w uzasadnieniu projektu ustawy, tj. „przeciwdziałanie działalności organizacji terrorystycznych, które wykorzystują internet do promowania swojej ideologii, zamieszczania instruktażu w zakresie sposobu prowadzenia zamachów terrorystycznych oraz komunikowania się ze swoimi zwolennikami” może uzasadniać konieczność blokowania pewnych treści w internecie. Jednakże zbyt ogólny sposób ukształtowania przesłanek pozwalających na zastosowanie tego środka, nieprecyzyjne określenie jego możliwego zakresu oraz procedura niezapewniająca wystarczających gwarancji przed jego nadużywaniem, sprawiają, że zaproponowane przez projektodawcę regulacje należy ocenić krytycznie. Stwarzają one bowiem duże ryzyko arbitralnego korzystania z tego narzędzia przez organy państwa i nie zapewniają ścisłej kontroli nad tym, aby było ono stosowane wyłącznie w deklarowanym wyżej celu, z zachowaniem odpowiedniej równowagi pomiędzy koniecznością ochrony wolności słowa a potrzebą zwalczania terroryzmu. Z tych względów, w ocenie HFPC, zaproponowana regulacja wymaga wprowadzenia istotnych zmian w projekcie ustawy, które będą uwzględniały przedstawione wyżej standardy międzynarodowe. Dodatkowo projektodawca powinien rozważyć wprowadzenie mechanizmów zapewniających przejrzystość korzystania przez organy państwa z regulacji umożliwiającej blokowania treści w internecie, wprowadzając np. – zgodnie z zaleceniem Specjalnego Sprawozdawcy ONZ – jawną i dostępną publicznie listę zablokowanych stron wraz z uzasadnieniem wyjaśniającym, dlaczego zastosowano wobec nich ten środek.

4.4. Szerszy dostęp do danych osobowych

Projekt przewiduje zmiany skutkujące poszerzeniem dostępu służb (w szczególności ABW) do szeregu danych dotyczących zarówno obywateli, jak i cudzoziemców.

Art. 9 projektu przewiduje dostęp ABW, Policji i Straży Granicznej do **danych biometrycznych** cudzoziemców – obrazu linii papilarnych oraz utrwalanie wizerunku twarzy. Zgromadzone na tej podstawie dane będą następnie przekazywane Komendantowi Głównemu Policji i włączane do jej baz. Z jednej strony gromadzenie danych na podstawie art. 9 ma odnosić się do cudzoziemców, z drugiej jednak strony pierwszą przesłanką zastosowania art. 9 jest „wątpliwość co do tożsamości osoby”. Takie określenie powoduje, że niemożliwe jest zrealizowanie podstawowego założenia art. 9 projektu, tj. zbierania danych biometrycznych jedynie od cudzoziemców.

Art. 9 przewiduje gromadzenie danych w przypadku związku cudzoziemca z działalnością terrorystyczną, co oznacza, że tworzona jest szczególna podstawa prawna do gromadzenia informacji mogących mieć związek z jedną kategorią przestępstw. Przykładowo, Policja posiada obecnie kompetencję do pobierania od osób odcisków linii papilarnych w trybie i przypadkach określonych w przepisach kodeksu postępowania

¹⁵ Wyrok z 2 października 2008 r., skarga nr 36109/03.

karnego lub też w celu identyfikacji osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość, jeżeli ustalenie tożsamości w inny sposób nie jest możliwe (por. art. 15 ust. 1 pkt 3a ustawy o Policji). Ustawodawca celowo ograniczył zbieranie danych do zasad i trybu wynikających z kodeksu postępowania karnego (art. 74, art. 192a k.p.k.). Ma to przede wszystkim zabezpieczyć prawa osób, których dane mają zostać zgromadzone. Kodeks postępowania karnego odnosi możliwość gromadzenia danych do oskarżonego (art. 74 § 2 k.p.k.) oraz osób podejrzanych (art. 192a k.p.k.). Tymczasem art. 9 projektu nie posługuje się żadną kategorią kodeksową, lecz bardzo ogólnym sformułowaniem „istnienia podejrzenia”: nielegalnego przekroczenia granicy RP, zamiaru nielegalnego przebywania na terytorium RP, związku osoby ze zdarzeniem terrorystycznym. Ponadto podstawą do zgromadzenia linii papilarnych na podstawie art. 9 może być wątpliwość co do deklarowanego celu pobytu na terytorium RP oraz fakt, iż osoba mogła uczestniczyć w szkoleniu terrorystycznym.

Również Straż Graniczna posiada już w pewnym zakresie takie uprawnienia. Wynikają one z ustawy o cudzoziemcach (art. 13 pkt 10 oraz pkt 24), tj. istnieje możliwość pobierania odcisków palców i wizerunku twarzy w postępowaniach prowadzonych na podstawie tej ustawy (m.in. postępowanie w sprawie o zobowiązanie do powrotu, a decyzja o zobowiązaniu do powrotu jest wydawana przez Straż Graniczną także w sytuacji, gdy cudzoziemiec stanowi zagrożenie – art. 302 ust. 1 pkt 9 ustawy o cudzoziemcach). Ponadto art. 295 ustawy o cudzoziemcach przyznaje Straży Granicznej możliwość pobierania odcisków linii papilarnych cudzoziemca w trakcie kontroli legalności pobytu. Jednym z wymogów legalnego pobytu jest niestwarzanie zagrożenia dla bezpieczeństwa.

Natomiast z punktu widzenia ogólnego celu ustawy – zapewnienia bezpieczeństwa publicznego – wątpliwe wydaje się koncentrowanie się jedynie na danych dotyczących cudzoziemców. Całkowicie pomija się w ten sposób ewentualne zagrożenie, jakie może wynikać z działań obywateli Polski. Ponadto, rozróżnienie takie, w połączeniu z szerokimi i nieostryimi przesłankami, ma charakter arbitralny i nosi znamiona dyskryminacji.

Projekt przewiduje, że Prezes Rady Ministrów określi w drodze rozporządzenia sposób i tryb pobierania i gromadzenia obrazów linii papilarnych oraz utrwalanie wizerunku twarzy. Ponieważ gromadzenie takich danych nie będzie wiązało się z żadnym postępowaniem, którego cudzoziemiec byłby stroną, łatwo przewidzieć, że pobieranie takich danych będzie wiązało się z koniecznością użycia środków przymusu bezpośredniego, które nie mogą zostać uregulowane na poziomie rozporządzenia. Ustawa nie przewiduje również zasad usuwania zgromadzonych danych w wypadku, gdy nie są one niezbędne dla realizacji któregośkolwiek z zadań danej służby lub jeśli zostały zgromadzone na skutek omyłki.

Ponadto, projekt przyznaje Szefowi ABW dostęp do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach prowadzonych przez m.in.: inne służby, ministrów, Szefa Urzędu ds. Cudzoziemców, Prezesa Urzędu Komunikacji Elektronicznej, Prezesów ZUS oraz KRUS, Komisję Nadzoru Finansowego, jednostki

samorządu terytorialnego oraz jednostki organizacyjne im podległe oraz nadzorowane przez wszystkie te podmioty. Ponadto, Szef ABW uzyska dostęp do obrazu z monitoringów wizyjnych umieszczonych w obiektach użyteczności publicznej, przy drogach publicznych i innych miejscach publicznych. Zarówno dane z rejestrów, jak również dane z monitoringu będą udostępniane w trybie znowelizowanego art. 34 ustawy o ABW.

Dostęp ABW do rejestrów Szefa Urzędu ds. Cudzoziemców przewiduje już art. 450 ust. 1 pkt 2 ustawy o cudzoziemcach, który stanowi, że dane w rejestrach wymienionych w tym przepisie¹⁶ udostępnia się m.in. ABW w zakresie niezbędnym do realizacji jej zadań ustawowych. Art. 453 i art. 454 ustawy o cudzoziemcach wskazuje na tryb udostępniania danych z rejestrów, który przewiduje m.in. możliwość przeprowadzenia kontroli podmiotów, które mają dostęp do danych. Projektowany art. 10 w zakresie dostępu do tych samych rejestrów Szefa Urzędu ds. Cudzoziemców przewiduje inny tryb udostępniania – na podstawie art. 34 ustawy o ABW. Zachodzi wątpliwość, jaki jest zatem wzajemny stosunek art. 10 projektu i art. 450 ust. 1 pkt 2 ustawy o cudzoziemcach w zakresie dostępu ABW do rejestrów prowadzonych przez Szefa Urzędu ds. Cudzoziemców, tj. czy stanowi on *suprefluum* i jednocześnie rozszerzenie zakresu dostępu ABW do rejestrów prowadzonych przez Szefa Urzędu ds. Cudzoziemców względem obowiązujących regulacji ustawy o cudzoziemcach, czy też stanowi on ogólną podstawę dostępu ABW do rejestrów prowadzonych przez Szefa Urzędu ds. Cudzoziemców, zaś wyliczenie, do których konkretnie rejestrów ma dostęp ABW określone jest w ustawie o cudzoziemcach.

Projekt znacząco ułatwia Szefowi ABW dostęp do wszelkich danych zgromadzonych w rejestrach publicznych, w tym danych wrażliwych, poprzez dodanie art. 34 ust. 2a ustawy o ABW. Przepis ten przewiduje dostęp do zgromadzonych danych w formie teletransmisji, co z technicznego punktu widzenia poszerza zakres danych zgromadzonych we wszelkich rejestrach publicznych, do których ABW będzie miało dostęp. Warto mieć przy tym na uwadze, że taka forma dostępu do bazy danych oznacza możliwość ewentualnej (nielegalnej) ingerencji w zgromadzone dane. Ustawa nie tworzy żadnych zabezpieczeń w tym zakresie, zaś sposób przetwarzania danych przez ABW w dalszym ciągu pozostaje poza jakimkolwiek zewnętrznym nadzorem. Na gruncie ustawy ABW brak również rozwiązania analogicznego do tego funkcjonującego na gruncie ustawy o CBA, tj. statuującego urząd niezależnego od szefa służby pełnomocnika ds. danych osobowych.

Co więcej projektodawca, zamiast uregulować zasady funkcjonowania monitoringu wizyjnego w miejscach publicznych, przyznał Szefowi ABW możliwość dostępu do wszelkich nagrań z monitoringu (art. 10 pkt 2 projektu).

Projekt przyznaje również Agencji Bezpieczeństwa Wewnętrznego dostęp do tajemnicy bankowej, jeśli jest to niezbędne dla zapobiegania lub ścigania przestępstw z art. 5 ust. 1

¹⁶ Zbiór tych rejestrów zostanie na podstawie projektu poszerzony o centralny rejestr wizowy (art. 450 w zw. z art. 449 ust. 2 pkt 17 ustawy o cudzoziemcach).

pkt 2 ustawy o ABW (dodanie art. 34a ustawy o ABW). Wydaje się, że zmiana taka może być uzasadniona w szczególności w świetle zadania ABW, jakim jest ściganie przestępstw „godzących w podstawy ekonomiczne państwa”. Niestety ustawa nie reguluje, czym są te kategorie przestępstw. Ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji i niektórych innych ustaw¹⁷ podejmując próbę wykonania wyroku Trybunału Konstytucyjnego¹⁸ nie znowelizowała jednak brzmienia art. 5 ust. 1 pkt 2 lit. b, a jedynie zmieniła art. 27 ust. 1 regulujący podstawy stosowania kontroli operacyjnej przez ABW. Tym samym uzyskanie przez ABW danych telekomunikacyjnych, internetowych czy również – w świetle projektu – tajemnicy bankowej będzie oparte na nieprecyzyjnej przesłance, jaką jest ściganie (zapobieżenie popełnienia oraz wykrycie lub ustalenie sprawców) przestępstw „godzących w podstawy ekonomiczne państwa”. Pomimo, iż cała procedura będzie skonstruowana analogicznie do procedury obowiązującej w Policji (art. 20 ust. 3 ustawy o Policji), przesłanki skorzystania z tych kompetencji będą na tyle nieostre, że uniemożliwią zweryfikowanie, czy ABW jest powołana do ścigania danego typu przestępstw.

4.5. Ocena bezpieczeństwa systemów teleinformatycznych (cyberbezpieczeństwo)

Jednym z proponowanych narzędzi walki z terroryzmem jest przyznanie Agencji Bezpieczeństwa Wewnętrznego kompetencji do przeprowadzania ocen bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej oraz systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej (art. 32a w zw. z art. 5 ust. 1 pkt 2a ustawy o ABW).

Mimo, że oceny takie mają być prowadzone zgodnie z rocznym planem, możliwe będzie przeprowadzenie takiej oceny z jego pominięciem. Ocena taka ma polegać na przeprowadzeniu testów bezpieczeństwa w celu identyfikacji zagrożeń. Projekt przyznaje Agencji w tym zakresie określone uprawnienia (art. 32a ust. 7-8 ustawy o ABW).

Wydaje się, że zbiór tych systemów, wobec których prowadzona będzie „ocena bezpieczeństwa”, jest niezmiernie szeroki i z całą pewnością będzie obejmować podmioty prywatne, np. operatorów telekomunikacyjnych czy operatorów świadczących usługi drogą elektroniczną. Tym samym Agencja będzie miała dostęp do informacji zawartych w tym systemie. Agencja będzie miała ustawowy obowiązek zniszczenia uzyskanych w ten sposób informacji, które nie będą mogły zostać wykorzystane do realizacji zadań ustawowych ABW. Z uwagi jednak na fakt, że również nad tak prowadzoną działalnością ABW **nie będzie żadnego zewnętrznego nadzoru**, nie istnieją żadne gwarancje, które zabezpieczą przed nadużyciami kompetencji, np. w celu obejścia wymogów (np. uprzedniej zgody sądu) związanych z prowadzeniem kontroli operacyjnej

¹⁷ Dz. U. poz. 147.

¹⁸ Trybunał orzekł, że art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji.

na podstawie art. 27 ust. 6 pkt 4 ustawy o ABW. Realizacja takiej kompetencji może ponadto umożliwić dostęp ABW do informacji stanowiących tajemnice zawodowe, np. adwokacką lub dziennikarską. Możliwość takich nadużyć jest tym bardziej prawdopodobna, że kolejność prowadzenia takich ocen wynikająca z rocznego planu może zostać pominięta (art. 32a ust. 2 ustawy o ABW).

Co więcej, projektowany art. 32b przewiduje, że w przypadku powzięcia informacji o wystąpieniu zdarzenia o charakterze terrorystycznym dotyczącego systemów lub danych, o których mowa w art. 32a, Szef ABW może żądać od podmiotów obsługujących te systemy informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji systemów, w tym haseł, kodów dostępu. Z brzmienia projektowanego art. 32b ustawy o ABW możliwe będzie również używanie tych systemów przez ABW „w celu zapobiegania, reagowania na zdarzenia o charakterze terrorystycznym dotyczące systemów (...), a także zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców”. Wynika z tego, że przesłanki dostępu do tych niezmiernie wrażliwych danych będą bardzo szerokie, a jedynym podmiotem, który będzie weryfikował ich zasadność będzie sam Szef ABW.

Co więcej, Szef ABW będzie prowadził „centralny rejestr zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych” (art. 32d ustawy o ABW) oraz w oparciu o ten rejestr będzie mógł wydawać rekomendacje administratorom systemów teleinformatycznych określonych w art. 5 ust. 1 pkt 2a ustawy o ABW. Administratorzy będą mieli możliwość przedstawienia zastrzeżeń do rekomendacji wydanych przez ABW. Ponowne rekomendacje (podtrzymane lub zmienione) będą mogły zostać „wyegzekwowane” przez organy nadzorujące. Również i ta kompetencja ABW pozostaje poza jakimkolwiek niezależnym nadzorem. Uzasadnienie wskazuje jedynie, że „projektowane rozwiązanie pozwoli Agencji Bezpieczeństwa Wewnętrznego poszerzyć dostęp do informacji dotyczących charakteru zdarzeń w cyberprzestrzeni, co przełoży się na zwiększenie zdolności w zakresie zapobiegania tym zdarzeniom”.

5. Zmiany w postępowaniu karnym

Rozdział 5. projektu ustawy wprowadza przepisy szczególne dotyczące postępowania przygotowawczego. Wydaje się, że tego typu regulacja powinna zostać ujęta w ramy kodeksu postępowania karnego, a nie być częścią ustawy szczególnej.

Projektodawca tworzy m.in. szczególne podstawy do przeprowadzenia przeszukania pomieszczeń i innych miejsc oraz zatrzymania osoby podejrzewanej. Zgodnie z projektowanym art. 23 prokurator może postanowić o podjęciu takich działań w przypadku podejrzenia lub usiłowania popełnienia albo przygotowania przestępstwa o charakterze terrorystycznym, w celu wykrycia lub zatrzymania albo przymusowego doprowadzenia osoby podejrzewanej, a także w celu znalezienia rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, o ile istnieją uzasadnione podstawy do przypuszczania, że osoba podejrzewana lub wymienione rzeczy znajdują się na danym obszarze. Art. 23 ust. 3 wskazuje przy tym, iż przeszukania pomieszczeń mieszkalnych, innych miejsc, osób, odzieży i przedmiotów

podręcznych, a także zatrzymania osoby podejrzewanej można dokonać o każdej porze doby.

Możliwość dokonania nocnego przeszukania znana jest obowiązującemu kodeksowi postępowania karnego. Zgodnie z nim przeszukania zamieszkałych pomieszczeń można dokonywać w porze nocnej tylko w wypadkach nie cierpiących zwłoki (art. 221 § 1 k.p.k.). Doktryna przyjmuje przy tym, że pod pojęciem wypadków niecierpiących zwłoki należy rozumieć konkretne okoliczności, które wskazują na możliwość ukrycia, przemieszczenia czy zniszczenia przedmiotów, a także ucieczki lub ukrycia poszukiwanej osoby¹⁹.

Tym samym już obecne rozwiązania pozwalają na nocne przeszukania. Po pierwsze, zgodnie z k.p.k. dopuszczalne przez całą dobę jest przeszukiwanie pomieszczeń innych niż mieszkalne oraz osób, odzieży etc. Po drugie obecnie przeszukiwanie pomieszczeń mieszkalnych w porze nocnej dopuszczalne jest jedynie w wypadkach, w których organy państwa dysponują sprawdzonymi informacjami wskazującymi na konieczność dokonania jak najszybszego przeszukania. Projektowany art. 23 ust. 1 *in fine* przewiduje łagodniejszą przesłankę, tj. istnienie uzasadnionych podstaw do przypuszczenia, że osoba podejrzewana lub wymienione rzeczy znajdują się na danym obszarze.

Istnieje przy tym ryzyko, iż przesłanka, o której mowa wyżej, będzie stanowić dla służb specjalnych podstawę do przeprowadzania swoistych „przeszukań trałowych”, a więc przeszukiwania dużej ilości pomieszczeń na danym obszarze z nadzieją znalezienia konkretnej osoby. Projektodawca w tym wypadku rezygnuje bowiem z wymogu, aby dokonanie przeszukania pomieszczeń i innych miejsc było związane z uzasadnionymi podstawami do przypuszczenia, że osoba podejrzana lub wymienione rzeczy tam się znajdują (art. 219 k.p.k.). Zastępuje je natomiast wymogiem, aby istniały uzasadnione podstawy do przypuszczenia, że osoba podejrzewana lub wymienione rzeczy znajdują się na danym obszarze.

Przy takiej przesłance służby będą uprawnione do przeszukiwania pomieszczeń mieszkalnych w całych dzielnicach. Zakładając więc, że np. domniemany terrorysta wsiadł na stacji metra Centrum w pociąg w kierunku Kabat, służby otrzymają kompetencje do tego, aby przeszukać wszystkie pomieszczenia na południe od stacji metra – Centrum. Wydaje się, że wymogiem minimum do tak szerokiej ingerencji w prywatność obywateli powinno być przynajmniej powiązanie jej z najwyższymi stopniami zagrożenia terrorystycznego, o którym mowa w przedmiotowym projekcie.

Jednocześnie projektodawca posługuje się w art. 23 projektu pojęciem „osoby podejrzewanej”, które jest nieznanym procedurze karnej. Kodeks postępowania karnego rozróżnia bowiem trzy kategorie osób znajdujących się w zainteresowaniu organów ścigania, czy też szerzej wymiaru sprawiedliwości:

¹⁹ S. Steinborn, Kodeks postępowania karnego. Komentarz do wybranych przepisów, LEX/el 2016.

- oskarżonego, tj. osobę, przeciwko której wniesiono oskarżenie do sądu, a także osobę, co do której prokurator złożył wniosek wskazany w art. 335 § 1 lub wniosek o warunkowe umorzenie *postępowania*.
- podejrzanego, tj. osobę, co do której wydano postanowienie o przedstawieniu zarzutów albo której bez wydania takiego postanowienia postawiono zarzut w związku z przystąpieniem do przesłuchania w charakterze podejrzanego.
- osobę podejrzaną, o której mowa w art. 192a k.p.k. lub 219 k.p.k.

Analiza projektu oraz jego lakonicznego uzasadnienia, nie pozwala na odgadnięcie szczegółowej treści używanego w nim pojęcia „osoba podejrzewana”. Na podstawie nazwy nie można wykluczyć, iż w wyniku jego pośpiesznej redakcji, doszło do mylnego użycia pojęcia „osoba podejrzewana” zamiast „osoba podejrzana”. Gdyby jednak uznać, że użycie tego pojęcia ma charakter celowy, to trudno określić charakter i pozycję procesową takiego podmiotu, a co za tym idzie - przysługujące mu gwarancje procesowe. W szczególności nie wiadomo, czy za osobę podejrzewaną należy uznać każdy podmiot znajdujący się w zainteresowaniu organów ścigania, czy też należy identyfikować ją wężiej, np. jako osobę, wobec której podjęto już czynności weryfikujące. Ta druga interpretacja zbliżałaby jednak rozumienie pojęcia „osoba podejrzewana” w kierunku znanej procedury „osoby podejranej” wskazując jednocześnie na błąd projektodawcy²⁰.

Na zakres zastosowania art. 23 i 24 projektu znaczny wpływ będzie miało także poszerzenie definicji pojęcia „przestępstwa o charakterze terrorystycznym”. Kodeksowa definicja stanowi, iż przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej, a także groźba popełnienia takiego czynu. Projektodawca proponuje, aby definicja ta obejmowała wszystkie czyny zagrożone karą pozbawienia wolności do lat 3, o ile zostały popełnione w jednym z opisanych wyżej celów.

W oczywisty sposób rozszerzenie tej definicji wpłynie na szersze zastosowanie projektowanej ustawy, co może nastęrczać wątpliwości z punktu widzenia szeregu uwag zgłoszonych do jej treści.

Niewątpliwie zmiana ta pozwala jednak także na włączenie w zakres pojęcia „przestępstwa o charakterze terrorystycznym” szeregu czynów zabronionych polegających na przygotowaniu do popełnienia określonego przestępstwa. Wśród czynów tych znajdują się m.in. przygotowanie zamachu na jednostkę sił zbrojnych RP (art. 140 § 3 k.k.), przygotowanie do sprowadzenia niebezpieczeństwa dla wielu osób poprzez sprowadzenie zagrożenia epidemiologicznego (art. 168 w zw. z art. 165 § 1 ust. 1k.k.),

²⁰ Nie jest jasne, jaka jest relacja między wykazem osób z art. 6 ust. 1 a „osobą podejrzewaną”, o której mowa w art. 23 projektu.

przygotowaniu do umieszczenia na statku powietrznym urządzenia zagrażającego bezpieczeństwu wielu osób (art. 168 w zw. z art. 167 § 1 k.k.).

Krytyczniej należy się natomiast odnieść do treści art. 24 projektowanej ustawy. Zgodnie z nim w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, jeżeli wymaga tego dobro postępowania przygotowawczego, postanowienie o przedstawieniu zarzutów można sporządzić na podstawie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych, w tym czynności, o których mowa w art. 7 projektowanej ustawy.

Podstawowy problem wiąże się z wykorzystaniem „informacji pochodzących z czynności operacyjno-rozpoznawczych”, na których przeprowadzenie sąd nie wyraził następczej zgody. Wydaje się, że w takim wypadku nie będzie miał zastosowania art. 168a k.p.k., w którym wprost mowa o „dowodach”. W ocenie HFPC pojęcia tego nie da się skutecznie odnieść do „informacji z czynności operacyjno-rozpoznawczej”, o której mowa w art. 24 projektu.

Co więcej, regulacja art. 24 projektu może prowadzić do ograniczenia prawa do obrony podejrzanego. W związku z tym, iż informacje gromadzone w ramach czynności operacyjno-rozpoznawczych mają charakter niejawni, przeglądanie akt postępowania, sporządzanie z nich odpisów i kopii będzie odbywało się w trybie określonym w art. 156 § 4 k.p.k., co samo w sobie jest dość uciążliwe. Nadto wydaje się, że poprzez użycie materiałów niejawnych dosyć częste zastosowanie będzie miała regulacja art. 156 § 5 k.p.k. pozwalająca odmówić udostępnienia akt postępowania stronom, ze względu na ochronę interesu państwa.

Art. 24 ust. 2 projektu stanowi, że do zastosowania tymczasowego aresztowania może dojść w przypadku podejrzenia popełnienia przestępstwa o charakterze terrorystycznym. Samoistną przesłanką zastosowania takiego środka jest uprawdopodobnienie popełnienia, usiłowania lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym. Proponowana zmiana rezygnuje więc z ugruntowanych rozwiązań pozwalających na stosowanie środków zapobiegawczych w wypadku spełnienia dwóch przesłanek – ogólnej i szczególnej. W zamian za to wprowadza jedną przesłankę o „mieszanym” charakterze. Przesłanka ta zastępuje wymóg stwierdzenia, na podstawie zebranych dowodów, dużego prawdopodobieństwa popełnienia przez podejrzanego zarzucanego mu czynu wymogiem jedynie uprawdopodobnienia tej okoliczności. Sąd nie będzie musiał więc badać tego, czy z dużym prawdopodobieństwem podejrzanym popełnił dany czyn. Będzie mógł poprzestać jedynie na ustaleniu, że mógł on taki czyn popełnić. Nawet najslabsze ustalenie wskazujące na ten fakt, będzie musiało być uznane za wypełniające przesłankę uprawdopodobnienia, niezbędną do zastosowania tymczasowego aresztowania.

Jednocześnie nie jest jasne, co będzie podstawą ustaleń sądu. Odwołanie poczynione w art. 24 ust. 2 do ust. 1 tegoż artykułu może sugerować, że sąd w toku rozstrzygania o 14-dniowym tymczasowym aresztowaniu będzie mógł się opierać na informacjach uzyskanych z czynności operacyjno-rozpoznawczych, niewprowadzonych do

postępowania w charakterze dowodu. Poza zgłoszoną już wątpliwością, czy rozwiązanie to nie utrudni prawa podejrzanego do obrony, wskazać należy, że informacje takie mogą być dla sądu nieweryfikowalne.

Z jednej strony sąd będzie stał przed koniecznością oceny informacji uzyskanej od np. informatora służb (nieutrwalonej w formie protokołu), z którym w dodatku nie miał on sam bezpośredniego kontaktu, z drugiej zaś będzie na nim spoczywała społeczna presja tymczasowego aresztowania domniemanego terrorysty. Te dwa elementy sprowadzą orzekanie o tymczasowym aresztowaniu z roli czynności prawnej do czynności faktycznej, w której 99,9% wniosków prokuratora będzie zasadne.

Jak wskazuje doktryna prawa konstytucyjnego „prawo do odwołania (od decyzji o pozbawieniu wolności – przyp. aut.) implikuje przyznanie sądowi odpowiednich uprawnień w zakresie prowadzenia postępowania dowodowego w celu wszechstronnego zbadania okoliczności pozbawienia wolności”²¹. Tymczasem proponowane rozwiązania wskazują jako podstawę tymczasowego aresztowania jedynie niewielki stopień prawdopodobieństwa popełnienia danego czynu. Jednocześnie zdają się sugerować, że prawdopodobieństwo to będzie można wykazać za pomocą informacji z czynności operacyjno-rozpoznawczych, które dla sądu stosującego tymczasowy areszt będą trudne do oceny i nieweryfikowalne. Kombinacja tych dwóch elementów, w połączeniu z presją społeczną i medialną stosowania tymczasowego aresztowania wobec domniemanego terrorysty, mogą powodować, że sądy będą sprowadzane do roli notariusza i pozbawione realnej możliwości dokonania oceny dowodów, a co za tym idzie kontroli zasadności detencji. Wydaje się, że takie rozwiązanie stoi w sprzeczności z gwarancjami *habeas corpus* ujętymi w ramach art. 41 Konstytucji.

Powstaje również pytanie, czy oparcie postanowienia o tymczasowym aresztowaniu na podstawie informacji uzyskanych z czynności operacyjno-rozpoznawczych będzie oznaczało, że czynności te będą musiały być udostępnione, zgodnie z regułą art. 249a k.p.k. podejrzanemu oraz jego obrońcy. Przy uznaniu, że informacje te nie mają charakteru dowodu, zgodnie z literalnym brzmieniem k.p.k. wymóg ten nie musiałby być w istocie spełniony. Na wątpliwości te, z uwagi na bardzo lakoniczne uzasadnienie przedmiotowego projektu nie da się jednak odpowiedzieć.

6. Ochrona praw cudzoziemców

Projekt ustawy posługuje się pojęciem „osoba niebędąca obywatelem polskim”, z kolei ustawa z 12 grudnia 2013 o cudzoziemcach²² zawiera definicję cudzoziemca i jest nim „każdy, kto nie posiada obywatelstwa polskiego”. Wydaje się, że projekt bez potrzeby wprowadza nowe pojęcie będące tożsamym z już funkcjonującym w polskim systemie prawa pojęciem cudzoziemca.

²¹ M. Safjan, L. Bosek (red.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Legalis/el 2016.

²² Dz. U. poz. 1650, ze zm.

Projekt wprowadza zmiany w ustawie z 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin²³ (art. 46 projektu). Dodawany jest art. 73c, który przenosi na ministra spraw wewnętrznych uprawnienie do wydawania decyzji o wydaleniu obywatela UE lub członka rodziny nie będącego obywatelem UE. Brak jest uzasadnienia, dla którego kompetencja ta została przeniesiona z wojewody na ministra, zwłaszcza, że do tej pory nie pojawiły się argumenty wskazujące na to, aby wojewodowie prowadzili postępowania w sprawie o wydalenie ww. kategorii cudzoziemców w sposób wadliwy. Przesłanką wydania takiej decyzji jest „obawa, że [osoby te] mogą prowadzić działalność terrorystyczną lub szpiegowską albo podejrzanych o popełnienie jednego z tych przestępstw”. Rozdział V ustawy o wjeździe na terytorium RP obywateli UE również przewiduje możliwość wydania decyzji o wydaleniu obywatelowi UE lub członkowi rodziny niebędącemu obywatelem UE, w oparciu o przesłankę zagrożenia dla bezpieczeństwa państwa (a w tej kategorii mieszczą się niewątpliwie osoby, które mogą prowadzić działalność terrorystyczną).

Projektowany art. 73 ust. 2 ustawy o wjeździe na terytorium RP przewiduje możliwość natychmiastowego przymusowego wykonania decyzji Ministra Spraw Wewnętrznych o wydaleniu z terytorium RP. Natychmiastowe i przymusowe wydalenie powoduje istotne ograniczenie konstytucyjnego prawa do odwołania się i prawa do sądu. W przypadku takiego wydalenia obywatel UE lub członek rodziny mogą nie mieć żadnej możliwości skutecznego złożenia odwołania czy skargi do sądu. Natomiast w przypadku złożenia takiego odwołania poważnego ograniczenia doznaje ich prawo do czynnego udziału w postępowaniu, jak i możliwość skorzystania z pozytywnego rozstrzygnięcia ich odwołania, gdyż cudzoziemiec może nie dowiedzieć się o wyniku sprawy.

Art. 54 pkt 2 projektu nowelizuje ustawę o cudzoziemcach i przenosi ze Straży Granicznej na ministra spraw wewnętrznych uprawnienie do wydawania decyzji o zobowiązaniu cudzoziemca do powrotu w sytuacji, gdy istnieje obawa prowadzenia działalności terrorystycznej lub szpiegowskiej. Także tu brak jest uzasadnienia, dla którego kompetencja ta została przeniesiona ze Straży Granicznej na ministra, zwłaszcza, że do tej pory nie pojawiły się argumenty wskazujące na to, aby Straż Graniczna prowadziła postępowania w sprawie o zobowiązanie do powrotu w sposób zasadniczo wadliwy. Także w tym wypadku projekt wprowadza możliwość natychmiastowego przymusowego wykonania decyzji wydanej przez ministra. Analogiczne rozwiązanie dotyczące pozostałych rodzajów decyzji o zobowiązaniu do powrotu zawiera art. 315 ust. 5 ustawy o cudzoziemcach, który pozwala na natychmiastowe wykonanie decyzji o zobowiązaniu do powrotu w sytuacji, gdy została ona wydana ze względów bezpieczeństwa.

Również w tym wypadku poważnemu ograniczeniu ulega skuteczność kontroli sądowej w sytuacji, gdy cudzoziemiec przebywa poza terytorium RP i poza terytorium UE. Ponadto, w wypadku takich spraw pojawia się kwestia braku dostępu do informacji niejawnych zgromadzonych przez służby, stanowiących podstawę decyzji do

²³ Dz. U. z 2014, poz. 1525, ze zm.

zobowiązaniu do powrotu. Zgodnie z art. 74 k.p.a. strona postępowania nie ma możliwości dostępu do akt sprawy w sytuacji, gdy zawierają one informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne” (a należy założyć, że w sprawach prowadzonych na podstawie przepisów ustawy takie informacje wystąpią). Tak więc w takich sprawach gwarancja prawa do obrony zostaje poważnie ograniczona.

7. Stopnie alarmowe – wpływ na prawa i wolności

Projekt przewiduje uregulowanie na poziomie ustawowym zasad wprowadzania stopni alarmowych powiązanych z prawdopodobieństwem wystąpienia zdarzenia o charakterze terrorystycznym²⁴. Kolejne stopnie wprowadza i zmienia Prezes Rady Ministrów po zasięgnięciu opinii Ministra Spraw Wewnętrznych oraz Szefa ABW. Jak wynika z uzasadnienia, w wypadku pojawienia się zagrożenia, w pierwszej kolejności zostaną wprowadzone stany alarmowe na podstawie ustawy antyterrorystycznej, a dopiero następnie – w razie takiej konieczności – stany nadzwyczajne uregulowane w odrębnych ustawach. Projekt próbuje zarysować przesłanki decydujące o wprowadzeniu kolejnych stopni alarmowych, jednak nie wskazuje, jakie będą skutki dla osób znajdujących się na terytorium, na którym wprowadzony został jeden z wyższych stopni alarmowych. Rozporządzenie Prezesa Rady Ministrów, które zostanie wydane na podstawie art. 15 ust. 5 projektu odnosi się do przedsięwzięć podejmowanych przez organy władzy publicznej. Może to rodzić wątpliwości, czy tryb pracy organów publicznych w przypadku kolejnych stopni nie powinien zostać uregulowany na poziomie ustawy. W projektowanej regulacji treść normy ustawowej zostanie dookreślona w formie rozporządzenia. Konsekwencje wprowadzenia poszczególnych stopni też powinny zostać uregulowane na poziomie ustawy, skoro będzie oddziaływać na sytuację obywateli.

Projekt próbuje również uregulować kwestię kierownictwa działań antyterrorystycznych (art. 17 i 18 projektu). Nie jest jednak jasne, przykładowo, kto sprawuje kierownictwo takich działań na terenie lotnisk, zaś w przypadku jednostek wojskowych - kto sprawuje kierownictwo takich działań wobec pracowników cywilnych takich jednostek.

Projekt przewiduje, że wprowadzając trzeci lub czwarty stopień alarmowy, Minister Spraw Wewnętrznych może zarządzić zakaz odbywania zgromadzeń publicznych lub imprez masowych na obszarze objętym stopniem alarmowym, „jeżeli jest to konieczne dla ochrony życia i zdrowia ludzi lub bezpieczeństwa publicznego”. Wydanie takiego zakazu, będzie miało bezpośredni (automatyczny) wpływ na decyzję właściwego organu jednostki samorządu terytorialnego, który na podstawie art. 20 ust. 2 będzie zobowiązany do wydania zakazu zgromadzenia lub decyzji o jego rozwiązaniu.

Może to rodzić istotne komplikacje szczególnie w wypadku prowadzonych już imprez masowych. Obecnie przepisy ustawy o bezpieczeństwie imprez masowych nakładają na organ podejmujący decyzję o przerwaniu imprezy masowej obowiązek oceny, czy

²⁴ Jak wynika z uzasadnienia projektu, obecnie system taki funkcjonuje w oparciu o zarządzenie z 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego i obejmuje jedynie organy administracji publicznej.

przerwanie imprezy masowej może spowodować zagrożenie bezpieczeństwa (art. 31 ust. 4a oraz art. 34a ust. 2 ustawy o bezpieczeństwie imprez masowych). Tymczasem w świetle projektowanego art. 20, właściwy organ jest zobowiązany – na podstawie wcześniejszej decyzji Ministra Spraw Wewnętrznych – do m.in. przerwania imprezy masowej. Pominięcie procedur oceny ryzyka (obowiązujących na podstawie ustawy o bezpieczeństwie imprez masowych) może stanowić realne zagrożenie bezpieczeństwa dla osób uczestniczących w takim wydarzeniu.

Art. 20 ust. 3 projektu przewiduje możliwość złożenia odwołania od decyzji o zakazie do właściwego sądu. Przepis w proponowanym kształcie nie przewiduje jednak terminu na złożenie takiego odwołania. Projektodawca powinien uregulować, w jakim zakresie stosuje się w takiej sytuacji przepisy m.in. Prawa o zgromadzeniach. Przedmiotem kontroli ze strony sądu będzie w takim wypadku *de facto* decyzja Ministra Spraw Wewnętrznych. Dla przeprowadzenia rzetelnej kontroli sądowej wobec zakazu zgromadzenia wydanego na podstawie ustawy antyterrorystycznej, kluczowe znaczenie będzie miała możliwość weryfikacji przesłanek podjęcia takich decyzji, co może okazać się z kolei utrudnione. Podstawą wprowadzenia trzeciego lub czwartego stopnia alarmowego mogą być bowiem uzyskane wiarygodne i potwierdzone informacje, które najprawdopodobniej będą objęte jedną z klauzul ochrony informacji niejawnych. Istnieje zatem poważna wątpliwość, czy projektowany kształt zaproponowanych regulacji będzie umożliwiał rzetelne zweryfikowanie decyzji Ministra Spraw Wewnętrznych. To z kolei będzie miało konsekwencje dotyczące wolności zgromadzeń w Polsce.

8. Specjalne użycie broni (tzw. strzał snajperski)

Projekt wprowadza pojęcie tzw. specjalnego użycia broni, polegające na możliwości takiego jej zastosowania, którego skutkiem będzie śmierć osoby (art. 22 projektu). Możliwość skorzystania z tej kompetencji będzie obejmować działania kontrterrorystyczne (tj. podejmowane wobec sprawców, osób przygotowujących lub pomagających w dokonaniu przestępstwa o charakterze terrorystycznym, prowadzone w celu wyeliminowania bezpośredniego zagrożenia dla życia, zdrowia oraz mienia), jeżeli jest to niezbędne dla przeciwdziałania zamachowi, a inne użycie broni jest niewystarczające. Projektowany przepis przewiduje nawet możliwość wydania przez osobę kierującą działaniami kontrterrorystycznymi rozkazu specjalnego użycia broni przez funkcjonariusza.

W ocenie Helsińskiej Fundacji Praw Człowieka, takie rozwiązanie jest niedopuszczalne. Trybunał Konstytucyjny w wyroku z 30 września 2008 r. dotyczącym możliwości zestrzelenia samolotu porwanego przez terrorystów, wskazał, że w polskich warunkach ustrojowo-politycznych nie wydaje się zasadne konstruowanie szczególnych koncepcji teoretyczno- i filozoficzno-prawnych „zawieszenia” czy też „modyfikacji” gwarancji praw obywatelskich, koniecznych w okresie „wojny z terroryzmem”. Istniejące obecnie ogólne uregulowania, dotyczące stosowania w takim wypadku prawnokarnej konstrukcji „stanu wyższej konieczności” w przypadku użycia broni palnej jest całkowicie wystarczające, aby podejmować działania służące zapewnieniu bezpieczeństwa. Tym bardziej niezrozumiała jest konstrukcja oparta na możliwości wydania rozkazu przez

dowódcę grupy, którego ocena danej sytuacji może być o wiele gorsza, niż ocena funkcjonariusza, który w danej sytuacji użyje broni. W dalszym ciągu dla prawidłowego zabezpieczenia porządku publicznego, kluczowe znaczenie ma kwestia odpowiedniej rekrutacji oraz szkolenia funkcjonariuszy, jak również kwestia zagwarantowania odpowiedzialności za wykonywane obowiązki, w tym również użycie broni palnej. Z tego względu projektowany przepis jest zbędny oraz nieproporcjonalny.

9. Zagrożenia dla swobody wypowiedzi

Oprócz wspomnianej w pkt. 4.3 niniejszej opinii możliwości blokowania „danych informatycznych” lub „usług teleinformatycznych” w systemie teleinformatycznym, projekt ustawy zawiera dodatkowo szereg innych rozwiązań mogących godzić w swobodę wypowiedzi. Dotyczy to w szczególności regulacji, które będą umożliwiały poważną ingerencję w informacje znajdujące się pod ochroną tajemnic zawodowych, m.in. tajemnicy dziennikarskiej obejmującej ochronę dziennikarskich źródeł informacji. Projektodawca nie przewidział bowiem jednocześnie żadnych szczególnych zabezpieczeń, które zapewniłyby, że zaproponowane w projekcie ustawy środki nie będą służyły obejściu gwarancji wynikających z tajemnic zawodowych. Do grup najbardziej narażonych na nadużycia związane z rozszerzeniem kompetencji ABW i innych podmiotów w projekcie ustawy są dziennikarze i ich informatorzy. Odnosi się to przede wszystkim do takich elementów projektu, jak daleko idące środki inwigilacji podejmowane wobec osób niebędących obywatelami Polski (art. 8 projektu; w kontekście dziennikarskim grupą narażoną na inwigilację mogą być w tym przypadku zagraniczni korespondenci) czy obowiązek rejestracji kart pre-paid (art. 41). Są to rozwiązania umożliwiające pozyskanie danych, które mogą prowadzić do nieuprawnionej identyfikacji osób udzielających informacji dziennikarzom.

Zapewnienie odpowiednich gwarancji tajemnicy dziennikarskiej, w tym gwarancji nieujawniania danych dziennikarskich informatorów, jest niezbędnym elementem realizacji swobody wypowiedzi i wolności mediów (art. 54 i art. 14 Konstytucji oraz art. 10 EKPC, zob. też wyroki ETPC ws. *Goodwin p. Zjednoczonemu Królestwu*²⁵, *Sanoma Uitgevers B.V p. Holandii*²⁶). W rekomendacji Komitetu Ministrów Rady Europy o prawie dziennikarzy do nieujawniania swoich źródeł informacji²⁷ podkreślono, że niedopuszczalne są wszelkie działania podejmowane przez organy państwa wobec dziennikarzy, jeśli mają na celu obejście prawa do zachowania w tajemnicy tożsamości dziennikarskiego źródła informacji. Dotyczy to wszelkich form inwigilacji, takich jak: stosowanie podsłuchu, analiza aktywności dziennikarza w internecie, analiza billingów, śledzenie dziennikarza czy wykorzystywanie monitoringu wizyjnego do ustalenia, z kim się spotyka. Zbyt swobodny dostęp służb do narzędzi umożliwiających inwigilację czy poznanie danych dziennikarskiego informatora w inny sposób ma negatywny wpływ na

²⁵ Wyrok ETPC z 27 marca 1996 r., skarga nr 28957/95.

²⁶ Wyrok ETPC z 14 września 2010 r. (Wielka Izba), skarga nr 38224/03.

²⁷ Rekomendacja Komitetu Ministrów Rady Ministrów R (2000)7 z dnia 8 marca 2000 r. w sprawie prawa dziennikarzy do nieujawniania swoich źródeł informacji.

gotowość źródeł do ujawniania mediom faktów istotnych z punktu widzenia interesu publicznego. Jak wielokrotnie podkreślał ETPC, bez odpowiedniej ochrony, informatorzy dziennikarzy mogą odmawiać pomocy mediom w informowaniu społeczeństwa o sprawach wzbudzających zainteresowanie publiczne. W rezultacie, ważna rola prasy – publicznego kontrolera („public watchdog”) – może ulec osłabieniu (*Goodwin p. Zjednoczonemu Królestwu*). Co więcej, działania zmierzające do ustalenia tożsamości źródeł dziennikarskich w sposób niezależny od dziennikarza (np. przez analizę metadanych), są uznawane za środek znacznie bardziej drastyczny i groźny, niż żądanie ujawnienia informatora mające miejsce podczas bezpośredniego przesłuchania. Z orzecznictwa ETPC (zob. sprawy *Roemen i Schmitt p. Luksemburgowi*²⁸ oraz *Ernst i Inni p. Belgii*²⁹) wynika bowiem, że depozytariuszem tajemnicy podczas przesłuchania jest sam dziennikarz, który ma wówczas rzeczywistą kontrolę nad jej ujawnieniem. Tymczasem informator, wiedząc, że prawo zezwala na podjęcie wielu niezależnych od dziennikarza działań, które mogą doprowadzić do ujawnienia jego tożsamości, nie może polegać na zaufaniu do przedstawicieli mediów. Tym samym może nie być skłonny do przekazywania dziennikarzom ważnych informacji, utrudniając realizację przynależnej im funkcji kontrolnej. Łatwy dostęp organów państwowych do wszelkich środków inwigilacji, które mogą być podejmowane także wobec dziennikarzy, stwarza zatem dla informatora, w kontekście jego poczucia bezpieczeństwa, znacznie groźniejszą sytuację – traci on pewność, że jego dane pozostaną pod ochroną tajemnicy dziennikarskiej.

Dlatego też, w ocenie HFPC, istotne jest wprowadzenie do projektu ustawy szczegółowych rozwiązań zapewniających efektywną ochronę informacjom objętym tajemnicą zawodową, w szczególności tajemnicą dziennikarską. Mimo, że tajemnica ta jest aktualnie chroniona na poziomie ogólnym na mocy art. 15-16 prawa prasowego oraz przez art. 180 k.p.k. w ramach postępowania karnego, rozwiązania proponowane w projekcie ustawy wymykają się istniejącym ramom prawnym, które mogą nie być wystarczające dla ochrony dziennikarskich źródeł informacji, jeśli ustawa weszłaby w życie w obecnym kształcie zaproponowanym w omawianym projekcie.

Projektowany obowiązek rejestracji tzw. kart pre-paid powinien również skutkować weryfikacją obowiązujących obecnie regulacji dotyczących dostępu służb do danych telekomunikacyjnych. Wielokrotnie w dyskusji publicznej wskazywano bowiem, że obowiązujące regulacje dotyczące dostępu służb do tego typu danych, w tym brak m.in. uprzedniej kontroli sądu, wynikały z faktu dużej liczby numerów niezarejestrowanych i braku wiedzy o danych abonenta. Zwiększony zakres danych dostępnych u operatora powinien zatem skutkować wzmocnieniem kontroli uprzedniej nad pozyskiwaniem tych danych przez służby. Co więcej, nie jest jasne, w jaki sposób rejestracja kart pre-paid przełoży się na skuteczniejsze przeciwdziałanie zdarzeniom o charakterze terrorystycznym. Tym bardziej, że przez ostatnie lata służby w oparciu o prowadzoną analizę wielokrotnie były w stanie ustalić tożsamość abonenta.

²⁸ Wyrok ETPC z 25 lutego 2003 r., skarga nr 51772/99.

²⁹ Wyrok ETPC z 15 lipca 2003 r., skarga nr 33400/96.

Projekt ustawy wymaga ponadto przeprowadzenia analizy wpływu innych proponowanych w nim regulacji na wolność słowa. Art. 37 projektu nowelizujący ustawę – Prawo lotnicze przewiduje np. możliwość zniszczenia, unieruchomienia albo przejęcia kontroli nad lotem bezzałogowego statku powietrznego (w tym modelu latającego) przez Policję, Straż Graniczną, Biuro Ochrony Rządu, ABW, CBA, SKW, SWW, Służbę Celną, Służbę Więzienną, żołnierzy Żandarmerii Wojskowej i Sił Zbrojnych RP oraz pracowników specjalistycznych uzbrojonych formacji ochronnych. Wątpliwości wzbudzają nieostre przesłanki, w oparciu o które będzie można dokonać ww. czynności, szeroki krąg podmiotów uprawnionych do ich dokonania oraz brak szczegółowej procedury weryfikacji ich zgodności z prawem. W szczególności jednak należy zaznaczyć, że proponowana regulacja nie uwzględnia tego, że bezzałogowe statki powietrzne stają się dziś coraz częściej kolejnym narzędziem wykorzystywanym przez dziennikarzy do gromadzenia informacji (takim jak np. aparaty fotograficzne) i w związku z tym ich stosowanie przez przedstawicieli mediów powinno być chronione na mocy gwarancji swobody wypowiedzi. Można wskazać na liczne przykłady użycia tzw. dronów przez dziennikarzy w interesie publicznym, które dotyczyły np. relacjonowania przebiegu i weryfikacji wielkości zgromadzeń publicznych, dostarczania informacji o rozmiarach katastrof naturalnych bądź informacji o skali działań wojennych i o ich ofiarach, a także przekazywania informacji z innych miejsc, do których bezpośredni dostęp dziennikarzy byłby niemożliwy z uwagi na fizyczne ograniczenia lub zagrożenie dla bezpieczeństwa³⁰. Warto podkreślić również, że na fakt, iż korzystanie przez dziennikarzy z tzw. dronów mieści się w ramach wolności słowa oraz na obowiązek tworzenia przez państwo prawa, które zapewnia mediom odpowiednie gwarancje dla używania tych urządzeń w celach związanych z wykonywaniem funkcji publicznego stróża, zwraca wprost uwagę Specjalna Sprawozdawczyni OBWE ds. wolności słowa w komunikacie dotyczącym stosowania dronów w dziennikarstwie (nr 2/2016). Dlatego też projektodawca powinien wziąć pod uwagę, że nieuzasadniona ingerencja w korzystanie z ww. urządzeń przez dziennikarzy, stosujących je do celów gromadzenia materiałów do publikacji, może oznaczać utrudnianie krytyki prasowej sprzeczne z art. 6. ust. 4 prawa prasowego.

9. Konkluzje

Projekt ustawy o działaniach antyterrorystycznych w celu zapewnienia bezpieczeństwa publicznego przyznaje służbom nowe kompetencje poważnie ingerujące w prawa i wolności, nie stwarzając żadnych narzędzi nadzoru nad sposobem wykonywania tych kompetencji. Główne źródło zagrożenia, któremu ustawa ma zapobiegać, tj. terroryzm jest niezwykle skomplikowanym zjawiskiem społecznym. Doświadczenia i przyczyny zamachów w Brukseli oraz w Paryżu powinny zostać przeanalizowane wieloaspektowo i nie mogą sprowadzać się do konkluzji o potrzebie przyznania służbom nowych uprawnień, które będą realizowane bez żadnego zewnętrznego nadzoru. Takie rozwiązanie jest tym bardziej niebezpieczne, że może się opierać – jak wskazuje projekt rozporządzenia określającego zdarzenia o charakterze terrorystycznym – o przesłanki

³⁰ D. Goldberg, M. Corcoran, R. G. Picard, Remotely Piloted Aircraft Systems and Journalism. Opportunities and Challenges of Drones in News Gathering, University of Oxford, June 2013.

prowadzące do dyskryminacji ze względu na pochodzenie etniczne czy wyznawaną religię. Kształt projektu wpisuje się w negatywną narrację skierowaną przeciwko cudzoziemcom. Z punktu widzenia przyczyn terroryzmu, projektowane rozwiązania mogą przynieść skutek odwrotny do zamierzonego.

Pojemność zaproponowanego pojęcia „zdarzenia o charakterze terrorystycznym” i związana z tym możliwość korzystania przez władzę wykonawczą z nowych uprawnień, może stanowić zagrożenie dla pewności prawa oraz poczucia bezpieczeństwa obywateli. Co więcej, niektóre z przewidzianych uprawnień, m.in. tzw. strzał snajperski, w sposób bezpośredni zagrażają bezpieczeństwu.

Projekt całkowicie pomija wypracowany w ciągu ostatnich 25 lat krajowy i międzynarodowy standard ochrony praw i wolności, m.in. orzecznictwo Europejskiego Trybunału Praw Człowieka i Trybunału Konstytucyjnego. Co więcej, znaczna część projektowanych rozwiązań powiela obowiązujące regulacje, uszczegóławia je, tworząc *de facto* ustawę do spraw ścigania jednej (acz pojemnej i nieostrej) kategorii przestępstw.

W ocenie Helsińskiej Fundacji Praw Człowieka projekt ustawy o działaniach antyterrorystycznych wymaga dalszych prac legislacyjnych, w szczególności usunięcia rozwiązań polegających na przyznaniu służbom nowych uprawnień wkraczających w prawa i wolności, które pozostają poza jakąkolwiek niezależną zewnętrzną kontrolą. Co więcej, dalsze prace nad ustawą powinny zostać uzupełnione o rzetelne i szerokie konsultacje społeczne, w szczególności z udziałem ekspertów ds. bezpieczeństwa. Prawo przyjmowane pośpiesznie zagraża zarówno wolności, jak i bezpieczeństwu.

Z wyprzedzeniem stwierdzam,



Helsińska Fundacja Praw Człowieka
SEKRETARZ ZARZĄDU
Piotr Kłodoczny
Piotr Kłodoczny