# Przegląd prac konkursowych
# Edycja VII (2016/2017)

**Zespół redakcyjny** Elżbieta Dąbrowska (sekretarz Redakcji)
Grażyna Osuchowska (redakcja, korekta)
Agnieszka Dębska (skład)

**Projekt okładki** Radosław Kostyra



**ISBN 978-83-938217-8-5**

Wszystkie zamieszczone artykuły wyrażają poglądy autorów

**Agencja Bezpieczeństwa Wewnętrznego**
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota” w Emowie
05-462 Wiązowna, ul. Nadwiślańczyków 2

**Redakcja**
tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 645
e-mail: redakcja.pbw@abw.gov.pl
www.abw.gov.pl

**Materiał zamknięto i oddano do druku w styczniu 2019 r.**

**Druk:** Biuro Logistyki
Agencji Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
tel. (+48) 22 58 57 657

# SPIS TREŚCI

## Szanowni Państwo,

od 2011 r. Agencja Bezpieczeństwa Wewnętrznego jest organizatorem konkursu Szefa ABW na najlepszą pracę dyplomową dotyczącą bezpieczeństwa wewnętrznego państwa. Cieszy się on dużym zainteresowaniem. Co roku na konkurs wpływa kilkadziesiąt prac licencjackich, magisterskich, a od 2017 r. – również doktorskich z renomowanych polskich uczelni. Treści w nich prezentowane stanowią ciekawe ujęcia tematów konkursowych, obejmujących m.in. takie zagadnienia z zakresu szeroko pojętego bezpieczeństwa narodowego, jak: rola i zadania służb specjalnych w demokratycznym państwie prawa i w państwach autorytarnych, konstytucyjne prawa obywateli a uprawnienia służb specjalnych czy bezpieczeństwo Polski i Europy w XXI wieku – zagrożenia i wyzwania.

Doceniając wysiłek uczestników konkursu, Agencja postanowiła wydać fragmenty nagrodzonych prac w ramach „Biblioteki Przeglądu Bezpieczeństwa Wewnętrznego". W wydaniu tym znalazły się prace laureatów siódmej edycji konkursu (lata 2016/2017).

Z przyjemnością polecamy lekturę tej publikacji. Mamy nadzieję, że poszerzy ona Państwa wiedzę oraz będzie stanowić inspirację dla osób, których zainteresowania naukowe oscylują wokół zagadnień dotyczących problematyki bezpieczeństwa naszego kraju.

**Redakcja**
**„Przeglądu Bezpieczeństwa Wewnętrznego"**

**Maciej Białek**

# Wojna hybrydowa a bezpieczeństwo Rzeczpospolitej Polskiej[1]

## 1. Pojęcie wojny hybrydowej

Obecna sytuacja polityczno-wojskowa na wschodzie Ukrainy i Półwyspie Krymskim, a także sposób relacjonowania jej przez światowe i polskie media może przeciętnemu odbiorcy informacji dawać do zrozumienia, że pojęcie wojna hybrydowa wymyślili Rosjanie i zastosowali w praktyce pierwszy raz w historii na początku 2014 r. Rzeczywistość jest jednak odmienna.

Słownikowa definicja określa hybrydę jako (…) *coś, co składa się z różnych elementów, często do siebie niepasujących*[2]. Wojna zaś, w klasycznym XX-wiecznym rozumieniu, oznacza (…) *zorganizowaną (przygotowaną) formę konfliktu zbrojnego między państwami, narodami, blokami państw i organizacjami niebędącymi państwami/narodami, jako kontynuację polityki (ideologii, religii) środkami przemocy, których głównym wyrazem jest walka zbrojna w celu osiągnięcia określonych interesów politycznych, ekonomicznych lub ideologicznych (religijnych)*[3]. Na tym etapie rozważań można zatem przyjąć, że wojna hybrydowa to taka wojna, w której co najmniej jedna ze stron konfliktu prowadzi działania za pomocą metod, form i środków nieprzystających do siebie na pierwszy rzut oka, różniących się od siebie.

Za teoretycznym określeniem wojny hybrydowej na płaszczyźnie naukowej stoją amerykańscy analitycy wojskowi[4]. W 2002 r. William J. Nemeth, major Korpusu Piechoty Morskiej USA, opublikował pracę poświęconą analizie wojny rosyjsko-czeczeńskiej[5]. Stwierdził w niej, że hybrydowość owego konfliktu była spowodowana różnorodnym charakterem czeczeńskiego społeczeństwa, co bezpośrednio wpłynęło na sposób

[1] Fragment pracy magisterskiej pt. *Wojna hybrydowa a bezpieczeństwo Rzeczypospolitej Polskiej* (Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Wydział Prawa i Administracji). Praca zajęła III miejsce w siódmej edycji *Ogólnopolskiego konkursu Szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa* (edycja 2016/2017). Autor wykorzystał rozdział 1 pt. *Wojna hybrydowa a współczesna Europa*, podrozdziały: 1 – *Pojęcie wojny hybrydowej* i 2 – *Zagrożenie wojną hybrydową ze strony Federacji Rosyjskiej*; rozdział 2 pt. *Regulacje stanów nadzwyczajnych w kontekście przeciwdziałania zagrożeniom hybrydowym*, podrozdziały: 2 – *Wybrane regulacje stanu wojennego w odniesieniu do potencjalnego zagrożenia hybrydowego na terytorium Polski* i 3 – *Instytucje stanu wyjątkowego i stanu klęski żywiołowej wobec potencjalnego zagrożenia hybrydowego na terytorium Polski*; rozdział 3 pt. *Zarządzanie kryzysowe i ochrona cyberprzestrzeni jako narzędzia w walce z zagrożeniami hybrydowymi w Polsce*, podrozdział 4 – *Wojna hybrydowa w cyberprzestrzeni – zagrożenia dla Polski.*

[2] *Słownik języka polskiego PWN*, http://sjp.pwn.pl/slowniki/hybryda.html [dostęp: 3 I 2017].

[3] *Słownik terminów z zakresu bezpieczeństwa narodowego*, B. Zdrodowski (red.), Warszawa 2008, s. 158.

[4] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne", Warszawa 2015, s. 40.

[5] W.J. Nemeth, *Future war and Chechnya: A case for hybrid warfare*, Monterey 2002, http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1&isAllowed=y [dostęp: 3 I 2017].

prowadzenia przez nie działań zbrojnych[6]. Według niego Czeczeni łączą w sobie elementy nowoczesnej religijności i politycznych teorii z tradycyjną organizacją społeczną i zachowaniem obyczajów[7]. Nemeth wskazuje, że powyższe cechy społeczeństw decydują o charakterze prowadzonej wojny, a jej hybrydowa postać jest widoczna w:

1) organizacji wojskowej, która odzwierciedla poziom rozwoju społeczno-politycznego, a teoria i doktryna wojskowa jest odbiciem norm panujących w danej wspólnocie,
2) sile militarnej rozumianej inaczej niż w zachodnich koncepcjach, która jest przez nie kwestionowana,
3) możliwości używania przez własne siły do celów strategicznych zaawansowanych technologicznie systemów, w sposób wykraczający poza ich pierwotne przeznaczenie,
4) asymetrii w walce, która jest nie tylko różnicą w możliwościach i sposobach jej prowadzenia, lecz także w obowiązujących normach społecznych i stopniu akceptacji zasad międzynarodowych,
5) zrozumieniu przez państwa zachodnie, że normy istniejące w obszarze euroatlantyckim są obce społeczeństwom hybrydowym, co jest niekorzystne dla dyplomatów oraz sił zbrojnych tych państw podczas negocjacji lub walki,
6) nowym paradygmacie, w którym zakłada się wojnę prowadzoną w coraz większym stopniu między państwami a aktorami niepaństwowymi[8].

Inny amerykański wojskowy Frank G. Hoffman, na podstawie badań różnych rodzajów konfliktów oraz Strategii Bezpieczeństwa Narodowego USA z 2005 r., stwierdził, że wojny hybrydowe (…) *zawierają zestaw różnych sposobów walki, wliczając w to działania niekonwencjonalne, nieregularne taktyki i formacje, akty terrorystyczne, w tym masową przemoc i gwałt, oraz działania przestępcze*[9]. Wojna hybrydowa może być prowadzona pomiędzy dwoma państwami bądź też z udziałem różnych podmiotów niepaństwowych. Uczestniczą w niej różne oddziały lub jeden większy oddział (wojskowy, paramilitarny, służb specjalnych itp.), a ich działania są podporządkowane osiągnięciu efektu synergii w fizycznym i psychologicznym wymiarze konfliktu. Synergia może być osiągnięta na wszystkich poziomach wojny – operacyjnym, taktycznym i strategicznym[10]. Widoczny jest w tym momencie psychologiczny wymiar walki, który oprócz fizycznego zniszczenia przeciwnika jest uważany za integralną część działań hybrydowych. Czynnik psychologiczny w prowadzeniu wojen hybrydowych pojawia się w większości opracowań na ten temat i jest traktowany jako element niezbędny do tego, aby mówić o hybrydowości danego konfliktu. Także Nemeth pisał o czynniku psychologicznym w kontekście konfliktu rosyjsko-czeczeńskiego, stwierdzając

[6] Tamże, s. 71.
[7] Tamże.
[8] Zob. tamże, s. 73–76.
[9] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, http://www.potomac-institute.org/images/stories/publications/potomac_hybridwar_0108.pdf, s. 29 [dostęp: 4 I 2017].
[10] Tamże, s. 8.

jednoznacznie, że to Czeczeni potrafili skuteczniej niż Rosjanie prowadzić operacje psychologiczne[11].

Hoffman uznał wojnę Izraela z Hezbollahem z 2006 r. za klasyczny przykład nowoczesnego konfliktu hybrydowego[12]. Jako uzasadnienie podaje między innymi, że bojownicy Hezbollahu, którzy są podmiotem niepaństwowym, potrafili rzucić wyzwanie zachodniemu modelowi prowadzenia działań zbrojnych i wykorzystywać słabe punkty Sił Obronnych Izraela. Wskazuje także na skuteczne połączenie miejskiej partyzantki z wykorzystaniem nowoczesnej technologii przez zdecentralizowane i świetnie wyszkolone jednostki Hezbollahu, które potrafiły urządzać zasadzki i maskować się wśród ludności cywilnej. Bojownicy tej organizacji umieli także podsłuchiwać telefony komórkowe izraelskich żołnierzy oraz odkodowywać ich częstotliwości radiowe, używali także ciężkich pocisków przeciwokrętowych i przeciwpancernych. Wszystkie te działania były obudowane efektownymi dla odbiorców operacjami informacyjnymi, na czele z pokazywaniem brutalności żołnierzy izraelskich i wychwalaniem swoich, często małych, sukcesów[13].

Wyżej wspomniani autorzy wywarli duży wpływ na upowszechnienie wśród amerykańskich wojskowych i analityków wiedzy na temat znaczenia wojen hybrydowych, co przekładało się na tworzenie kolejnych definicji tego zjawiska. W podręczniku polowym z 2011 r., przygotowanym przez dowództwo US Army dla amerykańskich żołnierzy, zagrożenie hybrydowe określono jako zróżnicowaną i dynamiczną kombinację sił regularnych i nieregularnych oraz elementów kryminalnych, które są połączone w celu osiągnięcia korzystnych wyników. Przeciwnik hybrydowy może również wykorzystywać globalne sieci komputerowe, żeby wpływać na postrzeganie konfliktu przez światową opinię publiczną i ją kształtować[14]. John McCuen za k o n f l i k t h y b r y d o w y uznał (…) *walkę przeciw uzbrojonemu wrogowi i szerzej walkę o kontrolę i poparcie miejscowej ludności w strefie walki, poparcie interweniujących państw na wewnętrznym froncie oraz poparcie społeczności międzynarodowej*[15]. Mocniej od samej walki zbrojnej akcentuje on „wojnę o dusze" tubylców, sojuszników i światowej opinii publicznej. Ten element ma ogromne znaczenie już po właściwym starciu zbrojnym, gdyż w tym momencie jest potrzebna stabilizacja polityczna, ekonomiczna, społeczna i kulturowa danego terytorium. Artur Gruszczak stwierdza, że właśnie w tej fazie, w której następuje przenikanie się siły militarnej z cywilnym zarządzaniem sytuacją pokonfliktową, hybrydowość konfliktu może się ujawnić z całą mocą i stanowić o poważnej zmianie celów strategicznych, operacyjnych i taktycznych[16].

[11] Zob. W.J. Nemeth, *Future war and Chechnya*…, s. 57–59.
[12] F.G. Hoffman, *Conflict in the 21st Century*..., s. 35.
[13] Zob. tamże, s. 35–42.
[14] *US Army, Field Manual 3-0 Operations C-1*, Washington 2011, https://fas.org/irp/doddir/army/fm3-0.pdf, s. 1–5 [dostęp: 7 I 2017].
[15] R.W. Glenn, *Thoughts, on „Hybrid" Conflict*, „Small Wars Journal" z 2 marca 2009 r., http://smallwarsjournal.com/mag/docs-temp/188-glenn.pdf, s. 3 [dostęp: 7 I 2017].
[16] Zob. A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red.), Warszawa 2011, https://www.bbn.gov.pl/download/1/8729/Asymetriaihybrydowoscstarearmiewobecnowychkonfliktow.pdf, s. 14–16 [dostęp: 8 I 2017].

W Polsce roboczą definicję wojny hybrydowej zamieściło na swojej stronie internetowej Biuro Bezpieczeństwa Narodowego. Ma ona na celu swoiste uporządkowanie dyskusji na ten temat i rozwój świadomości społecznej o współczesnym bezpieczeństwie. Wojna hybrydowa jest w niej określona jako (…) *wojna łącząca w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp.*[17]

Po przedstawieniu wojny hybrydowej według zachodniej, a precyzyjniej mówiąc – amerykańskiej teorii sztuki wojennej, naturalne w kontekście obecnej sytuacji międzynarodowej wydaje się zaprezentowanie pojmowania tego zagadnienia przez rosyjskich analityków, strategów i przywódców politycznych. Na początku koniecznie należy zaznaczyć, że przed konfliktem na Ukrainie w rosyjskim dyskursie termin „wojna hybrydowa" prawie się nie pojawiał. Jeśli jednak był on już używany, to w odniesieniu do amerykańskich interwencji w Afganistanie i Iraku i walki przeciw partyzantom i powstańcom islamskim[18]. Po aneksji Krymu i nasileniu walk we wschodnich obwodach Ukrainy ten termin stał się jednak kolejnym elementem walki propagandowej pomiędzy szeroko pojmowanym Zachodem a Kremlem. Według Rusłana Puchowa, dyrektora Centrum Analiz Strategii i Technologii w Moskwie, Rosja nie prowadzi na Ukrainie żadnej wojny hybrydowej, której przejawami miałyby być nowe i nieznane wcześniej rozwiązania militarne i pozamilitarne – w tym użycie na szeroką skalę wojsk powietrznodesantowych i sił specjalnych w połączeniu z działaniami informacyjnymi, psychologicznymi i radioelektronicznymi. Uważa także, że Rosja przeprowadziła swoją operację przy maksymalnym wykorzystaniu istniejących warunków, natomiast przypisywanie jej przez zachodnich oficjeli stosowania nowej, groźnej taktyki, jest jedynie próbą zdyskredytowania tego kraju na arenie międzynarodowej[19]. Podobne stanowisko reprezentują Andriej Manojło, były funkcjonariusz Federalnej Służby Bezpieczeństwa, profesor Państwowego Uniwersytetu Moskiewskiego, oraz Aleksandr Bartosz, członek korespondent Akademii Nauk Wojskowych Sztabu Generalnego Sił Zbrojnych FR. Uznają oni, że wojny hybrydowe to wymysł amerykańskich wojskowych, którzy dzięki temu realizują swoje globalne interesy, osłabiając w ten sposób swoich największych przeciwników – Rosję i Chiny, m.in. przez inicjowanie tzw. kolorowych rewolucji (jak np. na Ukrainie w 2004 r. i 2013 r.). Te działania uznaje on za pewnego rodzaju zaczątek dalszych działań hybrydowych[20].

Takie oficjalne postawienie sprawy przez Rosjan nie oznacza bynajmniej, że działania określane przez Zachód jako hybrydowe są nieobecne w ich teorii i praktyce wojskowej

[17] *(Mini)słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 8 I 2017].

[18] M. Wojnowski, *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne", Warszawa 2015, s. 10.

[19] Zob. tamże, s. 11–12.

[20] Zob. tamże, s. 15–16.

bądź politycznej. Używając własnego zestawu pojęć, poszczególne elementy wojen hybrydowych są wpisywane do urzędowych dokumentów, a wojskowi najwyższego szczebla oraz cywilni doradcy polityczni i naukowcy podkreślają ich znaczenie dla bezpieczeństwa narodowego. Ma to swój bardzo ważny kontekst historyczny i geopolityczny, który zostanie szerzej omówiony w kolejnym podrozdziale. Szef Sztabu Generalnego Sił Zbrojnych FR gen. Walerij Gierasimow przewiduje, że w XXI wieku wojny będą prowadzone z większym niż w przeszłości udziałem instrumentów politycznych, ekonomicznych i humanitarnych wraz z manipulowaniem umysłami ludzi zamieszkujących rejon konfliktu. Środki militarne, w tym wojnę informacyjną i operacje specjalne, uważa on za element wspierający powyższe działania, natomiast otwarte użycie u zbrojonych oddziałów ma być tylko przypieczętowaniem sukcesu w końcowej fazie konfliktu. Duży nacisk kładzie także na nowoczesne technologie informacyjne, które mogą być środkiem osłabiania potencjału wojskowego przeciwnika[21]. W zaktualizowanej w 2014 r. *Doktrynie Wojennej FR*[22] można zauważyć nawiązania do działań, które wpisują się w ogólne koncepcje wojen hybrydowych. W pkt 12. *Doktryny* jako jedne z zewnętrznych zagrożeń wojennych dla FR zidentyfikowano m.in.: działalność międzynarodowych radykalnych ugrupowań zbrojnych, a w rejonach przygranicznych – prywatnych zagranicznych organizacji paramilitarnych; wykorzystywanie w celach wojskowo-politycznych technologii informacyjnych i komunikacyjnych do prowadzenia działań sprzecznych z prawem międzynarodowym; istnienie w państwach graniczących z FR wrogich reżimów, których polityka jest zagrożeniem dla FR oraz wywrotową działalność służb i organizacji specjalnych innych państw i ich koalicji przeciw FR.

W pkt 15. jako jedną z cech współczesnych konfliktów wojennych wskazano (…) *kompleksowe wykorzystanie siły militarnej, politycznych, ekonomicznych, informacyjnych i innych środków o charakterze pozamilitarnym, realizowanych przy wykorzystaniu potencjału protestacyjnego ludności oraz sił prowadzących operacje specjalne*[23]. Nie ulega zatem wątpliwości, że poglądy Gierasimowa i zapisy oficjalnego dokumentu strategicznego są zbieżne, jeśli chodzi o używanie środków charakterystycznych dla konfliktów nazywanych obecnie hybrydowymi. W obu wymienionych przypadkach następuje stosowanie kombinacji elementów militarnych i pozamilitarnych, używanie nowoczesnych technologii, uwzględnianie nastawienia miejscowej ludności oraz prowadzenie operacji specjalnych. Nie można się temu dziwić, gdyż jest to naturalne, że najwyższy rangą wojskowy w swoich wystąpieniach i publikacjach reprezentuje i legitymizuje strategiczne myślenie władz politycznych, a oficjalna doktryna wojenna jest jego egzemplifikacją.

Jak już wcześniej wspomniano, działania informacyjne, psychologiczne i cybernetyczne są jednym z najważniejszych elementów wojen w ogóle, a nowoczesne wojny hybrydowe jeszcze bardziej to unaoczniają. Wpływanie na percepcję zdarzeń przez obserwatorów i uczestników konfliktu, dezinformowanie, wywoływanie masowego

[21] Zob. Ł. Skoneczny, *Wojna hybrydowa*…, s. 43–44.
[22] *Doktryna wojenna Federacji Rosyjskiej*, „Bezpieczeństwo Narodowe" 2015, nr 2.
[23] Zob. tamże, s. 177–206, tłumaczenie robocze BBN.

strachu lub wręcz przeciwnie – zapewnianie o braku zagrożenia, funkcjonują w praktyce prowadzenia wojen od zarania dziejów. Słynny strateg chiński Sun Tzu już w VI wieku p.n.e. pisał: *Strategia wojny polega na przebiegłości i stwarzaniu złudzeń* (…) *Staraj się wprowadzić wroga w błąd, stwórz dezorganizację w jego armii i dopiero wtedy uderzaj*. I dalej: *Kiedy wróg jest zjednoczony, spróbuj go rozdzielić*[24]. Dodając do tego nowoczesne technologie informacyjne, łączące cały świat i mogące być narzędziem wykorzystywanym do przesyłania wytworzonych komunikatów, oraz systemy teleinformatyczne, stanowiące często infrastrukturę krytyczną państw, stwarza się wiele możliwości wykorzystania własnych zasobów i umiejętności w walce, w której fizycznie nie ucierpi żaden człowiek. Ale w wyniku tej walki mogą zostać zdestabilizowane obszary, społeczności lub też całe narody i państwa.

Powyższe działania można zbiorczo ująć w koncepcję w a l k i i n f o r m a c y j n e j. Jest to szerokie pojęcie, które zawiera w sobie różne elementy związane z ogromnym znaczeniem informacji we współczesnym świecie i możliwym jej wykorzystaniem w stosunkach międzynarodowych oraz konfliktach zbrojnych. Zastosowanie informacji jest ściśle powiązane z powstaniem i rozwojem społeczeństwa informacyjnego, w którym zasoby informacyjne stały się jednym z najistotniejszych czynników potencjału cywilizacyjnego, a bez właściwie ukształtowanej sfery informacyjnej nie mogą sprawnie funkcjonować państwa i społeczeństwa[25]. Niezbędnym warunkiem funkcjonowania społeczeństwa informacyjnego jest produkcja, gromadzenie i obieg informacji[26].

Według Davida Stupplesa częściami składowymi walki informacyjnej są: walka elektroniczna, walka cybernetyczna oraz operacje psychologiczne. Celem walki elektronicznej jest zakłócenie lub zneutralizowanie fal elektromagnetycznych, co może spowodować paraliż wojskowych systemów komunikacji czy naprowadzania broni. Walka cybernetyczna to cyberataki przeprowadzane przez Internet przeciwko sieciom cyfrowym, które powodują niemożność ich używania przez właścicieli, oraz przeciw przemysłowym systemom sterowania w zakładach produkcyjnych lub elektrowniach. Z kolei operacje psychologiczne mają obniżać morale i dobre samopoczucie danego narodu, mogą także być wykorzystane do rozpowszechniania przez serwisy społecznościowe fałszywych informacji, plotek lub wywołania strachu[27].

Pierwsze dwa elementy wiążą się z technologicznym aspektem funkcjonowania podmiotu zaatakowanego. Zakłócenie, wyłączenie (czasowe lub stałe), zniekształcenie, zniszczenie lub wykorzystanie infrastrukturalnych części systemów teleinformatycznych niezgodnie z ich przeznaczeniem może spowodować, że dany podmiot nie będzie miał dostępu do własnych zasobów krytycznych. Brak tego dostępu może z kolei

[24] Sun Tzu, *Sztuka wojny*, http://www.lazarski.pl/fileadmin/user_upload/dokumenty/student/Sun_Tzu_sztuka_wojny.pdf [dostęp: 9 I 2017].
[25] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 42.
[26] M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa 2008, s. 80.
[27] Zob. D. Stupples, *The next war will be an information war, and we're not ready for it*, https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218 [dostęp: 11 I 2017].

doprowadzić do podjęcia niewłaściwej decyzji ze względu na brak rzetelnych informacji, niemożliwości efektywnego komunikowania się (np. wewnątrz jednostek sił zbrojnych lub dowódców wojskowych z ich cywilnymi zwierzchnikami), wycieku informacji tajnych bądź też do wywołania ogólnego chaosu w społeczeństwie spowodowane np. awarią systemów wodociągowych, ciepłowniczych lub telekomunikacyjnych. Natomiast operacje psychologiczne są osadzone bardziej w kontekście społeczno-polityczno-kulturowym i wiążą się z takimi zagadnieniami, jak propaganda, dezinformacja, wspieranie zaprzyjaźnionych ruchów politycznych, dyplomacja oraz manipulacja.

Realizację tych często podstępnych działań państwo powierza swoim służbom wywiadowczym (cywilnym i wojskowym)[28]. Mogą one, wykorzystując sieć agenturalną, którą tworzą opiniotwórczy dziennikarze, publicyści, eksperci czy politycy różnego szczebla, dyskretnie rozpowszechniać poglądy i informacje zgodnie z narracją narzuconą przez władze państwowe. Takie działania mogą być skuteczne zwłaszcza w sytuacji, gdy dany agent wpływu jest szanowaną osobistością, a jego zdanie jest często przytaczane w środkach masowego przekazu jako wypowiedź „niezależnego eksperta" lub „męża stanu". Na arenie międzynarodowej ważną rolę do odegrania w zakresie walki informacyjnej mają dyplomaci (w przypadku podmiotów państwowych). Będą oni kłamać na temat konkretnych wydarzeń lub osób, jeśli dostaną takie polecenie od władz centralnych i jeżeli służy to narodowemu interesowi, a zwłaszcza gdy dotyczy bezpieczeństwa narodowego[29].

Innym bardzo popularnym sposobem na ukrycie prawdy jest stosowanie tzw. szumu informacyjnego. Jest to umyślne wprowadzenie do mediów, a przez nie – do świadomości masowej publiczności, ogromnej liczby informacji na temat, który aktualnie jest rozpatrywany. Rozpowszechnianie różnych wersji tego samego zdarzenia, podawanie wielu nazwisk, możliwych przyczyn, skutków, sprawców oraz liczby ewentualnych ofiar powoduje zamęt w umysłach ludzkich i niemożność dotarcia do potrzebnej i rzetelnej informacji[30]. Tego typu działania dają lepsze rezultaty, jeśli są prowadzone przeciw społeczeństwom państw demokratycznych aniżeli społeczeństwom państw autorytarnych czy totalitarnych[31]. Demokracja charakteryzuje się swobodą wymieniania poglądów, na którą władze nie mają wpływu, co sprzyja rozpowszechnianiu informacji zniekształconych, tendencyjnych lub nieprawdziwych. W społeczeństwach zamkniętych i kontrolowanych przez służby państwowe trudniej o funkcjonowanie „nieprawomyślnych" osób czy organizacji, gdyż są one skrupulatnie monitorowane, ograniczane jest ich działanie lub takie osoby są wręcz eliminowane z życia publicznego. Można zatem przyjąć za Gabrielem Nowackim, że działania psychologiczne polegają na (…) *skoncentrowanym oddziaływaniu na sferę uczuciową człowieka, grupy społecznej poprzez przekonywanie i przekazywanie pewnych idei, poglądów, norm, czy też wzorców zachowań*

[28] M. Minkina, B. Gałek, *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015, s. 64.
[29] Zob. tamże, s. 18–19.
[30] M. Golka, *Bariery w komunikowaniu*…, s. 155.
[31] M. Minkina, B. Gałek, *Kłamstwo i podstęp*…, s. 54.

*oraz wykorzystaniu wszelkich możliwości perswazji, sugestii i argumentowania oraz manipulacji do wywoływania zmian w postawach i zachowaniu podmiotu oddziaływań w skomplikowanym otoczeniu społecznym, złożonej sytuacji polityczno-militarnej*[32].

Podsumowanie dotychczasowych rozważań na temat pojęcia wojna hybrydowa i jego zakresu pozwala na stwierdzenie, że prowadzenie wojny hybrydowej, a co za tym idzie również obrona przed nią, wymaga holistycznego podejścia do wojny i bezpieczeństwa. W ramach tej koncepcji mamy do czynienia z bardzo dynamicznym i intensywnym łączeniem środków prowadzenia wojny konwencjonalnej z użyciem ciężkiej artylerii, pojazdów, wojsk powietrznodesantowych, piechoty, okrętów wojennych itp. ze środkami niekonwencjonalnymi, takimi jak: działania dywersyjne na terenie wroga, partyzantka miejska, tajne operacje wywiadowcze i paramilitarne, często prowadzone przez lokalne ochotnicze jednostki powstańcze czy milicyjne (nierzadko wyszkolone przez wojska specjalne jednego z uczestników konfliktu), zamachy terrorystyczne czy działania stricte kryminalne. Te i inne metody siłowe są obudowane szeroką gamą działań cybernetycznych i psychologicznych, z wszechstronnym wykorzystaniem nowoczesnych technologii. Wymienione działania są elementem wspierającym agresję fizyczną z jednej strony, z drugiej zaś mogą w sprzyjających warunkach być czynnikiem, który pozwoli na osiągnięcie celów politycznych bez spowodowania śmierci chociażby jednego żołnierza lub obywatela.

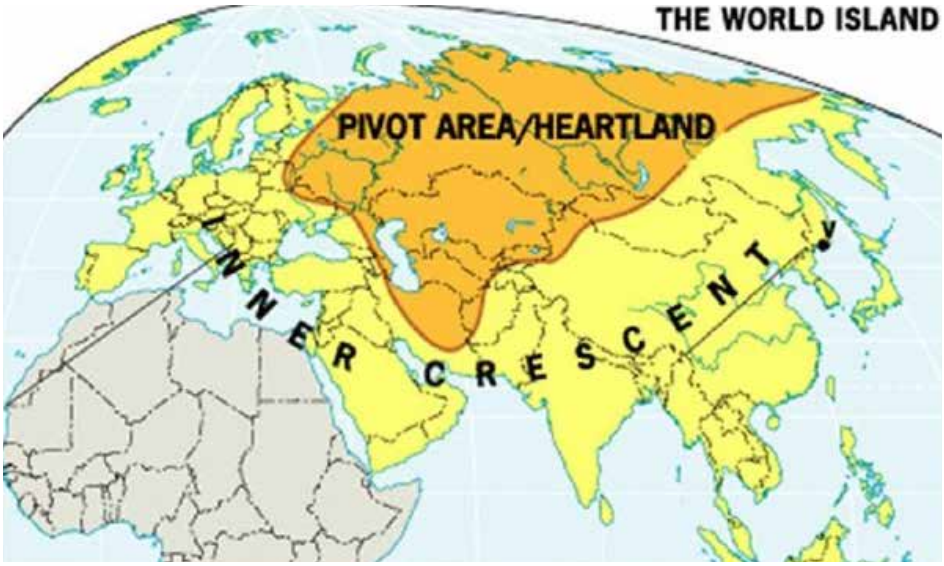
Jednak samo sprzężenie tych cech nie czyni współczesnej wojny tak wyjątkową. Wydaje się, że kluczem do hybrydowości jest współistnienie czasoprzestrzenne różnych generacji wojen, które przenikają się i konfrontują na polu walki lub w operacjach innych niż wojna[33]. Ponadto role przypisywane zwyczajowo uczestnikom konfliktu zbrojnego nie są stałe, dynamicznie się zmieniają, co powoduje trudności w opanowaniu rozproszonej przestrzeni walki, która wyszła ze schematu terytorialności w klasycznym rozumieniu[34]. Sytuację dodatkowo komplikuje możliwość uczestniczenia w konflikcie aktorów niepaństwowych oraz to, że wojna hybrydowa może przybrać formę nieregularnej agresji poniżej progu otwartej wojny, co ma swoje konsekwencje dla stosowania bądź niestosowania prawa międzynarodowego i zachowań jego podmiotów. Zrozumienia pojęcia hybrydowości wojny nie ułatwia też to, że brakuje jednej obowiązującej definicji owego zjawiska, co również staje się przedmiotem przerzucania się tezami propagandowymi. (…)

## 2. Geopolityczno-historyczne uwarunkowania rosyjskiej koncepcji wojny hybrydowej

Obecna aktywność Rosji na arenie międzynarodowej oraz jej ideologiczne uzasadnienie to w dużej mierze oparcie się na klasycznej geopolitycznej idei z początku XX wieku. Wtedy to brytyjski geograf Halford Mackinder upowszechnił koncepcję „Heartlandu",

[32] G. Nowacki, *Działania psychologiczne w działaniach sojuszniczych*, Warszawa 2003, s. 55.
[33] A. Gruszczak, *Hybrydowość współczesnych wojen*…, s. 11.
[34] M. Banasik, R. Parafianowicz, *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe AON" 2015, nr 2, s. 5.

czyli „serca kontynentu". Wyłożył w niej, że panowanie nad wschodnią, północną i zachodnią częścią kontynentu euroazjatyckiego jest podstawowym warunkiem światowej politycznej dominacji[35]. Zarówno dawniej, jak i współcześnie większość tego obszaru zajmuje Rosja. Według Mackindera „Heartland" jest najważniejszą częścią „Światowej Wyspy", która obejmuje Europę, Azję i Afrykę. Jego słynne uniwersalne prawo geopolityczne brzmi: *Kto panuje nad wschodnią Europą, ten włada 'Heartlandem', kto panuje nad 'Heartlandem', ten włada 'Światową Wyspą', kto panuje nad 'Światową Wyspą', ten włada światem*[36].




**Mapa.** Koncepcja „Heartlandu" H.J. Mackindera.
Źródło: http://www.strategic-culture.org/news/2016/12/19/geopolitics-globalization-and-world-order.html [dostęp: 13 I 2017].

Powyższa teoria ma wielu zwolenników w Rosji, co nie może dziwić, gdyż niejako z urzędu uznaje się ją za najważniejszą w kształtowaniu porządku w Eurazji, a co za tym idzie i na świecie. Chęć opanowania i podporządkowania sobie tego terenu była podstawą strategicznego myślenia w państwie rosyjskim. Najwyraźniej imperializm rosyjski objawiał się w poglądach myślicieli należących do nurtu słowianofilskiego i panslawistycznego. Ci pierwsi krytycznie oceniali zarówno kulturę zachodnioeuropejską, jak i państwowość rosyjską i postulowali stworzenie własnej cywilizacji duchowej na podstawie szerokiego oddziaływania kultury prawosławnej. Panslawiści z kolei wprost mówili o konieczności zbudowania wielkiego mocarstwa łączącego wszystkich Słowian pod przewodnictwem Rosji. Celem nadrzędnym było utworzenie państwa

[35] P. Eberhardt, *Koncepcja „Heartlandu" Halforda Mackindera*, „Przegląd Geograficzny" 2011, nr 2, s. 252.
[36] Tamże, s. 257–261.

imperialnego na terenie od Pacyfiku do Morza Śródziemnego. Ów imperializm rosyjski legł u podstaw ideologii eurazjatyckiej, która powstała wśród emigracji rosyjskiej po Rewolucji Październikowej[37].

Geograficzne położenie Rosji na dwóch kontynentach wywoływało u jej obywateli poczucie swoistej odrębności wobec łacińskiej cywilizacji Zachodu i chińsko-indyjskiej cywilizacji Wschodu, przy czym eurazjaci chętniej zwracali się w kierunku wschodnim, będąc przekonanymi o byciu spadkobiercami polityki imperium mongolskiego. Było to o tyle zaskakujące, że w kulturze i mentalności rosyjskiej Azja była traktowana jako symbol brutalności i zacofania. Jednak zwrot na Wschód był spowodowany nastrojami antyzachodnimi i próbą obrony tradycyjnych wartości duchowych[38]. Niechęć wobec Zachodu miała swoje podłoże także w religii prawosławnej. Właśnie na prawosławiu chcieli budować swoje imperium eurazjaci, a sprzeciw wobec zachodniego katolicyzmu był jednym z elementów spajających ich myśl. Byli oni także przeciwni powstającym wówczas rządom bolszewików, którzy represjonowali Cerkiew. Prawosławie miało być nie tylko czynnikiem religijnym, lecz także kulturalnym, społecznym, historycznym i politycznym[39]. (…)

### 3. Przesłanki wprowadzenia stanu wojennego

Spośród trzech stanów nadzwyczajnych wymienionych w Konstytucji RP największe konsekwencje są związane z ogłoszeniem stanu wojennego[40]. Według art. 229 może on zostać wprowadzony w razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium RP lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciw agresji[41].

Pierwsza z przesłanek jest najbardziej niedookreślona. Wiąże się ona z prawidłowym wskazaniem źródła zagrożenia, które może pochodzić od jednego państwa lub grupy państw sojuszniczych[42]. Główną rolę w tym zakresie powinny odgrywać służby specjalne, które są odpowiedzialne za zapewnienie wolnego od zagrożeń istnienia państwa[43]. W kontekście przeciwdziałania zagrożeniom zewnętrznym odpowiednie zatem będą Agencja Wywiadu i Służba Wywiadu Wojskowego. Agencja Wywiadu jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego państwa i odpowiada za uzyskiwanie, analizowanie, przetwarzanie i przekazywanie stosownym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP oraz jej potencjału ekonomicznego i obronnego, a także za rozpoznawanie

[37] Tenże, *Rosyjski eurazjatyzm i jego konsekwencje geopolityczne*, „Przegląd Geograficzny" 2005, nr 2, s. 172–173.
[38] Zob. J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, s. 97–100.
[39] Tamże, s. 101–102.
[40] T. Bryk, *Przegląd regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego" 2011, nr 1, s. 226.
[41] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r*. (Dz.U. z 1997 r. nr 78 poz. 483, ze zm.).
[42] B. Opaliński, *Stan wojenny we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2011, nr 7–8, s. 68.
[43] M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, s. 33.

i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość oraz nienaruszalność terytorium RP[44]. Służba Wywiadu Wojskowego jest właściwa w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek podległych lub nadzorowanych przez ministra obrony narodowej. Do zadań SWW należy uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa potencjału obronnego RP, bezpieczeństwa i zdolności bojowej sił zbrojnych RP i warunków realizacji przez siły zbrojne RP zadań poza granicami państwa, a także rozpoznawanie i przeciwdziałanie militarnym zagrożeniom zewnętrznym godzącym w obronność RP oraz zagrożeniom międzynarodowym terroryzmem[45]. Obie służby wykonują w zakresie swoich zadań czynności operacyjno-rozpoznawcze i analityczno-informacyjne[46]. (…)

Powyższa przesłanka wprowadzenia stanu wojennego w warunkach zagrożenia hybrydowego może implikować pewne trudności ze wspomnianym już prawidłowym identyfikowaniem źródła tego zagrożenia. Podmiot atakujący może głęboko konspirować swoje działania i czynności dezinformacyjne, zarówno wobec polskich służb specjalnych, jak i innych ośrodków i jednostek analityczno-informacyjnych, ulokowanych w różnych organach państwa. Możliwe jest np. skryte wspieranie grup dywersyjnych, terrorystycznych czy legalnych organizacji, które działałyby ze szkodą dla bezpieczeństwa i obronności RP.

Zgodnie z ustawą o stanie wojennym zarówno we wniosku Rady Ministrów do Prezydenta, jak i w rozporządzeniu Prezydenta o wprowadzeniu stanu wojennego, musi zostać podana przyczyna jego wprowadzenia[47]. Oznacza to, że powyższe podmioty są zobowiązane do jasnego określenia zagrożenia zewnętrznego, któremu państwo jest zmuszone się przeciwstawić. Wskazanie państwa bądź podmiotu atakującego może się wiązać ze stanowczą reakcją dyplomatyczną, której zadaniem jest odsunięcie od tego państwa lub podmiotu oskarżeń o spowodowanie takiego zagrożenia. Komplikuje to sytuację polityczną w skali międzynarodowej, wpływając na traktowanie zaistniałego stanu przez sojuszników Polski. Jak już wspomniano, atak hybrydowy może odbyć się poniżej progu otwartej agresji zbrojnej. Taka sytuacja wymusza właściwe uzasadnienie stanu wojennego poparte solidnymi dowodami, które w razie konieczności powinny być podane do publicznej wiadomości. Ilustracją powyższych trudności może być zajęcie Półwyspu Krymskiego. Władze Federacji Rosyjskiej twierdziły wówczas, że są to działania lokalnych oddziałów samoobrony, podczas gdy w rzeczywistości były to nieoznakowane rosyjskie wojska. Według Ukraińców do 1 marca 2014 r. na Krym zostało przerzuconych z Rosji ok. 6 tys. żołnierzy, 10 śmigłowców i 30 transporterów opancerzonych, a rosyjska Flota Czarnomorska

[44] Art. 2 i art. 6 ust. 1 pkt 1 i 2 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz.U. z 2017 r. poz. 1920, ze zm.).

[45] Art. 2 i art. 6 ust. 1 pkt 1 i 2 *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: Dz.U. z 2017 r. poz. 1978, ze zm.).

[46] Odpowiednio art. 22 i art. 26 ustawy o ABW oraz AW, a także ustawy o SKW oraz SWW.

[47] Art. 2 ust. 2 i art. 3 ust. 2 *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (t.j.: Dz.U. z 2017 r. poz. 1932).

stacjonująca w Sewastopolu została postawiona w stan najwyższej gotowości bojowej[48]. Ponieważ w polskim porządku prawnym stan wojenny jest pojęciem regulującym sytuację wewnętrzną państwa, to zewnętrzne reakcje na jego wprowadzenie lub chęć wprowadzenia nie powinny mieć wpływu na decyzyjność władz RP, zwłaszcza że zagrożone może być bezpieczeństwo narodowe. Jednak warto pamiętać, że społeczność międzynarodowa może zostać poddana pewnej presji ze strony podmiotu atakującego, szczególnie jeśli jest to ważny gracz na arenie międzynarodowej, dysponujący sprawną dyplomacją i możliwościami oddziaływania informacyjnego na szeroką skalę. (…)

## 4. Przesłanki wprowadzenia stanu wyjątkowego

Drugim ze stanów nadzwyczajnych, jaki został zawarty w Konstytucji RP, jest stan wyjątkowy[49]. W myśl art. 230 ust. 1 w razie (…) *zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić, na czas oznaczony, nie dłuższy niż 90 dni, stan wyjątkowy na części albo na całym terytorium państwa*. Tak jak ustawa o staniej wojennym, tak i ustawa o stanie wyjątkowym precyzuje, że te zagrożenia mogą być spowodowanie działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni[50].

Przesłankami do wprowadzenia stanu wyjątkowego są zagrożenia: konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego. W ustawie nie zawarto wyrażenia, że są to zagrożenia wewnętrzne, jak to miało miejsce w przypadku stanu wojennego w odniesieniu do zagrożenia zewnętrznego. Jednak biorąc pod uwagę, że wymienione dobra są skierowane do wewnątrz państwa (ustrój państwa, bezpieczeństwo obywateli i porządek publiczny wewnątrz Rzeczpospolitej) oraz to, że przesłanka zewnętrznego zagrożenia została zarezerwowana dla stanu wojennego, można przyjąć, że źródła zagrożenia należy szukać w granicach państwa[51].

Przepisy, które mogą być potwierdzeniem takiego rozumowania, można znaleźć w przywoływanych już wcześniej ustawach kompetencyjnych służb specjalnych, jednak tym razem w odniesieniu do Agencji Bezpieczeństwa Wewnętrznego oraz Służby Kontrwywiadu Wojskowego. Agencja Bezpieczeństwa Wewnętrznego jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Do jej zadań należy m.in.: rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a zwłaszcza w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa, oraz uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku

[48] M. Gołda-Sobczak, *Krym jako przedmiot sporu ukraińsko-rosyjskiego*, Poznań 2016, s. 185.

[49] Przepisy regulujące stan wyjątkowy zostaną omówione w takim zakresie, w jakim różnią się od regulacji stanu wojennego. W przypadku zbieżności nastąpi odesłanie do stosownych przepisów prawa lub fragmentu pracy.

[50] Art. 2 ust. 1 *Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (t.j.: Dz.U. z 2017 r. poz. 1928).

[51] K. Prokop, *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej*, Białystok 2005, s. 74.

konstytucyjnego[52]. Służba Kontrwywiadu Wojskowego jest właściwa w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej sił zbrojnych RP oraz innych jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych. Do zadań SKW należy m.in. rozpoznawanie, zapobieganie oraz wykrywanie, przestępstw przeciwko Rzeczpospolitej Polskiej określonych w rozdziale XVII *Kodeksu karnego* dokonywanych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych RP i innych jednostek organizacyjnych MON[53]. (…) Żadna inna formacja nie ma takich kompetencji. Ponadto obie służby są właściwe w sprawach ochrony bezpieczeństwa wewnętrznego lub ochrony przed zagrożeniami wewnętrznymi.

Podobnie jak w przypadku określenia zewnętrznego źródła zagrożenia hybrydowego i wprowadzania stanu wojennego, tak i w stanie wyjątkowym przesłanką będzie zagrożenie wewnętrzne. Zaistnienie ataku hybrydowego, którego źródłem będzie w całości podmiot mający siedzibę w Polsce oraz w żaden sposób niepowiązany organizacyjnie, finansowo, osobowo lub ideowo z podmiotem zagranicznym, jest mało prawdopodobne. Przeprowadzenie operacji hybrydowej o istotnych skutkach politycznych, terytorialnych czy finansowych, której przygotowanie w całości odbywałoby się na terytorium Rzeczpospolitej i bez jakiejkolwiek zewnętrznej ingerencji państwowej lub pozapaństwowej, byłoby bardzo trudne do zrealizowania. Bardziej prawdopodobna jest sytuacja, w której zewnętrzne podmioty przez głęboko zakamuflowaną inspirację wywrotowych organizacji lub indoktrynację pewnej specyficznej grupy społecznej, etnicznej, religijnej lub politycznej przeprowadzają atak hybrydowy na Polskę. W przypadku inspiracji zewnętrznej wprowadzenie stanu wyjątkowego byłoby zatem skutkiem błędnej identyfikacji źródła zagrożenia, gdyż zgodnie z przywoływanymi wcześniej przepisami w razie zewnętrznego zagrożenia państwa wprowadza się stan wojenny. Inaczej sprawa wygląda w przypadku długotrwałej indoktrynacji, której dopuszczają się różnego rodzaju media. Może to spowodować przejęcie propagowanych w nich idei jako własnych i na tym gruncie mogą one być inspiracją do utworzenia organizacji zagrażającej konstytucyjnemu ustrojowi państwa. Byłoby to możliwe przy uwzględnieniu długiej perspektywy czasowej, konieczności skrytego zgromadzenia zarówno zasobów ludzkich, jak i finansowo-materialnych niezbędnych do przeprowadzenia ataku hybrydowego. (…)

## 5. Wojna hybrydowa w cyberprzestrzeni – zagrożenia dla Polski

Cyberprzestrzeń jest pełnoprawnym polem walki w koncepcji wojny hybrydowej. Otwarte użycie siły militarnej w toku jej prowadzenia w Europie zaistniało tylko na terytorium Ukrainy, co pozwoliło Rosji zdestabilizować wschodnie regiony tego kraju. Przeciwko państwom, na których terenie przeprowadzenie tego rodzaju ataku nie jest możliwe lub byłoby z różnych względów bardzo trudne, są prowadzone intensywne

[52] Art. 1 i art. 5 ust. 1 pkt 1 i 4 ustawy o ABW oraz AW.
[53] Art. 1 i art. 5 ust. 1 pkt 1 i 4 ustawy o SKW oraz SWW.

działania naruszające bezpieczeństwo w cyberprzestrzeni oraz propagandowo-informacyjne. Cyberprzestrzeń jest dla takiej aktywności szybkim kanałem rozprowadzającym. W niniejszym podrozdziale zostaną omówione wspomniane powyżej działania w kontekście polskiego bezpieczeństwa.

Kładzenie dużego nacisku na prowadzenie działań hybrydowych w cyberprzestrzeni jest spowodowane odmiennością tego rodzaju konfrontacji w porównaniu z klasycznymi wymiarami walki: lądowym, morskim, powietrznym i kosmicznym. Ta odmienność wynika z trzech czynników. Po pierwsze nieistnienie barier terytorialnych i materialnych w cyberprzestrzeni uniezależnia prowadzenie operacji od granic geograficznych. Po drugie postęp technologiczny XXI wieku pozwala na nieustanne redukowanie kosztów prowadzenia działań w cyberprzestrzeni. Po trzecie zaś podmiot prowadzący działania w tym wymiarze może łatwiej zachować anonimowość[54].

Brak bezpośrednich dowodów prowadzenia działań ofensywnych w cyberprzestrzeni przez państwo daje możliwość odsunięcia od siebie podejrzeń na arenie międzynarodowej oraz wykorzystywania wysuwanych oskarżeń do swoich celów, np. propagowania wśród własnych obywateli idei „oblężonej twierdzy", co konsekwentnie czyni Rosja. Pisze o tym w swojej publikacji Jolanta Darczewska, która przytacza aktywność rosyjskich mediów zapowiadających nową doktrynę bezpieczeństwa informacyjnego Rosji. Budują one powyższą ideę np. przez wysuwanie stwierdzeń, że jedynym sposobem zapewnienia bezpieczeństwa informacyjnego jest wspólny wysiłek wszystkich użytkowników Internetu, dziennikarzy, organów władzy, społeczeństwa obywatelskiego itp.[55]

### 5.1. Hybrydowe ataki na systemy i sieci teleinformatyczne

W zależności od przeznaczenia i konstrukcji systemu teleinformatycznego można wyróżnić jego bezpieczeństwo „na zewnątrz" i „do wewnątrz". Wymiar zewnętrzny dotyczy ochrony przed zagrożeniami zarówno środowiska, w którym pracuje dany system, jak i człowieka. Zagrożenia mogą być spowodowane nieprawidłowym działaniem samego systemu i odnoszą się głównie do tzw. przemysłowych systemów sterowania, np. monitorujących stan zdrowia pacjenta, nadzorujących ruch kolejowy czy sterujących bronią pokładową w pojazdach wojskowych. Wymiar wewnętrzny dotyczy ochrony przed zagrożeniami informacji przechowywanej, przetwarzanej i przesyłanej w sieci lub systemie teleinformatycznym, szczególnie w sieciach biurowych, bankowych czy naukowych[56].

Według K. Lidermana do podstawowych kategorii zagrożeń poprawnego funkcjonowania sieci i systemów informacyjnych (których częścią są systemy i sieci teleinformatyczne) zalicza się:

1) katastrofy naturalne,

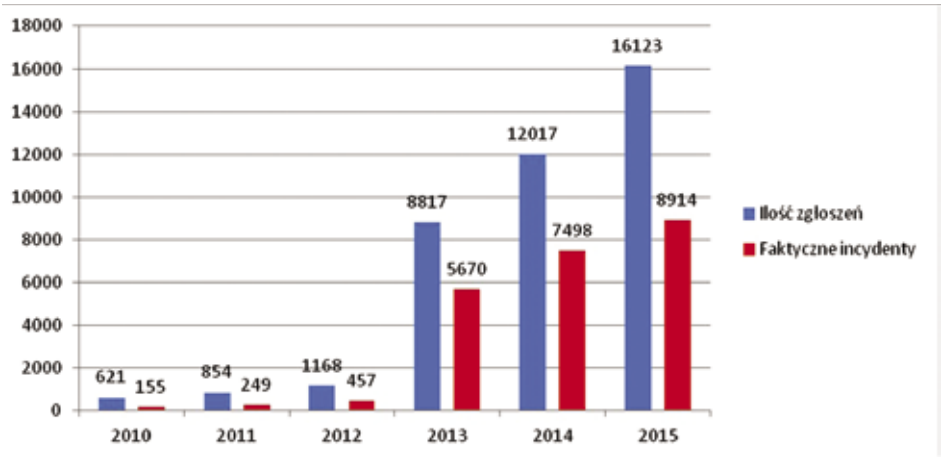
[54] F. Bryjka, *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej*, w: *Bezpieczeństwo personalne a bezpieczeństwo strukturalne*, t. 3: *Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*, T. Grabińska, Z. Kuźniar (red. nauk.), Wrocław 2015, s. 119–120.

[55] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, s. 31.

[56] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 30–31.

2) błędy spowodowane przez osoby, które wykorzystują lub obsługują systemy informacyjne,
3) błędy w organizacji pracy i procedurach,
4) celowe, szkodliwe działania ludzi skierowane na systemy informacyjne,
5) awarie sprzętu (elementów i podzespołów mechanicznych, elektronicznych, elektromechanicznych) i wady oprogramowania[57]. (…)

W 2015 r. (nie opublikowano jeszcze raportu za 2016 r.) Zespół CERT.GOV.PL[58] zanotował łącznie 16 123 zgłoszenia, z których 8914 zostało zakwalifikowanych jako faktyczne incydenty. Ta różnica jest spowodowana tym, że część zgłoszeń to tzw. *false-positives*, czyli przypadki błędnego interpretowania przez osobę zgłaszającą legalnego ruchu sieciowego, a także wielokrotnym zgłaszaniem tych samych incydentów, szczególnie przez systemy automatyczne (np. za pośrednictwem platformy N6)[59]. W porównaniu z 2014 r. nastąpił wzrost liczby zgłoszeń, których zarejestrowano wówczas 12 017, z czego 7498 uznano za incydenty[60]. Tendencja wzrostowa w liczbie zgłoszeń i incydentów istnieje od samego początku publikowania raportów o stanie bezpieczeństwa cyberprzestrzeni RP, mamy więc do czynienia zarówno ze wzrostem inicjatyw mających na celu ochronę cyberprzestrzeni, jak i ze wzrostem liczby zidentyfikowanych zagrożeń.




**Wykres.** Liczba zgłoszeń i faktycznych incydentów odnotowanych przez Zespół CERT.GOV.PL w latach 2010–2015.

Źródło: Opracowanie własne na podstawie raportów o stanie bezpieczeństwa cyberprzestrzeni RP z lat 2010–2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 3 VI 2017].

[57] Tamże, s. 33.

[58] W dniu 28 VIII 2018 r. CERT.GOV.PL przekształcił się w CSIIRT.GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (podstawa: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. z 2018 r. poz. 1560) – przyp. red.

[59] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [dostęp: 2 VI 2017].

[60] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [dostęp: 2 VI 2017].

Tak jak w 2014 r., również w 2015 r. największy udział w zarejestrowanych incydentach miały przypadki botnetów, choć sama ich liczba nieznacznie spadła – z 4681 w 2014 r. do 4284 w 2015 r. Botnet to zazwyczaj duża sieć komputerów, które zostały przejęte przez przestępców za pomocą złośliwego oprogramowania. Przestępcy zmieniają dany komputer w bota (zombie) i mogą go kontrolować przez Internet bez wiedzy jego użytkownika. Botnety są używane np. do rozsyłania spamu, rozprzestrzeniania wirusów, atakowania serwerów i komputerów oraz popełniania innych przestępstw i oszustw. Dochodzi do sytuacji, w których przestępcy udostępniają sobie wzajemnie sieci botnet. Przykładem działania botnetu może być otrzymanie maila z linkiem reklamowym. Po kliknięciu linka następuje pobranie programu do kradzieży danych lub programu szpiegującego, a także do powiększania liczby komputerów zainfekowanych[61].

Jak duże zagrożenie stanowi umiejętnie użyta sieć botnet pokazuje przypadek jej wykorzystania przez rosyjskiego hakera Jewgienija Bogaczewa. Stworzył on botnet o nazwie Gameover ZeuS, dzięki któremu ukradł ponad 100 mln dolarów z amerykańskich kont bankowych. Zainfekowaniu uległy także komputery na terenie Wielkiej Brytanii. Pomimo zidentyfikowania sprawcy przez organy ścigania, żyje on na wolności i mieszka w Rosji[62]. Amerykańscy dziennikarze uważają, że botnet wynaleziony przez Bogaczewa został użyty w latach 2011–2014 przez rosyjskie służby wywiadowcze do szpiegowania komputerów amerykańskiej administracji, m.in. do poszukiwania dokumentów zawierających stanowisko rządu USA wobec Rosji oraz niejawnych dokumentów Departamentu Obrony. Twierdzą oni także, że Bogaczew pracuje dla jednej z jednostek specjalnych nadzorowanych przez FSB[63]. FBI wyznaczyło nagrodę w wysokości 3 mln dolarów za pomoc w schwytaniu Bogaczewa[64].

Uderzenie hakerów w system bankowy nie ominęło Polski. W lutym 2017 r. wyszło na jaw, że od października 2016 r. prowadzono przemyślany i zaawansowany atak na systemy teleinformatyczne banków przy użyciu zainfekowanej strony internetowej Komisji Nadzoru Finansowego. Hakerzy wykorzystali zaufanie pracowników banków do urzędowej strony organu nadzorczego, jakim jest Komisja Nadzoru Finansowego. Na stronie KNF wyświetlała się jej standardowa zawartość, a jednocześnie na każdy komputer łączący się z tą stroną przenosił się dodatkowy kod, który był tam umieszczony. Posłużono się przy tym niezaktualizowaną aplikację strony. W systemie informacyjnym KNF zmodyfikowano kod JavaScript, który w rezultacie nakłaniał komputery do pobrania i uruchomienia skryptu ze złośliwego serwera. Następnie ten skrypt badał, czy dany komputer należy do systemu obranego za cel ataku. Zainfekowany pierwotnie komputer został użyty do zarażania następnych, a te, podłączone do Internetu, były używane

[61] https://www.cybsecurity.org/pl/co-to-jest-botnet-i-dlaczego-nalezy-zachowac-ostroznosc/ [dostęp: 3 VI 2017].
[62] http://technowinki.onet.pl/biznes-i-finanse/nowy-bohater-rosji-haker-ktory-okradl-usa-bez-wstawania-z-kanapy/zhmdr [dostęp: 3 VI 2017].
[63] http://technowinki.onet.pl/oprogramowanie/rosyjskie-sluzby-wykorzystaly-botnet-do-szpiegowania-amerykanskiej-administracji/qg4cqk [dostęp: 3 VI 2017].
[64] http://www.tvn24.pl/wiadomosci-ze-swiata,2/dla-fbi-jewgienij-bogaczew-wart-jest-trzy-miliony-dolarow,723039.html [dostęp: 3 VI 2017].

do sterowania powstałą w ten sposób siecią – botnetem. W wyniku ataku nie zostały skradzione żadne pieniądze, więc pojawiły się podejrzenia, że celem była kradzież danych osobowych klientów banków i ich historia finansowa. Rozpatrywano także wersję, że był to jeden z etapów ataku, następnym zaś będzie kradzież zasobów finansowych. Nie jest też jasne, jaki podmiot przeprowadził powyższy atak. Dziennikarze gazety „New York Times" sugerowali, że odpowiedzialnością należy obarczyć służby specjalne Korei Północnej, które miały zaatakować również amerykańskie banki. Podnoszono także, że w podobny sposób działała grupa hakerska Lazarus, która jest łączona z atakiem na Sony Pictures z 2014 r. oraz kradzieżą 81 mln dolarów z centralnego banku Bangladeszu w 2016 r. Do tej pory nie można jednoznacznie określić, kto stał za atakiem na polskie banki i KNF. Możliwe, że w ogóle nie uda się tego ustalić[65]. Biorąc jednak pod uwagę to, że z Rosji następuje największa liczba ataków na polskie komputery[66], można uznać, że może to być element prowadzenia wojny hybrydowej.

W 2015 r. na drugim miejscu pod względem liczby stwierdzonych incydentów uplasowały się błędne konfiguracje (podatność) serwerów lub usług funkcjonujących w instytucjach administracji państwowej i u operatorów infrastruktury krytycznej. Odnotowano 3921 takich incydentów, co stanowi wzrost o 11 proc. w stosunku do 2014 r. Jako przyczynę wskazano zidentyfikowanie nowych źródeł podatności[67]. Zespół CERT.GOV.PL zaklasyfikował te zagrożenia jako niecelowe działanie ludzkie (…). Wskazano, że do skuteczności ataków w dużej mierze przyczyniają się takie czynniki, jak: nieodpowiednie podejście do problemu bezpieczeństwa systemów, nieodpowiednie procedury w instytucjach, brak dedykowanych zespołów i pracowników odpowiedzialnych za reagowanie na incydenty oraz zauważalna tendencja do ograniczania nakładów finansowych na bezpieczeństwo teleinformatyczne. Konieczne jest też organizowanie szkoleń dla przyjmowanych pracowników oraz – cyklicznie – dla całej kadry pracowniczej, a także systematyczne przeprowadzanie testów bezpieczeństwa. Mimo działań CERT.GOV.PL, inicjatywa dotycząca ochrony systemów leży po stronie podmiotów zainteresowanych, które często nie wcielają w życie rekomendacji i ostrzeżeń do nich wysyłanych[68].

Według CERT.GOV.PL trzecim rodzajem incydentów występujących najczęściej w 2015 r. był tzw. phishing, który jest zaliczany do incydentów typu „inżynieria społeczna". Phishing to metoda bazująca na podstępie wobec nieświadomego użytkownika Internetu, który otrzymuje wiadomość pocztą elektroniczną lub odwiedza stronę łudząco przypominającą taką, której używa i której ufa. Zostaje on poproszony np. o aktualizację, zatwierdzenie jakiejś informacji czy odwiedzenie określonej strony w związku

[65] Por. http://rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 3 VI 2017]; https://www.cashless.pl/temat-dnia/2433-new-york-times-to-koreanczycy-stali-za-atakiem-na-knf-i-polski-sektor-bankowy, [dostęp: 3 VI 2017]; https://niebezpiecznik.pl/post/jak-przeprowadzono-atak-na-knf-i-polskie-banki-oraz-kto-jeszcze-byl-na-celowniku-przestepcow/ [dostęp: 3 VI 2017].

[66] Dane firmy F-Secure opracowane na podstawie badań przeprowadzonych od października 2016 r. do marca 2017 r., http://www.rp.pl/Telekomunikacja-i-IT/304289934-Rosyjscy-hakerzy-masowo-atakuja-polskie-komputery.html#ap-1 [dostęp: 3 VI 2017].

[67] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*…, s. 7.

[68] Tamże, s. 8.

z problemem, który rzekomo się pojawił. Wtedy następuje przekierowanie na podstawioną przez hakerów stronę, która jest wykorzystywana do wyłudzania danych potrzebnych np. do logowania na konto bankowe lub inny serwis[69]. W 2015 r. ogólna liczba incydentów z zakresu inżynierii społecznej wyniosła 257, co jest równoznaczne ze wzrostem o 116 proc. w stosunku do 2014 r. Administracja państwowa zgłosiła do CERT.GOV.PL 71 proc. ogółu wiadomości typu phishing, a przedsiębiorstwa najważniejsze dla bezpieczeństwa narodowego zgłosiły 21 proc. takich incydentów[70].

Ataki typu phishing stają się coraz bardziej popularne wśród cyberprzestępców. Według raportu firmy PhishMe, która zajmuje się neutralizowaniem takich zagrożeń, w pierwszym kwartale 2016 r. nastąpił wzrost liczby tego typu ataków o prawie 800 proc. w stosunku do analogicznego okresu 2015 r. Niepokoić może to, że wiadomości phishingowe zawierają nie tylko linki do stron ze złośliwym oprogramowaniem czy zachętę do podawania wrażliwych danych, lecz także coraz częściej wirusy typu ransomware[71]. Atak złośliwego oprogramowana zawierającego tego wirusa polega na zaszyfrowaniu plików na danym komputerze i żądaniu okupu od użytkownika za ich odszyfrowanie. W maju 2017 r. świat obiegła informacja o globalnym wirusie ransomware znanym pod nazwą WannaCry. Po zablokowaniu dostępu do posiadanych przez użytkownika danych żądał on od niego zapłaty w wysokości 300 dolarów przeliczonych na bitcoiny (wirtualną walutę). WannaCry odczuły takie firmy, jak FedEx, Renault, Nissan, koleje w Niemczech i Rosji oraz banki, firmy telekomunikacyjne i ministerstwa[72]. W Polsce zebrał on stosunkowo niewielkie żniwo, gdyż infekcje na terytorium RP stanowiły tylko 0,65 proc. światowych dobowych infekcji, ponadto nie dotknęły żadnego organu administracji publicznej[73].

Phishing był najczęściej obsługiwanym rodzajem incydentu teleinformatycznego przez CERT Polska również w 2016 r. i stanowił ponad połowę wszystkich przypadków[74]. CERT Polska otrzymał w 2016 r. łącznie 722 584 zgłoszenia tego rodzaju incydentów w polskich sieciach[75]. Ataki dotknęły klientów polskich banków. Klienci ING Banku Śląskiego, mBanku, BZ WBK, Banku Millennium i PKO BP otrzymywali fałszywe maile z prośbą o wpisanie swoich danych logowania w celu rzekomego odblokowania dostępu do konta[76]. Użytkownicy bankowości elektronicznej powinni pamiętać, że banki nigdy nie proszą swoich klientów o wpisywanie pełnych haseł

[69] https://www.avast.com/pl-pl/c-phishing [dostęp: 4 VI 2017].
[70] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*…, s. 41–42.
[71] http://www.cyberdefence24.pl/382418,kampanie-phishingowe-rosna-w-tempie-800-procent-rocznie [dostęp: 4 VI 2017].
[72] Zob. https://zaufanatrzeciastrona.pl/post/jak-najprawdopodobniej-doszlo-do-globalnej-infekcji-ransomare-wannacry/ [dostęp: 4 VI 2017].
[73] http://wyborcza.pl/7,156282,21815396,ransomware-wannacry-w-polsce-zainfekowanych-ponad-1-tys-urzadzen.html [dostęp: 4 VI 2017].
[74] *Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalności CERT Polska*, https://www.cert.pl/PDF/Raport_CP_2016.pdf s. 7 [dostęp: 4 VI 2017].
[75] Tamże, s. 68.
[76] Zob. https://www.cashless.pl/wiadomosci/bezpieczenstwo/item/199-atak-phishingowy-na-klientow-ing-banku-slaskiego [dostęp: 4 VI 2017], http://www.bankier.pl/wiadomosc/Atak-phishingowy-na-klientow-PKO-Banku-Polskiego-7358309.html [dostęp: 4 VI 2017].

oraz nie przesyłają odnośników służących zalogowaniu, logować należy się bezpośrednio ze strony banków.

Odmiana phishingu, jakim jest spearphishing, została zidentyfikowana jako narzędzie przeprowadzenia ataku, który miał na celu zakłócenie procesu wyborczego w USA w 2016 r.[77] Polegał on na wysyłaniu wiadomości phishingowych do ściśle określonych osób, co jest poprzedzone dokładnym wywiadem środowiskowym, w celu uzyskania danych, do których te osoby mają dostęp[78]. Skutkiem ataku była kradzież danych z systemów Partii Demokratycznej oraz ujawnienie korespondencji jej polityków. Spekulowano, że celem była nie tylko kompromitacja amerykańskiego systemu wyborczego, lecz także spowodowanie wygranej w wyborach prezydenckich kandydata Partii Republikańskiej Donalda Trumpa[79]. Amerykańskie służby specjalne w oficjalnym komunikacie podały, że za atakiem stał wywiad rosyjski[80].

Jak duże zamieszanie może spowodować awaria systemu teleinformatycznego używanego podczas przeprowadzania wyborów, można było się przekonać także w Polsce. W 2014 r. na skutek błędów w systemie używanym przez Państwową Komisję Wyborczą w czasie wyborów samorządowych doszło do problemów z obliczeniem głosów, podawano nieprawdziwe wyniki głosowań, trzeba było również prostować podany wcześniej podział mandatów. W przestrzeni medialnej mówiono o fałszerstwie wyborczym i konieczności ich powtórzenia. Zostało zachwiane zaufanie do organów państwa. Odbywały się demonstracje, ludzie wtargnęli do siedziby Państwowej Komisji Wyborczej, która zawiesiła swoją pracę[81]. Z raportu CERT.GOV.PL wynikało, że urzędnicy PKW zlekceważyli wcześniejsze sygnały o zainfekowaniu stron internetowych oraz przypadek upublicznienia serwera testowego ich systemu. Ponadto w pierwszym momencie odrzucono pomoc CERT.GOV.PL, ale poproszono o nią w późniejszym czasie[82].

### 5.2. Dezinformacja i propaganda w Internecie

Oprócz ataków i zagrożeń ukierunkowanych stricte na systemy i sieci teleinformatyczne ważne z punktu widzenia bezpieczeństwa Rzeczpospolitej odnotowuje się także przedmiotowe użycie Internetu w celu prowadzenia propagandy i dezinformacji, które jest narzędziem wsparcia działań militarnych i wywiadowczych. Wykorzystywane w tych celach osoby zostały przyporządkowane do dwóch kategorii:

1) działające na zlecenie i otrzymujące wynagrodzenie za zamieszczanie tendencyjnych komentarzy i wpisów na stronach internetowych i portalach społecznościowych,

[77] *Krajobraz bezpieczeństwa*…, s. 35.
[78] http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2013/33/spear-phishing-czyli-ataki-spersonalizowane.aspx [dostęp: 5 VI 2017].
[79] http://www.newsweek.pl/swiat/rosyjscy-hakerzy-ingerowali-w-wybory-w-usa-co-na-to-donald-trump-artykuly,402729,1.html [dostęp: 5 VI 2017].
[80] http://www.polskatimes.pl/fakty/swiat/a/usa-donald-trump-uznal-fakt-ze-rosja-stoi-za-cyberatakami-na-serwery-partii-demokratycznej,11667906/ [dostęp: 5 VI 2017].
[81] https://pl.wikipedia.org/wiki/Wybory_samorz%C4%85dowe_w_Polsce_w_2014_roku#cite_note-8 [dostęp: 5 VI 2017].
[82] http://www.rp.pl/artykul/1163284-PKW-ignorowala-ostrzezenia.html#ap-1 [dostęp: 5 VI 2017].

2) tzw. *useful idiots*, czyli nieświadomie przyczyniające się do szerzenia dezinformacji, które mogą być w tym celu inspirowane[83].

Do pierwszej kategorii można zaliczyć osoby, które są tzw. trollami. Publikują one wiadomości, teksty i tworzą komentarze mające przekłamywać rzeczywistość na korzyść określonego podmiotu. Podstawą przekłamania jest taki opis zdarzeń, aby jego wydźwięk był zgodny z założoną wcześniej ideą. Potwierdzeniem tego jest relacja byłego pracownika jednej z „agencji medialnych", która w istocie była prorosyjską i antyukraińską „fabryką" trolli. Osoby tam zatrudniane podzielono na kilka kategorii:

1) content managerzy: przepisują na nowo prawdziwe newsy w taki sposób, aby popierały rosyjski punkt widzenia, a szkalowały Ukraińców. Tak przerobione informacje są publikowane w portalach kontrolowanych przez „agencję",
2) blogerzy: publikują wpisy w portalach społecznościowych i na blogach,
3) ilustratorzy: wymyślają tematyczne obrazki, w tym tzw. memy internetowe[84],
4) specjaliści SEO: spamują linkami do treści umieszczonych na innych stronach.

Celem wspomnianej „agencji" było zwiększenie codziennie liczby czytelników zarządzanych przez nią serwisów o 3 tys. osób, a motywacją do pracy były dość atrakcyjne zarobki[85]. O znaczeniu tego typu działań w sieci, z dala od fizycznego pola walki, może świadczyć oficjalna informacja Brytyjskich Sił Zbrojnych ze stycznia 2015 r., że w kwietniu powstanie specjalna jednostka zajmująca się wykorzystaniem operacji psychologicznych i mediów społecznościowych, której zadaniem będzie wsparcie walk w epoce informacji[86]. Działania propagandowe w Internecie prowadzi także Państwo Islamskie, a zwalczanie tej organizacji – również w sieci – zapowiedzieli członkowie grupy hakerskiej Anonymous. Namierzają oni dane osobowe członków lub sympatyków Państwa Islamskiego dzięki analizie metadanych publikowanych zdjęć lub dokumentów oraz wyłudzają hasła do kont użytkowników za pomocą phishingu[87].

Od momentu rozpoczęcia aneksji Krymu przez Rosję zaobserwowano w Polsce wzrost liczby komentarzy pod artykułami, które miały wyraźnie prorosyjski, antyukraiński oraz antyamerykański charakter. Na przykład dziennikarze gazety „Newsweek" ustalili, że pod artykułami opisującymi sytuację na Ukrainie znacznie wzrosła liczba komentarzy, często wulgarnych, popierających działania rosyjskie (dane z 2014 r.). Po analizie adresów IP i ich geolokalizacji doszli do wniosku, że 80 proc. wpisów pochodzi spoza Polski, m.in. z Aten, San Francisco czy Zurychu. Ekspert z zakresu cyberterroryzmu

[83] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*…, s. 48.

[84] „Mem internetowy to dowolny fragment informacji, rozpowszechniany i powielany przy użyciu aktualnie funkcjonujących technologii komunikowania w Internecie (rozumianym jako globalna przestrzeń wirtualna). Może on przyjąć formę linku, materiału audio-wideo, obrazu/fotografii, całej strony internetowej, znacznika hash , frazy czy nawet pojedynczego słowa . Propagacja i agregacja memu odbywa się typowymi dla komunikacji sieciowej kanałami, tj. poprzez platformy mediów społecznościowych, blogi, e-maile, komunikatory, serwisy informacyjne oraz wszelkie pozostałe usługi umożliwiające kontakt między internautami", za: M. Zaremba, *Memy internetowe (2010–2011)*, „Media i Społeczeństwo" 2012, nr 2, s. 61.

[85] Zob. https://niebezpiecznik.pl/post/kulisy-pracy-rosyjskich-prorzadowych-trolli-internetowych/ [dostęp: 5 VI 2017].

[86] http://www.bbc.com/news/uk-31070114 [dostęp: 5 VI 2017].

[87] https://niebezpiecznik.pl/post/anonimowi-wypowiedzieli-wojne-isis-owi-jak-chca-z-nim-walczyc-w-sieci/ [dostęp: 5 VI 2017].

i były policjant Andrzej Mroczek stwierdził, że to standardowy wybieg hakerów w celu odsunięcia od siebie podejrzeń[88].

Dziennikarze i eksperci rozpoznali także wiele stron internetowych i organizacji, które są określane jako prorosyjskie. Są wśród nich partia „Zmiana" oraz Europejskie Centrum Analiz Geopolitycznych, które łączy osoba Mateusza Piskorskiego, aresztowanego przez ABW pod zarzutem szpiegostwa na rzecz Rosji. ABW uważa, że aktywność „Zmiany" była elementem działalności rosyjskiego wywiadu cywilnego SWR, a Piskorski brał w tym świadomy udział w celu manipulowania opinią społeczną[89]. Z kolei były dyplomata pracujący na Białorusi i w Rosji Witold Jurasz stwierdził, że Europejskie Centrum Analiz Geopolitycznych (…) *to organizacja tak jawnie prorosyjska i proputinowska, że nazwanie jej ekspozyturą rosyjskich wpływów nie jest nadużyciem*[90].

Marcin Rey prowadzi na portalu Facebook stronę pod nazwą „Rosyjska V kolumna w Polsce". Śledzi na niej działalność osób o prorosyjskich poglądach, wśród których są Piskorski oraz inni działacze „Zmiany": Nabil Al Malazi, Jarosław Augustyniak czy Konrad Rękas, a także inne osoby powiązane z tym środowiskiem[91]. Rey opublikował wiele zdjęć korespondencji środowisk prorosyjskich z Białorusinem Aleksandrem Usowskim, z której wynika, że finansował on m.in. manifestacje antyukraińskie w Polsce[92].

Do stron, które propagują rosyjskie poglądy, zaliczono również www.xportal.pl i www.kresy.pl. Redaktor naczelny pierwszej z nich Bartosz Bekier uważa prorosyjskich separatystów za powstańców i popiera dostawy broni z Rosji do Donbasu[93]. Jest on też przywódcą narodowo-radykalnej Falangi, a także był jednym z głównych mówców podczas manifestacji pod ambasadą Ukrainy w Warszawie, którą zorganizowano w celu potępienia działań wojsk ukraińskich[94]. Z kolei propagandowy wydźwięk artykułów publikowanych na www.kresy.pl opisuje Krzysztof Nieczypor na prowadzonej przez siebie stronie www.eastbook.eu[95]. Wskazuje on, że pod pretekstem tematyki kresowej są tam zamieszczane wiadomości chwalące rosyjską potęgę wojskową, jej sukcesy wojenne w Syrii oraz krytyka organizacji Szczytu NATO w 2016 r. w Warszawie, co miało być tylko prowokowaniem Rosji[96]. Publikacje zamieszczane na www.kresy.pl zostały także skrytykowane przez Stowarzyszenie Dziennikarzy Polskich, które oceniło, że portal stał się (…) *narzędziem propagandy rosyjskich separatystów*[97].

[88] http://www.newsweek.pl/swiat/wynajeci-rosjanie-cyber-bombarduja-polski-internet-newsweek-cyberatak,artykuly,281538,1.html [dostęp: 5 VI 2017].
[89] http://wyborcza.pl/1,75398,20132090,abw-partie-zmiana-zalozyli-rosjanie.html [dostęp: 5 VI 2017].
[90] http://wiadomosci.onet.pl/tylko-w-onecie/ecag-rozszerza-wplywy-w-polsce-jest-jawnie-prorosyjskie-i-proputinowskie/25h7l9 [dostęp: 5 VI 2017].
[91] Zob. https://www.facebook.com/RosyjskaVKolumnawPolsce/?fref=ts [dostęp: 5 VI 2017].
[92] http://wiadomosci.onet.pl/kraj/gw-kreml-potajemnie-finansowal-w-polsce-ruchy-antyukrainskie/byvkxhh [dostęp: 5 VI 2017].
[93] http://xportal.pl/?p=15402 [dostęp: 5 VI 2017].
[94] http://niezalezna.pl/58668-sympatycy-putina-w-warszawie-prorosyjska-manifestacja-pod-ambasada-ukrainy [dostęp: 5 VI 2017].
[95] http://www.eastbook.eu/2016/09/19/na-kolanach-przed-rosyjska-potega-o-dzialalnosci-portalu-kresy-pl/ [dostęp: 5 VI 2017].
[96] Zob. http://kresy.pl/publicystyka/nato-czyli-jak-prowokowac-rosje-nie-broniac-polski/ [dostęp: 5 VI 2017].
[97] http://www.sdpwarszawa.pl/aktualnosci-254,Zarzad_OW_SDP_zaniepokojony_postawa_kresy.pl.html [dostęp: 5 VI 2017].

Innym portalem uważanym za propagandowe narzędzie Rosji jest Sputnik News, który jest częścią rosyjskiej agencji informacyjnej Sputnik działającej w skali międzynarodowej[98]. Na jego łamach są publikowane m.in. teksty i wywiady z Rękasem, który stwierdza że brak próby rozwiązania konfliktu w Donbasie wynika tylko ze złej woli władz ukraińskich. Ukraina jest państwem upadłym, a NATO tylko ściąga na Polskę niebezpieczeństwo wojny, natomiast niebezpieczeństwo ze strony Rosji jest urojone[99]. Te rozmowy przeprowadza zawsze redaktor Sputnika Leonid Sigan, zajmujący się sprawami polskimi. Na froncie informacyjnym działa on już od 1943 r. jako spiker Związku Polskich Patriotów w Moskwie[100]. Ten związek był narzędziem Józefa Stalina i ZSRR do przygotowania warunków do przejęcia władzy w Polsce przez komunistów[101]. Niestety, działania Sputnika legitymizują znani polscy politycy. Udzielają oni wywiadów, w których krytykują działalność obecnego rządu. Nie jest to zabronione, lecz wypowiadanie się w medium otwarcie krytykującym podstawy polskiej polityki bezpieczeństwa (czyli sojusz z USA, członkostwo w UE i popieranie Ukrainy w walce z separatystami) wpisuje się w koncepcję wprowadzania coraz większych podziałów w polskim społeczeństwie. Gdy robi to Stefan Niesiołowski, zasłużony opozycjonista z czasów PRL i były przewodniczący sejmowej Komisji Obrony Narodowej, Marek Belka, były Prezes Rady Ministrów i były prezes Narodowego Banku Polskiego, oraz byli posłowie Joanna Senyszyn i Andrzej Rozenek[102], może to sprawiać wrażenie, że Sputnik jest wiarygodnym źródłem informacji. Działalność Sputnika oraz telewizji RT (dawniej: Russia Today) skrytykował także obecny prezydent Francji Emmanuel Macron, który stwierdził, że zachowywały się one (…) *jak organy wpływu, propagandy, i to kłamliwej propagandy*[103].

Artykuły zamieszczane na portalu Sputnik News są także komentowane w sposób bardzo tendencyjny lub wręcz kłamliwy. Przykładem mogą być komentarze zamieszczane pod artykułem opisującym krytyczny stosunek rosyjskiej Dumy do wspólnej deklaracji polskiego Sejmu i Rady Najwyższej Ukrainy o II wojnie światowej. W dokumencie jest napisane, że pakt Ribbentrop–Mołotow doprowadził do wybuchu II wojny światowej. Deputowani rosyjscy uznali, że ta deklaracja jest próbą rewizji historii ZSRR jako zwycięzcy wojny i jest podyktowana jedynie chęcią wspólnego zaszkodzenia Federacji Rosyjskiej[104]. (…)

[98] http://www.tvp.info/18949295/rosyjska-propaganda-teraz-po-polsku-sputnik-zaczal-nadawac [dostęp: 5 VI2017].

[99] https://pl.sputniknews.com/opinie/201512231686068-Konrad-Rekas-Donbas-konflikt-Ukraina/ [dostęp: 5 VI 2017], https://pl.sputniknews.com/opinie/201512231686228-Ukraina-gospodarka-bankrut-Konrad-Rekas-ideologia-banderowska/ [dostęp: 5 VI 2017], https://pl.sputniknews.com/polska/20150312108375/ [dostęp: 5 VI 2017].

[100] https://pl.sputniknews.com/polish.ruvr.ru/2013_05_10/Leonid-Sigan-dwie-trzecie-stulecia-w-jezyku-polskim/ [dostęp: 5 VI 2017].

[101] https://pl.wikipedia.org/wiki/Związek_Patriotów_Polskich [dostęp: 5 VI 2017].

[102] Zob. https://pl.sputniknews.com/opinie/201612174447693-Kaczynski-komunista-opinie/ [dostęp: 5 VI 2017], https://pl.sputniknews.com/opinie/201701134603782-Marek-Belka-specjalnie-dla-Sputnik-Polska-Leonid-Swiridow/ [dostęp: 5 VI 2017], https://pl.sputniknews.com/opinie/201706025591407-Senyszyn-szansa-suwerennosc-sankcje/ [dostęp: 5 VI 2017], https://pl.sputniknews.com/opinie/201602242141946-Obiecanki-cacanki-czyli-100-dni-niespenionych-obietnic-sigan/ [dostęp: 5 VI 2017].

[103] http://www.tvn24.pl/wiadomosci-ze-swiata,2/macron-rt-i-sputnik-byly-jak-organy-wplywu,744140.html [dostęp: 5 VI 2017].

[104] https://pl.sputniknews.com/polityka/201611304325679-duma-usa-wielka-brytania-deklaracja-pamieci-i-solidarnosci/ [dostęp: 5 VI 2017].

Grzegorz Baziur uważa, że stworzenie polskiej edycji Sputnika jest przejawem rosyjskiej agresji informacyjnej. Przytacza on opinię byłego wiceministra spraw zagranicznych Pawła Kowala. który powiedział, że (…) *w wojnie hybrydowej chodzi o narzucenie własnej narracji*, co jest zadaniem Sputnika[105]. W Polsce dodatkowym tematem, którego nośność zapewnia oddziaływanie informacyjne, jest katastrofa smoleńska oraz zwrot wraku samolotu i czarnych skrzynek[106]. Dziennik „Komsomolskaja Prawda" napisał, że niektórzy polscy politycy chętnie rewidują przyczyny katastrofy, a telewizja NTV stwierdziła w swoim materiale, że minister Antoni Macierewicz prowadzi wojnę informacyjną[107]. Z kolei Bohdan Piętka w swoim tekście na portalu Sputnik uznał, że ujawnienie błędów strony rosyjskiej podczas ekshumacji ciał osób, które zginęły 10 kwietnia 2010 r. pod Smoleńskiem, jest przejawem „antyrosyjskiej histerii"[108]. Głęboki podział polityczny wokół wyjaśniania przyczyn katastrofy, jaki wytworzył się w Polsce i jest widoczny chociażby w czasie obchodów kolejnych miesięcznic[109], stanowi podatny grunt dla oddziaływania na polskich polityków i obywateli. Antoni Dudek uważa, że spór o katastrofę smoleńską będzie trwał jeszcze długie lata i może nie doczekać się jednoznacznego rozstrzygnięcia. Dodał też, że warto pamiętać o tym, że (…) *w Polsce mieszkają – i mieszkać będą – ludzie, którzy już zauważyli beznadziejną jałowość i toksyczność smoleńskiej wojny*[110]. Jednak z punktu widzenia walki informacyjnej ten konflikt nie jest jałowy i służy do podsycania radykalnych postaw w celu dalszej dezorganizacji polskiego życia politycznego.

**Bibliografia:**

Banasik M., Parafianowicz R., *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe AON" 2015, nr 2, s. 5–25.

Baziur G., *„Po katastrofie smoleńskiej": polsko-rosyjska wojna informacyjna a geopolityka Federacji Rosyjskiej wobec Polski w latach 2010–2015*, „Przegląd Geopolityczny" 2016, t. 15, s. 135–152.

Bożek M., Czuryk M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, Wolters Kluwer.

Bryjka F., *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej*, w: *Bezpieczeństwo personalne a bezpieczeństwo strukturalne*, t. 3: *Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*, Wrocław 2015,

[105] G. Baziur, *„Po katastrofie smoleńskiej": polsko-rosyjska wojna informacyjna a geopolityka Federacji Rosyjskiej wobec Polski w latach 2010–2015*, „Przegląd Geopolityczny" 2016, t. 15, s. 140.

[106] Tamże, s. 144.

[107] http://wiadomosci.onet.pl/swiat/rosyjska-tv-ntv-wojna-informacyjna-antoniego-macierewicza/36z8sv [dostęp: 5 VI 2017].

[108] https://pl.sputniknews.com/opinie/201706045591743-Smolensk-Barbarzynstwo-Rosjan/ [dostęp: 5 VI 2017].

[109] Zob. np. https://wiadomosci.wp.pl/kolejna-miesiecznica-smolenska-krzyki-i-przepychanki-na-krakowskim-przedmiesciu-6099667047089281a [dostęp: 5 VI 2017].

[110] http://antoni-dudek.salon24.pl/407005,w-cieniu-smolenskiej-wojny [dostęp: 5 VI 2017].

Wydawnictwo Wyższej Szkoły Oficerskiej Wojsk Lądowych imienia generała Tadeusza Kościuszki, s. 115–131.

Bryk T., *Przegląd regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego" 2011, nr 1, s. 223–234.

Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, OSW.

*Doktryna wojenna Federacji Rosyjskiej*, „Bezpieczeństwo Narodowe" 2015, nr 2, s. 177–206 (tłumaczenie robocze BBN).

Eberhardt P., *Koncepcja „Heartlandu" Halforda Mackindera*, „Przegląd Geograficzny" 2011, nr 2, s. 251–266.

Eberhardt P., *Rosyjski eurazjatyzm i jego konsekwencje geopolityczne*, „Przegląd Geograficzny" 2005, nr 2, s. 171–192.

Glenn R.W., *Thoughts, on „Hybrid" Conflict*, „Small Wars Journal" z 2 marca 2009 r., http://smallwarsjournal.com/mag/docs-temp/188-glenn.pdf [dostęp: 7 I 2017].

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia i wyzwania*, Kraków 1999, Wydawnictwo Fundacji Postępu Telekomunikacji.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa 2008, Wydawnictwo Naukowe PWN.

Gołda-Sobczak M., *Krym jako przedmiot sporu ukraińsko-rosyjskiego*, Poznań 2016, Silva Rerum.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red.), Warszawa 2011, BBN, s. 9–18, https://www.bbn.gov.pl/download/1/8729/Asymetriaihybrydowoscstarearmiewobecnowychkonfliktow.pdf [dostęp: 8 I 2017].

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, Potomac Institute for Policy Studies, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 4 I 2017].

*Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalności CERT Polska*, CERT Polska, https://www.cert.pl/PDF/Raport_CP_2016.pdf. [dostęp: 4 VI 2017].

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012, Wydawnictwo Naukowe PWN.

*(Mini)słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*, BBN, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html. [dostęp: 8 I 2017].

Minkina M., Gałek B., *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015, RYTM.

Nemeth W.J., *Future war and Chechnya: A case for hybrid warfare*, Monterey 2002, Naval Postgraduate School, http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1&isAllowed=y [dostęp: 3 I 2017].

Nowacki G., *Działania psychologiczne w działaniach sojuszniczych*, Warszawa 2003, AON.

Opaliński B., *Stan wojenny we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2011, nr 7–8, s. 65–86.

Potulski J., *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, Wydawnictwo Uniwersytetu Gdańskiego.

Prokop K., *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej*, Białystok 2005, Temida 2.

*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [dostęp: 2 VI 2017].

*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [dostęp: 2 VI 2017].

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne", Warszawa 2015, s. 39–50.

*Słownik języka polskiego PWN*, http://sjp.pwn.pl/slowniki/hybryda.html [dostęp: 3 I 2017].

Stupples D., *The next war will be an information war, and we're not ready for it*, https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218 [dostęp: 11 I 2017].

Sun Tzu, *Sztuka wojny*, http://www.lazarski.pl/fileadmin/user_upload/dokumenty/student/Sun_Tzu_sztuka_wojny.pdf [dostęp: 9 I 2017].

*US Army, Field Manual 3-0 Operations C-1*, Washington 2011, https://fas.org/irp/dod-dir/army/fm3-0.pdf, s. 1–5 [dostęp: 7 I 2017].

Wojnowski M., *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne", Warszawa 2015, s. 7–38.

Zaremba M., *Memy internetowe (2010–2011)*, „Media i Społeczeństwo" 2012, nr 2, s. 60–73.

*Słownik terminów z zakresu bezpieczeństwa narodowego*, B. Zdrodowski (red.), Warszawa 2008, AON.

**Akty prawne:**

*Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r*. (Dz.U. z 1997 r. nr 78 poz. 483, ze zm.).

*Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: Dz.U. z 2017 r. poz. 1978, ze zm.).

*Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (t.j.: Dz.U. z 2017 r. poz. 1932).

*Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (t.j.: Dz.U. z 2017 r. poz. 1928).

*Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz.U. z 2017 r. poz. 1920, ze zm.).

**Źródła internetowe:**

http://antoni-dudek.salon24.pl/407005,w-cieniu-smolenskiej-wojny.

http://kresy.pl/publicystyka/nato-czyli-jak-prowokowac-rosje-nie-broniac-polski/.

http://niezalezna.pl/58668-sympatycy-putina-w-warszawie-prorosyjska-manifestacja-pod-ambasada-ukrainy.

http://rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/.

http://technowinki.onet.pl/biznes-i-finanse/nowy-bohater-rosji-haker-ktory-okradl-usa-bez-wstawania-z-kanapy/zhmdr.

http://technowinki.onet.pl/oprogramowanie/rosyjskie-sluzby-wykorzystaly-botnet-do-szpiegowania-amerykanskiej-administracji/qg4cqk.

http://wiadomosci.onet.pl/kraj/gw-kreml-potajemnie-finansowal-w-polsce-ruchy-anty-ukrainskie/byvkxhh.

http://wiadomosci.onet.pl/swiat/rosyjska-tv-ntv-wojna-informacyjna-antoniego-maciewicza/36z8sv.

http://wiadomosci.onet.pl/tylko-w-onecie/ecag-rozszerza-wplywy-w-polsce-jest-jawnie-prorosyjskie-i-proputinowskie/25h7l9.

http://www.bbc.com/news/uk-31070114.

http://www.cyberdefence24.pl/382418,kampanie-phishingowe-rosna-w-tempie-800-procent-rocznie.

http://www.eastbook.eu/2016/09/19/na-kolanach-przed-rosyjska-potega-o-dzialalnosci-portalu-kresy-pl/.

http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2013/33/spear-phishing-czyli-ataki-spersonalizowane.aspx.

http://www.newsweek.pl/swiat/rosyjscy-hakerzy-ingerowali-w-wybory-w-usa-co-na-to-donald-trump-,artykuly,402729,1.html.

http://www.newsweek.pl/swiat/wynajeci-rosjanie-cyber-bombarduja-polski-internet-newsweek-cyberatak,artykuly,281538,1.html.

http://www.polskatimes.pl/fakty/swiat/a/usa-donald-trump-uznal-fakt-ze-rosja-stoi-za-cyberatakami-na-serwery-partii-demokratycznej,11667906/.

http://www.rp.pl/artykul/1163284-PKW-ignorowala-ostrzezenia.html#ap-1.

http://www.rp.pl/Telekomunikacja-i-IT/304289934-Rosyjscy-hakerzy-masowo-atakuja-polskie-komputery.html#ap-1.

http://www.sdpwarszawa.pl/aktualnosci-254,Zarzad_OW_SDP_zaniepokojony_postawa_kresy.pl.html.

http://www.tvn24.pl/wiadomosci-ze-swiata,2/dla-fbi-jewgienij-bogaczew-wart-jest-trzy-miliony-dolarow,723039.html.

http://www.tvn24.pl/wiadomosci-ze-swiata,2/macron-rt-i-sputnik-byly-jak-organy-wplywu,744140.html.

http://www.tvp.info/18949295/rosyjska-propaganda-teraz-po-polsku-sputnik-zaczal-nadawac.

http://wyborcza.pl/1,75398,20132090,abw-partie-zmiana-zalozyli-rosjanie.html.

http://wyborcza.pl/7,156282,21815396,ransomware-wannacry-w-polsce-zainfekowanych-ponad-1-tys-urzadzen.html.

http://xportal.pl/?p=15402.

https://niebezpiecznik.pl/post/anonimowi-wypowiedzieli-wojne-isis-owi-jak-chca-z-nim-walczyc-w-sieci/.

https://niebezpiecznik.pl/post/jak-przeprowadzono-atak-na-knf-i-polskie-banki-oraz-kto-jeszcze-byl-na-celowniku-przestepcow/.

https://niebezpiecznik.pl/post/kulisy-pracy-rosyjskich-prorzadowych-trolli-internetowych/.

https://pl.sputniknews.com/opinie/201512231686068-Konrad-Rekas-Donbas-konflikt-Ukraina/.

https://pl.sputniknews.com/opinie/201512231686228-Ukraina-gospodarka-bankrut-Konrad-Rekas-ideologia-banderowska/.

https://pl.sputniknews.com/opinie/201602242141946-Obiecanki-cacanki-czyli-100-dni-niespenionych-obietnic-sigan/.

https://pl.sputniknews.com/opinie/201612174447693-Kaczynski-komunista-opinie/.

https://pl.sputniknews.com/opinie/201701134603782-Marek-Belka-specjalnie-dla-Sputnik-Polska-Leonid-Swiridow/.

https://pl.sputniknews.com/opinie/201706025591407-Senyszyn-szansa-suwerennosc-sankcje/.

https://pl.sputniknews.com/opinie/201706045591743-Smolensk-Barbarzynstwo-Rosjan/.

https://pl.sputniknews.com/polish.ruvr.ru/2013_05_10/Leonid-Sigan-dwie-trzecie-stulecia-w-jezyku-polskim/.

https://pl.sputniknews.com/polityka/201611304325679-duma-usa-wielka-brytania-deklaracja-pamieci-i-solidarnosci/.

https://pl.sputniknews.com/polska/20150312108375/.

https://pl.wikipedia.org/wiki/Wybory_samorz%C4%85dowe_w_Polsce_w_2014_roku#cite_note-8.

https://pl.wikipedia.org/wiki/Związek_Patriotów_Polskich.

https://wiadomosci.wp.pl/kolejna-miesiecznica-smolenska-krzyki-i-przepychanki-na-krakowskim-przedmiesciu-6099667047089281a.

https://www.avast.com/pl-pl/c-phishing.

https://www.cashless.pl/temat-dnia/2433-new-york-times-to-koreanczycy-stali-za-atakiem-na-knf-i-polski-sektor-bankowy.

https://www.cashless.pl/wiadomosci/bezpieczenstwo/item/199-atak-phishingowy-na-klientow-ing-banku-slaskiego; http://www.bankier.pl/wiadomosc/Atak-phishingowy-na-klientow-PKO-Banku-Polskiego-7358309.html.

https://www.cybsecurity.org/pl/co-to-jest-botnet-i-dlaczego-nalezy-zachowac-ostroznosc/.

https://www.facebook.com/RosyjskaVKolumnawPolsce/?fref=ts.

https://zaufanatrzeciastrona.pl/post/jak-najprawdopodobniej-doszlo-do-globalnej-infekcji-ransomare-wannacry/.

**Słowa kluczowe**: wojna hybrydowa, wojna informacyjna, geopolityka, stany nadzwyczajne, cyberprzestrzeń.

**Keywords**: hybrid warfare, information warfare, geopolitics, extraordinary measures, cyberspace.

**Daniel Czebiełko**

# Bezpieczeństwo energetyczne na przykładzie powiatu będzińskiego[1]

Dynamiczny rozwój technologiczny społeczeństwa globalnego oraz postępująca urbanizacja są związane z większym zapotrzebowaniem na energię elektryczną oraz cieplną we współczesnym świecie. Wszystkie czynności podejmowane przez ludzi wymagają różnej formy energii, bez względu na to, czy jest ona wykorzystywana do funkcjonowania systemów informatycznych, w przemyśle, czy też do ogrzewania domów. Dlatego tak ważne jest wydajne i sprawne wytwarzanie energii dla odbiorców.

Nie ulega wątpliwości, że problemem świata jest ciągły wzrost zapotrzebowania na energię elektryczną i cieplną. Jest to spowodowane szybkim rozwojem gospodarek oraz wzrostem liczby ludności na świecie. Szacuje się, że przy obecnym poziomie wytwarzania energii, m.in. elektrycznej, światowe zasoby nieodnawialnych źródeł energii zostaną wyeksploatowane. **W artykule opublikowanym przez CIRE podano, że węgla kamiennego i brunatnego starczy prawdopodobnie na 158 lat, ropy na 41 lat, a gazu na 63 lata**[2]. Równie istotnym problemem dla energetyki jest emisja m.in. pyłów czy tlenków węgla wywołana spalaniem węgla, mająca negatywny wpływ na środowisko. Nie ulega wątpliwości, że wraz z wyczerpywaniem się zasobów nieodnawialnych źródeł energii świat staje przed problemem zaistnienia licznych konfliktów, a wśród nich bardzo prawdopodobny wydaje się konflikt pomiędzy państwami importującymi energię a państwami produkującymi surowce do jej produkcji. Sektor wytwarzający energię jest ważnym elementem gospodarki każdego państwa, a zdobycie surowców energetycznych niejednokrotnie w historii było przyczyną konfliktów[3]. Tego typu kłopotów nie uniknie żadne państwo, w tym również Polska.

Głównym problemem energetycznym Polski jest niezmodernizowana infrastruktura techniczna, m.in. urządzenia energetyczne oraz linie przesyłowe, które są wykorzystywane do produkcji energii elektrycznej i cieplnej. Aktualny stan techniczny infrastruktury energetycznej ma niekorzystny wpływ na rozwój gospodarczy kraju, przyczynia się także do zanieczyszczenia atmosfery. Wraz z przystąpieniem do Unii Europejskiej (w 2004 r.) Polska zobowiązała się do przestrzegania dyrektyw unijnych narzucających

[1] Fragment pracy licencjackiej pt. *Bezpieczeństwo energetyczne na przykładzie powiatu będzińskiego* (Akademia Sytuki Wojennej). Praca została wyróżniona w siódmej edycji Ogólnopolskiego konkursu Szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2016/2017). Autor wykorzystał fragmenty: wstępu, rozdziału 1, 2 i 3. Autor jest studentem Akademii Sztuki Wojennej, Wydziału Bezpieczeństwa Narodowego.

[2] E. Mokrzycki, R. Ney, J. Siemek, *Światowe zasoby surowców energetycznych – wnioski dla Polski*, http://www.rynek-ciepla.cire.pl/pliki/2/swiatowe_zasoby.pdf [dostęp: 1 XI 2016].

Wszystkie wyróżnienia pochodzą od autora (przyp. red.).

[3] G. Bartodziej, M. Tomaszewski, *Polityka energetyczna i bezpieczeństwo energetyczne,* Racibórz–Warszawa 2009, s. 17.

krajom członkowskim liczne ograniczenia w dziedzinie ochrony środowiska, co przy obecnym stanie infrastruktury energetycznej może spowodować zamknięcie 70 proc. elektrowni zawodowych w Polsce. Taka sytuacja przyczyniałaby się zatem do utraty niezależności energetycznej Polski[4].

Równowaga między produkcją krajową a konsumpcją jest istotnym elementem zapewniania bezpieczeństwa energetycznego. Według Janusza Kowalskiego i Jakuba Kozery: *Bezpieczeństwo energetyczne jest częścią bezpieczeństwa narodowego, które obejmuje działania związane z pokryciem zapotrzebowania gospodarki na nośniki energii* (…)[5].

Na potrzeby niniejszej pracy ważne jest zdefiniowanie Krajowego Systemu Elektroenergetycznego (KSE). Krajowy System Elektroenergetyczny to inaczej zbiór elementów przeznaczonych do produkcji, przesyłu i dystrybucji energii elektrycznej na obszarze kraju oraz poza jego granicami. **System elektroenergetyczny składa się m.in. ze stacji transformatorowo-rozdzielczych**, **linii przesyłowych, elektrowni oraz odbiorników energii elektrycznej**. Jego funkcjonowanie ma na celu zapewnienie ciągłości dostaw energii dla całego obsługiwanego obszaru. Współcześnie w Polsce nie ma możliwości magazynowania wytwarzanej energii, co powoduje, że KSE musi nią racjonalnie gospodarować, a dodatkowo uwzględniać wahania cenowe pojawiające się na rynku energii.

Problemem energetyki na poziomie lokalnym, w tym także w powiecie będzińskim, jest ograniczenie kompetencji, odpowiedzialności i samorządności władz lokalnych. Działania związane z bezpieczeństwem energetycznym w powiecie będzińskim ograniczają się obecne do zatwierdzania planu zapotrzebowania na energię przez władze gmin, co przyczynia się do braku odpowiedzialności i samorządności w zakresie dostaw energii na potrzeby rynku lokalnego. W wyniku centralizacji polityki energetycznej państwa samorządy gminne borykają się z trudnościami organizacyjnymi i podziałem odpowiedzialności w czasie klęski żywiołowej lub kryzysu.

## 1. Środowisko i uwarunkowania powiatu będzińskiego

### 1.1. Ogólna charakterystyka powiatu będzińskiego

**Powiat będziński jest zlokalizowany w centralnej części województwa śląskiego i zajmuje łącznie powierzchnię 368 km**, co plasuje go na 13. miejscu wśród powiatów ziemskich[6] i miast na prawach powiatu w regionie śląskim[7]. Powiat będziński obejmuje następujące gminy: Będzin, Czeladź, Siewierz, Psary, Sławków, Mierzęcice, Wojkowice, Bobrowniki.

[4] A. Gradziuk i in., *Co to jest bezpieczeństwo energetyczne państwa?*, „Biuletyn PISM" 2002, nr 103, s. 705–708.

[5] J. Kowalski, J. Kozera, *Mapa zagrożeń bezpieczeństwa energetycznego RP w sektorach ropy naftowej i gazu ziemnego*, „Bezpieczeństwo Narodowe" 2009, nr 1–2, s. 301.

[6] Powiat ziemski jest jednostką samorządu terytorialnego obejmującą sąsiadujące ze sobą gminy, www.um.jelcz-laskowice.finn.pl [dostęp: 1 XI 2016].

[7] *Aktualizacja Strategii Rozwoju Powiatu Będzińskiego na lata 2009–2020*, Będzin 2014, s. 23.

Według Starostwa Powiatowego w Będzinie gęstość zaludnienia w powiecie jest wysoka, co jest charakterystyczne dla całego województwa śląskiego. Dowodem tego są wyniki w rankingach, w których powiat będziński zajmuje wysoką, trzecią, pozycję wśród wszystkich 17 powiatów ziemskich. Jeśli uwzględni się wszystkie powiaty ziemskie i miasta na prawach powiatu (36 jednostek), to powiat będziński znajduje się na wysokiej, 11. pozycji[8].

**Trzonem gospodarki powiatowej jest sektor elektroenergetyczny**. Na terenie powiatu są zlokalizowane przedsiębiorstwa energetyczne wytwarzające energie elektryczną oraz zakład produkujący kable elektroenergetyczne. W jednej z dzielnic Będzina, Łagisza, znajduje się **Elektrownia Łagisza, która jest ósmą w kraju pod względem mocy elektrownią opalaną węglem kamiennym**. Z kolei w dzielnicy Małobądz zlokalizowano Elektrociepłownię Będzin SA będącą największym lokalnym producentem energii cieplnej. Te obiekty to czołówka krajowych przedsiębiorstw branży energetycznej dostarczających energię elektryczną i ciepło zarówno mieszkańcom regionu, jak i mieszkańcom całego kraju.

Ważną gałęzią gospodarki powiatu jest logistyka. Najlepszym tego przykładem jest gmina Sławków, w której walorem gospodarczym są Paneuropejskie Korytarze Transportowe oraz szerokotorowy szlak kolejowy z Ukrainą, Rosją oraz Chinami. Gospodarkę powiatu tworzy także przemysł górniczy reprezentowany przez Górnicze Zakłady Dolomitowe w gminie Siewierz, które wydobywają kruszywa pod budowę dróg[9]. Elementem dopełniającym gospodarkę powiatu jest drobna wytwórczość, rzemiosło i usługi. (…)

## 2. Bezpieczeństwo energetyczne na terenie powiatu będzińskiego – stan aktualny

### 2.1. System bezpieczeństwa elektroenergetycznego na terenie powiatu

Koncentrując się na bezpieczeństwie elektroenergetycznym na poziomie powiatu, należy wspomnieć że jego podstawą jest Krajowy System Elektroenergetyczny składający się m.in. z **zespołów urządzeń przeznaczonych do: wytwarzania, przesyłu oraz rozdziału energii elektrycznej**[10]. Krajowy System Elektroenergetyczny charakteryzuje się również małym zróżnicowaniem paliwa, głównymi paliwami do wytwarzania energii elektrycznej **jest węgiel kamienny i brunatny**.

System bezpieczeństwa elektroenergetycznego na poziomie powiatu jest podobny do systemu KSE, który, jak już wspomniano, dzieli się na następujące podsystemy: podsystem wytwórczy, sieć przesyłowa, sieć dystrybucyjna.

Do **podsystemu wytwórczego** należą m.in. elektrownie systemowe, elektrownie przemysłowe, elektrociepłownie lokalne, elektrownie wodne, wiatrowe, słoneczne, opalane biomasą lub biogazem. Na potrzeby niniejszej pracy autor odnosi się do dwóch definicji: elektrownie systemowe oraz elektrownie przemysłowe.

[8] Tamże.
[9] Tamże, s. 38.
[10] Tamże.

Elektrownie systemowe rozumie się jako (…) *zakład, którego głównym zadaniem jest wytwarzanie dużych ilości energii elektrycznej, przesyłanej następnie przez sieci wysokich napięć do odbiorców w całym kraju*[11]. Natomiast elektrownia przemysłowa to (…) *zespół urządzeń wraz z potrzebnymi budowlami, służącymi do przetwarzania określonego rodzaju energii, na potrzeby zakładów przemysłowych*[12].

Polski podsystem wytwórczy składa się z czterech największych spółek państwowych i dwóch podmiotów prywatnych, które wytwarzają prąd elektryczny dla krajowego systemu. **Do spółek Skarbu Państwa należą: PGE, Energa, Tauron, Enea.** Natomiast **w skład spółek prywatnych wchodzą EDF Energy i RWE**. Największą spółką wytwarzającą energię elektryczną w KSE jest Grupa Kapitałowa Polskiej Grupy Energetycznej dysponująca 40 elektrowniami i 40 elektrociepłowniami. Przykładem największej elektrowni tej spółki jest **elektrownia Bełchatów, która wytwarza 5420 MWh**. Należy również wspomnieć, że PGE jest właścicielem dwóch kopalni węgla brunatnego, które stanowią źródło energii elektryczne i cieplnej. Według informacji zamieszczonych przez spółkę PGE **wyprodukowała ona 56,52 TWh w 2011 r.** energii elektrycznej, co stanowiło blisko 40 proc. produkcji krajowej.

Za **podsystem sieci przesyłowej** w KSE jest odpowiedzialna spółka pod nazwą Polskie Sieci Elektroenergetyczne (PSE) należąca do Skarbu Państwa. Odpowiada ona za zarządzanie sieciami i dalszy rozwój sieci przesyłowych na terytorium Polski. Spółka głównie zarządza liniami i stacjami elektroenergetycznymi o napięciu 750 kV, 400 kV oraz 220 kV, natomiast linie o niższym napięciu są zarządzane przez operatorów energii elektrycznej.

Należałoby postawić pytanie, czy oparcie produkcji energii elektrycznej i cieplnej na dużych koncernach (państwowych lub prywatnych) wpłynie negatywnie na zbudowanie potencjalnych przedsiębiorstw energetycznych na poziomie lokalnym? Prawdopodobnie należy się z takim poglądem zgodzić, ponieważ brak alternatywy dla aktualnego systemu elektroenergetycznego przy potencjalnym zniszczeniu lub uszkodzeniu sieci przesyłowych przez cyberataki lub złe warunki atmosferyczne może skutkować poważnymi konsekwencjami, m.in. stałym niedoborem energii elektrycznej w okresie zimowym, który doprowadziłby do wybuchu paniki wśród obywateli. Według autora utrata lub niedobór energii elektrycznej w okresie zimowym jest groźnym zjawiskiem dla bezpieczeństwa elektroenergetycznego kraju.

Reasumując, za politykę bezpieczeństwa energetycznego odpowiada minister do spraw energii, któremu podlegają państwowe spółki energetyczne i kopalnie wydobywające paliwo do wytwarzania energii elektrycznej. Zgodnie z przepisami zawartymi w ustawie – Prawo energetyczne[13] Ministerstwo Energii opracowuje politykę energetyczną państwa na podstawie ustanowionego prawa energetycznego, a także nakłada, m.in. na samorządy, zadania z nią związane.

[11] Tamże.
[12] *Nowy słownik języka polskiego*, Warszawa 2011, s. 128.
[13] *Ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne* (t.j.: Dz.U. z 2018 r. poz. 755, ze zm. – przyp. red.).

W obecnym systemie powiat nie ma wyznaczonych kompetencji związanych z polityką energetyczną państwa, co skutkuje brakiem odpowiedzialności samorządu powiatowego za bezpieczeństwo energetyczne. Jednocześnie obowiązujące prawo nie pozwala jednostkom powiatowym na zapewnienie dostaw energii i jej dystrybucję na swoim terenie.

W celu zrozumienia systemu bezpieczeństwa elektroenergetycznego na poziomie lokalnym warto posłużyć się schematem, na którym przedstawiono procedurę planowania energetycznego na terenie gminy (schemat 1). Jak już wspomniano, w obecnym systemie elektroenergetycznym powiat nie odgrywa dużej roli, w świetle prawa energetycznego nie ma żadnych kompetencji związanych z bezpieczeństwem energetycznym kraju. Samorząd powiatu jest w obecnym systemie pominięty, a jego potencjał niewykorzystany. Główne przedsięwzięcia związane z bezpieczeństwem energetycznym ciążą bezpośrednio na władzach gmin.


**Schemat 1.** Procedura planowania energetycznego na szczeblu gminy[14].

Źródło: Opracowanie własne na podstawie danych gminy Będzin, *Plan zapotrzebowania w ciepło, energię elektryczną i paliwa gazowe na obszarze miasta Będzin,* Katowice 2013, s. 22.

Z powyższego schematu wynika, że prezydent miasta, burmistrz oraz wójt mają obowiązek stworzyć plan zaopatrzenia w energię i aktualizować go co trzy lata. W planie jest zawarta: ocena aktualnego zapotrzebowania gminy na energię, określenie własnych

[14] Procedura SOOŚ – procedura strategicznej oceny oddziaływania na środowisko (przyp. red.).

zasobów paliw do produkcji energii oraz odnawialnych źródeł energii, identyfikacja przewidywanych możliwości rozwoju gminy na następne 15 lat, potrzeby energetyczne dla istniejących i planowanych zabudowań na kolejne 15 lat, propozycja niezbędnych działań w celu zapewnienia zaopatrzenia w energię, środki poprawy efektywności energetycznej, zakresy możliwej współpracy między gminami[15]. (…)

### 2.2. Akty normatywne

Podstawowym elementem w planowaniu energetycznym na poziomie lokalnym jest prawo, które w chwili obecnej nie nakłada na poszczególne jednostki samorządu terytorialnego bezpośredniej odpowiedzialności za tę dziedzinę. Dotychczasowe zadania nałożone na samorządy gminne zobowiązują gminy do planowania i organizacji zaopatrzenia w ciepło, energię elektryczną i paliwa gazowe na swoim terenie. Powoduje to, że luki prawne ograniczają rozwój lokalnych spółdzielni produkujących energię elektryczną i cieplną. Ta sytuacja może stanowić zagrożenie dla stabilności dostaw energii w obliczu współczesnych zagrożeń.

Zgodnie z art. 7 ust. 1 poz. 3 ustawy o samorządzie gminnym[16], **obowiązkiem gminy jest zaspokojenie zbiorowych potrzeb jej mieszkańców**. Wśród zadań własnych gminy wymienia się w szczególności sprawy: (…) *wodociągów i zaopatrzenia w wodę, kanalizacji, usuwania i oczyszczania ścieków komunalnych, utrzymania w czystości i porządku urządzeń sanitarnych oraz wysypisk, unieszkodliwienia odpadów komunalnych, zaopatrzenia w energię elektryczną i cieplną oraz gaz*.

W art. 18 ustawy – Prawo energetyczne wskazano, w jaki sposób gmina powinna wywiązywać się z obowiązków nałożonych na nią w ustawie o samorządzie gminnym. Te zapisy, odnosząc się do zadań gminy w zakresie zaopatrzenia w energię elektryczną, ciepło i paliwa gazowe, skupiają się wyłącznie na planowaniu, co jest dalece niewystarczające w obliczu współczesnych zagrożeń.

Powyższe działania nie zapewniają gminom zaopatrzenia w energię. Na jednostkach samorządowych – poza obowiązkiem planowania – powinny spoczywać obowiązki wykonawcze z zakresu zabezpieczenia dostaw energii przez stworzenie lokalnej sieci i pozyskanie alternatywnych źródeł energii.

Dla przykładu warto przypomnieć, że gminie podlegają jednostki, które zajmują się dostarczaniem wody i jej oczyszczaniem. Dzięki temu gminy są niezależne od systemu centralnego. Nie dotyczy to jednak zaopatrzenia w energię elektryczną, cieplną i gazową, gdyż w tym zakresie prawo energetyczne nie reguluje potencjalnej budowy niezależnego systemu elektroenergetycznego. Jednocześnie w bardzo ograniczonym stopniu pozwala na rozwój lokalnych struktur zabezpieczających dostawy energii elektrycznej i cieplnej.

[15] A. Jankowski, *Aktualizacja założeń do planu zaopatrzenia w ciepło, energię elektryczną i paliwa gazowe na obszarze miasta Będzin*, Katowice–Będzin 2013, Energoekspert, s. 22.

[16] U*stawa z dnia 8 marca 1990 r. o samorządzie gminnym* (t.j.: Dz.U. z 2018 r. poz. 994, ze zm.).

### 2.3. Infrastruktura

Infrastruktura elektroenergetyczna systemu bezpieczeństwa elektroenergetycznego powiatu będzińskiego jest obsługiwana miedzy innymi przez zakłady energetyczne, takie jak Elektrociepłownia Będzin S.A., Elektrownia Łagisza S.A. oraz mała elektrownia wodna w Siewierzu, które są elementami KSE.

Podstawowym paliwem dla elektrowni i elektrociepłowni jest węgiel kamienny dostarczany przez pobliskie kopalnie węgla kamiennego, które znajdują się w okolicznych miastach, m.in. w Jaworznie. Dla elektrowni wodnej paliwem jest **Czarna Przemsza**. W tabeli ukazano producentów energii elektrycznej w powiecie będzińskim.

**Tabela.** Produkcja energii elektrycznej i cieplnej w MWh i TJh na terenie powiatu będzińskiego.

| Elektrownie | Moc w MWh | Moc w TJh |
|---|---|---|
| Elektrownia Łagisza | 820 | 1,206 |
| Elektrociepłownia Będzin | 78 | 1,492 |
| Mała elektrownia wodna w Siewierzu | 10 | 0 |

Źródło: Opracowanie własne na podstawie danych z Elektrowni Łagisza, Elektrociepłowni Będzin, małej elektrowni wodnej w Siewierzu.

Głównym zakładem wytwarzającym oraz dostarczającym energię elektryczną i cieplną mieszkańcom powiatu będzińskiego jest elektrownia Łagisza. Obecnie należy ona do Grupy TAURON Wytwarzanie SA. W skład infrastruktury technicznej elektrowni wchodzą **trzy bloki o mocy po 120 MWeh każdy i jeden o mocy 460 MWeh, co daje łączną moc energii elektrycznej 820 MWeh,**[17] **oraz moc cieplną o wysokości 335,20 MWth**[18].

Jak się okazuje elektrownia posiada również najnowocześniejszy element, jakim jest blok o mocy 460 MW, którego sercem jest kocioł fluidalny CFB. Kocioł parowy z paleniskiem fluidalnym charakteryzuje się lepszą redukcją zawartości siarki w spalinach w czasie produkcji energii oraz efektywniejszą produkcją energii elektrycznej. **Moc kotła szacuje się na 1000 MWt**, **co jest w stanie zapewnić energię dla 1 mln 100 tys. ludzi**. Według informacji podawanych przez Tauron kocioł fluidalny CFB jest jedynym tego typu rozwiązaniem w Europie, co czyni go jednym z najbardziej innowacyjnych rozwiązań technologicznych w wytwarzaniu energii elektrycznej w Polsce. Na zdjęciu 1 przedstawiono blok o mocy 460 MW zlokalizowany na terenie elektrowni Łagisza.

[17] TAURON Wytwarzanie, http://www.tauron-wytwarzanie.pl [dostęp: 5.XII 2016].

[18] Obecna sprawność wytwarzania przy wskaźniku zużycia paliwa na produkcję energii elektrycznej brutto w 2000 r. była równa 9731 KJ/KWh. Wskaźnik potrzeb własnych bloków energetycznych – 7,71%. Wskaźnik potrzeb własnych bloków energetycznych powiększony o potrzeby ogólne elektrowni – 9,78%. Zob. TAURON Wytwarzanie, http://www.tauron-wytwarzanie.pl/oddzialy/lagisza/Strony/opis.aspx [dostęp: 5 XII 2016 ].

**Zdj. 1.** Blok Elektrowni Łagisza o mocy 460 MW posiadający kocioł fluidalny CFB.
Źródło: TAURON Wytwarzanie SA.

Drugim elementem istotnym dla bezpieczeństwa elektroenergetycznego powiatu będzińskiego są linie przesyłowe KSE rozciągnięte na całym jego obszarze. Na terenie powiatu będzińskiego można zidentyfikować linie wysokiego napięcia. Są one głównymi punktami zasilania i stacjami rozdzielczymi, m.in. Łagisza, która na swoim terenie oprócz elektrowni posiada także dwie rozdzielnie o mocy 400 kV, 220 kV, 100 kV oraz 110 kV, 20 kV, 6 kV, a także Główny Punkt Zasilania (GPZ). Główny Punkt Zasilania (…) *jest elementem systemu elektroenergetycznego przeznaczonym do rozdzielenia lub przetwarzania energii elektrycznej*[19], zasilającym energią elektryczną miasto lub kilkanaście miast. Oprócz Łagiszy na terenie powiatu znajdują się też inne GPZ, np. na terenie sąsiedniej gminy Czeladź znajdują się GPZ o mocy 110 kV, 30 kV i 6 kV, KWK Jowisz w Wojkowicach o mocy 110 kV, 30 kV, 6 kV, w Siewierzu o mocy 110, 15 kV oraz w Sarnowie o mocy 110 kV oraz 20 kV.

Infrastruktura przesyłowa jest najważniejszym elementem bezpieczeństwa energetycznego, ponieważ ich brak lub uszkodzenie powoduje, że cały system elektroenergetyczny, który jest połączony liniami, przestaje funkcjonować. (...)

## 3. Bezpieczeństwo energetyczne w powiecie będzińskim – kierunki rozwoju

### 3.1. System bezpieczeństwa elektroenergetycznego na terenie powiatu

Ta część pracy jest poświęcona ukazaniu potencjalnej modyfikacji KSE z uwzględnieniem systemu lokalnego na terenie powiatu będzińskiego. Nowe rozwiązanie

[19] W. Dołęga, *Stacje elektroenergetyczne*, Wrocław 2007, s. 9.

charakteryzowałoby się zrównoważonym wytwarzaniem i dystrybucją energii elektrycznej, które przede wszystkim tworzyłoby alternatywę w postaci lokalnego systemu elektroenergetycznego.

Pomysł został zaczerpnięty z polityki elektroenergetycznej obowiązującej w niektórych krajach Unii Europejskiej, opartej na istniejących spółdzielniach wykorzystujących odnawialne źródła energii (OZE). Skutkami polityki elektroenergetycznej w Unii Europejskiej są następujące zmiany: wzrost znaczenia sieci dostosowanych do przyłączenia dużych, scentralizowanych generacji odnawialnych, powstanie małych, lokalnych klastrów sieciowych, zapewniających usługi systemowe, obejmujące zdecentralizowaną generację lokalną, magazyny energii oraz aktywnych odbiorców oraz dwukierunkowy przepływ mocy elektrycznej i informacji[20].

Według autora **w ustawie o samorządzie powiatowym**[21] **w art. 33b** należałoby dopisać wyodrębnioną jednostkę zajmującą się bezpieczeństwem energetycznym na poziomie powiatowym, która mogłaby nosić nazwę np. **Powiatowa Rezerwa Energetyczna (PRE)**. Lokalne przedsiębiorstwo podlegałoby bezpośrednio starostwu powiatowemu. Do głównych zadań przedsiębiorstwa należałoby wypracowanie i koordynowanie prac związanych z tworzeniem lokalnych przedsiębiorstw energetycznych oraz zarządzanie lokalną siecią przesyłu energii elektrycznej w powiecie. Ich działanie mogłoby być wzorowane na przykład na gminnych zakładach wodnokanalizacyjnych, które na poziomie gminnym odpowiadają za oczyszczanie i doprowadzenie wody pitnej do gospodarstw domowych. Dzięki PRE mieszkańcy powiatu będą mogli otrzymać energię elektryczną (…) *w tzw.* ***formule „doublesupply”****, to znaczy, że odbiorcy ci nie będą musieli wypowiadać umów z dotychczasowym dostawcą, mając w każdym czasie możliwość wyboru źródła zasilania*[22].

Gospodarstwa domowe i lokalni przedsiębiorcy również będą mieli możliwość uzyskania energii od lokalnych spółdzielni, które zapewniają bezpieczeństwo energetyczne mieszkańcom między innymi podczas wojny czy klęski żywiołowej. Jest to bardzo korzystne rozwiązanie zapewnieniajce bezpieczeństwo elektroenergetyczne kraju ponieważ PRE w swojej infrastrukturze technicznej będzie dysponowało autonomicznymi liniami przesyłowymi i jednostkami wytwórczymi.

Potencjalne przedsiębiorstwo pod nazwą PRE mogłoby być zlokalizowane w następujących gminach: Będzin, Czeladź, Psary, Siewierz, Sławków, Wojkowice, Mierzęcice, Bobrowniki. To na tych terenach mogłyby w przeszłości funkcjonować lokalne przedsiębiorstwa energetyczne. Dzięki zasobom geologicznym tego terenu w poszczególnych gminach powstaną miejscowe przedsiębiorstwa energetyczne, które będą się charakteryzować inną metodą wytwarzania energii elektrycznej dla PRE. Na przykład w gminach Czeladź, Wojkowice, Będzin będzie można wykorzystać złoża zamkniętych kopalń m.in. do gazyfikacji metanu, co umożliwi powstanie gazowni, która będzie produkowała

[20] M. Wrocławski, *Lokalne obszary bilansowania*, „Energia Elektryczna” 2012, październik, s. 1.
[21] *Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym* (t.j: Dz.U. z 2018 r. poz. 995, ze zm. – przyp. red.).
[22] A. Rabiega*, Spółdzielnia Nasza Energia*, http://nasza-energia.com/opis-projektu/ [dostęp: 17 XII 2016].

energię elektryczną. Natomiast w gminach Siewierz i Sławków lokalne przedsiębiorstwa będą mogły korzystać ze złóż geotermalnych.

Kolejnym elementem systemu będzie zintegrowana sieć elektroenergetyczna, która, według Mieczysława Wrocławskiego[23], będzie uzależniona od zachowania wytwórców, odbiorców oraz innych podmiotów działających na rynku wytwarzania energii.

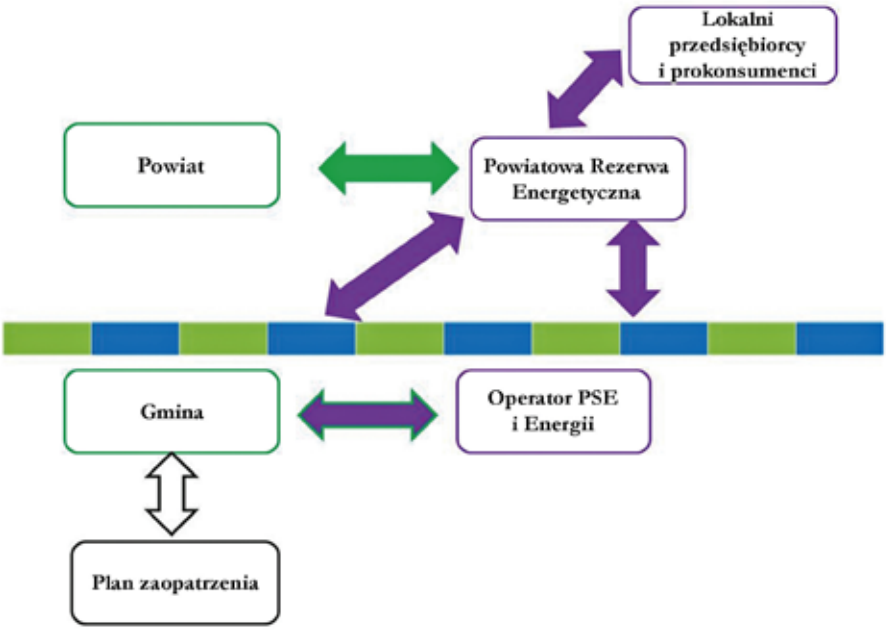
Oparte na zintegrowanych sieciach przesyłowych PRE zostaną połączone ze sobą, tworząc wspólny lokalny system elektroenergetyczny, przy jednoczesnym podłączeniu ich do Krajowego Systemu Elektroenergetycznego. Modelowo ukazuje to **Spółdzielnia Nasza Energia** działająca w województwie lubelskim, która zastosowała w dystrybucji miejscowy system przesyłu energii. Ta spółdzielnia wykorzystuje do dystrybucji energii **tzw. węzły energetyczne** (**Lokalny System Przesyłu, LSP)**, składające się z trzech urządzeń produkujących energię na terenie jednej gminy. Urządzenia wytwarzające energię są połączone kablami, które zapewniają przesył energii elektrycznej i cieplnej. Tylko jedno z tych urządzeń jest podłączone do krajowej sieci przesyłu.

W nowym systemie **powiat będzie odgrywać ważną rolę w polityce bezpieczeństwa energetycznego państwa dzięki realizacji polityki subsydiarności**[24]. Byłoby to związane z nadaniem kompetencji władzom powiatu w prawie energetycznym oraz utworzeniem PRE.

W obecnym planie o zaopatrzeniu gminy w energię znajdują się zapisy prawne, które dotyczą współpracy z innymi gminami, jednak taka współpraca istnieje tylko teoretycznie. Mimo to ten zapis daje możliwość powstania jednostki powiatowej, która skupiałaby gminy znajdujące się w granicach powiatu w zakresie dostaw energii i jej produkcji.

Aby zrozumieć koncepcję przemodelowania systemu bezpieczeństwa elektroenergetycznego powiatu, warto przeanalizować schemat 2.

[23] Tamże, s. 2.
[24] *Słownik Języka Polskiego PWN*, http://sjp.pl/subsydiarno%C5%9B%C4%87 [dostęp: 18 XII 2016].




**Schemat 2.** Koncepcja nowego systemu zaopatrywania w energię przez jednostki samorządu terytorialnego.

Źródło: Opracowanie własne na podstawie danych z gminy Będzin, *Plan zapotrzebowania w ciepło, energię elektryczną i paliwa gazowe na obszarze miasta Będzin,* Katowice 2013, s. 22.

Analiza schematu pozwala na stwierdzenie, że w obecnym systemie w gminie jest tworzony plan zaopatrzenia w energię dla tego terenu. Wójt kontroluje i współpracuje z operatorami, którzy wytwarzają lub przesyłają energię na terenie gminy. Widoczny jest tu brak włączenia w proces zaopatrywania w energię tak istotnej jednostki samorządu terytorialnego, jaką jest powiat. Uwzględnienie powiatu w powyższym planie zaopatrywania w energię elektryczną i cieplną zaowocowałoby lepszym zabezpieczeniem dostaw energii w przypadku ewentualnych niebezpieczeństw grożących zerwaniem tej płynności.

Operator energii (np. PGE SA) będzie również miał możliwość skorzystania z lokalnego systemu elektroenergetycznego w nagłych przypadkach, np. po uszkodzeniu systemu przesyłu energii. Te zabiegi mają na celu skuteczne zapobieżenie ewentualnym problemom z płynnością dostaw energii dla omawianego terenu oraz całego kraju.

### 3.2. Akty normatywne

Dotychczasowe rozważania prowadzą do wniosku, że należy podjąć analizę aktów prawnych, które kształtują bezpieczeństwo energetyczne na poziomie lokalnym, a także odgrywają ważną rolę w planowaniu energetycznym. Należy zatem wspomnieć o podstawach prawnych, które określają zadania i kompetencje poszczególnych jednostek terytorialnych, zobowiązanych do zapewnienia dostaw energii.

Po analizie aktów prawnych autor doszedł do wniosku, że, niestety, obowiązujące prawo energetyczne dotyczące lokalnej energetyki jest wadliwe, gdyż nie uwzględniono w nim zadań gminy dotyczących zaopatrzenia swoich obywateli w energię. Takie zadania są obecnie realizowane tylko teoretycznie. Najlepszym tego potwierdzeniem są zapisy w prawie energetycznym, koncesyjnym oraz podatkowym, które utrudniają gminie realizację zadań nałożonych przez ustawy: **o samorządzie powiatowym**, **Prawo energetyczne** i **Prawo geologiczne i górnicze**[25]. Tym samym stworzenie przez gminę systemu niezależnego od systemu centralnego jest utrudnione dla samorządu powiatowego. Dlatego też w wymienionych powyżej przepisach należałoby wprowadzić korekty legislacyjne.

Należałoby wprowadzić regulacje umożliwiające realizację **instalacji tzw. spółdzielni energetycznych**. Te zaś podlegałyby jednostce powiatowej, która stanowiłaby alternatywę w KSE. Dzięki wprowadzeniu proponowanych zmian można byłoby uniknąć problemów związanych z wymogami regulacyjnymi dla przedsiębiorców wytwarzających energię elektryczną i cieplną czy z uzyskaniem koncesji. To wszystko w dużym stopniu będzie umożliwiało rozwój lokalnej energetyki.

**Korekta legislacyjna w ustawie o samorządzie powiatowym powinna nastąpić w art. 4 ust. 1**, który dotyczy obszarów działania powiatu, przez dopisanie do zadań samorządów obszaru związanego z bezpieczeństwem energetycznym państwa. Według nowelizacji ustawy jednostka organizacyjna, która stanowiłaby narzędzie starostwa powiatowego w zakresie lokalnego bezpieczeństwa energetycznego, zajmowałaby się m.in. **lokalnym system elektroenergetycznym oraz współpracowałaby z lokalnymi producentami, operatorem PSE oraz operatorami wytwarzanej energii w KSE**.

Te zmiany legislacyjne umożliwiłyby samorządowi powiatowemu realne wprowadzenie Powiatowej Rezerwy Energetycznej.

### 3.3. Infrastruktura

Aby właściwie zrozumieć kierunki rozwoju bezpieczeństwa energetycznego w systemie elektroenergetycznym na terenie powiatu będzińskiego, nie można pominąć infrastruktury wykorzystywanej do produkcji energii elektrycznej i ciepła dla mieszkańców.

Rozwój lokalnych spółdzielni energetycznych wykorzystujących odnawialne źródła energii spowoduje, że właściciel zakładu będzie musiał zmienić rodzaj paliwa lub technologię produkcji energii cieplnej i elektrycznej. Modernizacja obecnie istniejącej na danym terenie infrastruktury opartej na węglu w perspektywie rozwoju energii OZE i lokalnych spółdzielni nie będzie dobrym rozwiązaniem z punktu widzenia środowiska czy polityki energetycznej kraju.

Potencjalnie nowym elementem infrastruktury technicznej w takim systemie na terenie powiatu będzińskiego będzie **elektrownia geotermalna**, która mogłaby korzystać z odkrytych już źródeł wód geotermalnych. Taką możliwość wykorzystania

[25] *Ustawa z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze* (t.j.: Dz.U. z 2017 r. poz. 2126, ze zm. – przyp. red.).

ciepła stwarzają okolice Siewierza i Sławkowa. W Polsce energia cieplna jest obecnie wykorzystywana w systemach ciepłowniczych, m.in. w Uniejowie. Dynamiczny rozwój technologii geotermalnej to szansa dla wytwarzania energii elektrycznej.

Zdaniem badaczy, m.in. Juliana Sokołowskiego, elektrownie geotermalne mają duży atut w porównaniu z innymi zakładami produkującymi energię elektryczną i cieplną, ponieważ posiadają stabilne i niezależne źródło wytwarzania energii oraz nie powodują zagrożeń środowiska naturalnego i jego zanieczyszczeń[26]. Elektrownia geotermalna przyczyniłaby się do rozwoju PRE w dziedzinie wytwarzania energii elektrycznej i cieplnej, a jednocześnie zmniejszyłby poziom zanieczyszczeń atmosferycznych na terenie powiatu będzińskiego.

Najlepszym przykładem wykorzystywania geotermii do produkcji energii cieplnej i elektrycznej w Polsce jest **ciepłownia w Pyrzycach**, która powstała w 1997 r. Temperatura źródeł geotermalnych w Pyrzycach **wynosi 64°C**[27].

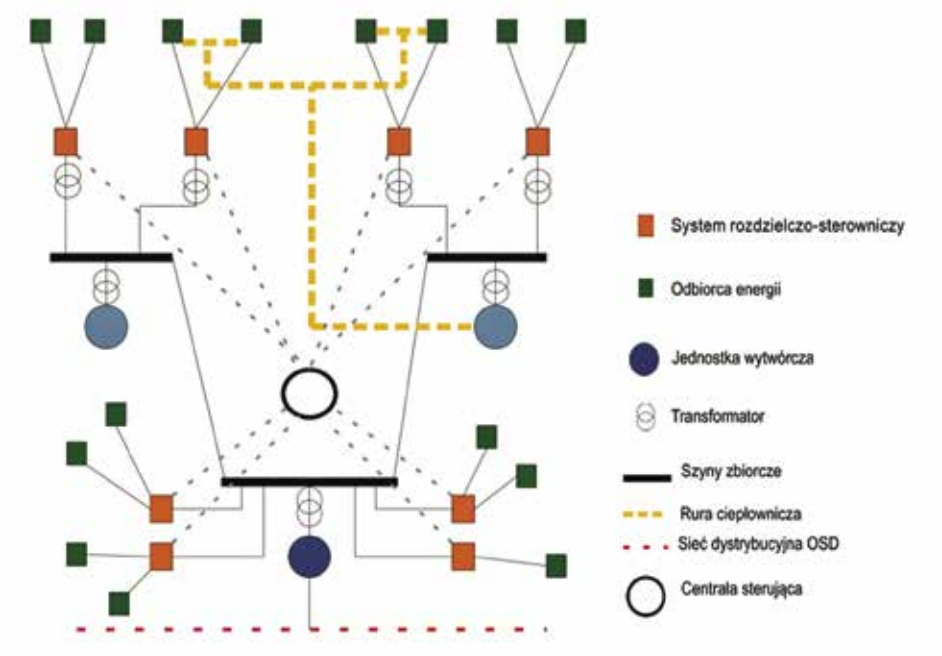
Zakład może się pochwalić posiadaniem **turbiny o mocy 40 MWh** oraz generatora, który wytwarza energię elektryczną. Gdyby zastosować takie rozwiązanie w powiecie będzińskim, gmina Siewierz stałaby się jednym z najważniejszych producentów energii w przyszłym PRE.

Dzięki temperaturze złóż geotermalnych znajdujących się na tym terenie, która wynosi 75°C, elektrownia Siewierz byłaby potencjalnie w stanie **produkować energię na poziomie 50 MWh**.

**Zdj. 2.** Ciepłownia geotermalna w Pyrzycach o mocy 40 MW.
Źródło: Geotermia Pyrzyce Sp. z. o.o.

[26] *Geotermia w Polsce*, Polska Geotermalna Asocjacja, http://www.pga.org.pl/geotermia-zasoby-polskie.html [dostęp: 23 XII 2016].
[27] Geotermia Przyrzyce, http://geotermia.inet.pl/informacje_ogolne.php [dostęp: 29 XII 2016].

Ważnym podsystemem bezpieczeństwa elektroenergetycznego powiatu jest **sieć przesyłowa.** W istniejącym obecnie systemie podstawą sieci przesyłowej jest KSE, co stwarza problem dla bezpieczeństwa energetycznego tego terenu. Jest to uwarunkowane brakiem alternatywnej sieci istotnej dla bezpieczeństwa energetycznego, która na poziomie lokalnym może mieć negatywny wpływ na funkcjonowanie władz w powiecie. Rozwiązaniem problemu byłoby zbudowanie **alternatywnego systemu przesyłu energii.** Według autora najlepszym rozwiązaniem technicznym sieci dystrybucji energii w przypadku przyszłej PRE są rozwiązania stosowane przez wspomnianą już Spółdzielnię Nasza Energia. System przesyłu energii wytworzonej przez tę Spółdzielnię składa się m.in. z Lokalnego Systemu Przesyłu, LPS (*Local Power System*), który jest w istocie instalacją odnawialnego źródła energii z przestrzennie rozmieszczonymi jednostkami wytwórczymi. Zasilanie odbywa się w formule *doublesupply*, bez konieczności wypowiadania dotychczasowej umowy sprzedaży energii. System rozdzielczo-sterowniczy sczytuje informacje o bieżącym zużyciu energii, obciążeniach i przepływach, kierując je następnie do centrali sterującej, gdzie są one analizowane. System może być też uzupełniany o inne źródła energii, np. źródła wiatrowe[28]. Lokalny System Przesyłu na poziomie gminy został przedstawiony na schemacie 3.




**Schemat 3.** Szczegółowy schemat mikrosystemu lokalnego zasilania na terenie jednej gminy.

Źródło: A. Rabiega, *Lokalny system zasilania odbiorców terenowych*, Warszawa 2014, s. 5.

[28] Zob. A. Rabiega, *Lokalny system zasilania odbiorców terenowych*, Warszawa 2014.

Widoczne na schemacie linie przerywane oznaczone kolorem żółtym to rury ciepła, natomiast kolorem czerwonym to sieci dystrybucyjne prądu. Oprócz sieci przesyłowej znajdują się tu trzy jednostki wytwórcze rozłożone na poszczególne elementy, połączone szynami zbiorczymi, będącymi (…) *zespołami przewodów sztywnych lub giętkich, do których przyłączone są elektrycznie poszczególne pola rozdzielcze*[29], oraz siedmioma transformatorami i rdzeniem lokalnego systemu zarządzającego przesyłem.

Rozwój lokalnych systemów przełożyłoby się na polepszenie warunków życia mieszkańców dzięki zmniejszeniu poziomu bezrobocia na terenie powiatu będzińskiego. Z punktu widzenia ekonomicznego byłoby to bardzo dobre rozwiązanie zarówno dla przedsiębiorców, jak i odbiorców. Zrównoważenie dostaw energii elektrycznej mogłoby pobudzić konkurencyjność między dużymi koncernami energetycznymi a lokalnymi zakładami, co spowodowałoby, że koszt wytworzonej energii byłby tańszy, gdyż tzw. PRE nie musiałoby płacić za emisję dwutlenku węgla. (…)

### 3.4. Wnioski

Nową koncepcję systemu bezpieczeństwa energetycznego powiatu można ująć w następujących punktach:

1. Budowa powiatowej jednostki organizacyjnej, nazwanej np. Powiatową Rezerwą Energetyczną, zmniejszy ryzyko utraty energii elektrycznej podczas zniszczenia elementów KSE lub ataku cybernetycznego na infrastrukturę techniczną, znajdującą się na terenie powiatu będzińskiego.
2. Dalszy rozwój energii odnawialnej w Polsce przyczyni się do budowy lokalnych systemów energetycznych, tzw. klastów energii.
3. Powstanie powiatowej jednostki organizacyjnej (PRE) oraz współpraca z Lasami Państwowymi w ramach Programu Operacyjnego Infrastruktura i Środowisko przyczyni się do ograniczenia zanieczyszczeń środowiska w powiecie będzińskim.
4. Rozwój klastrów energii na poziomie lokalnym zmniejszy koszty zużycia energii elektrycznej i cieplnej, a także umożliwi rozwój nowych firm w powiecie będzińskim, co obniży poziom bezrobocia na tym terenie.
5. Precyzyjne zapisy prawne ułatwią mieszkańcom powiatu jednoczesne podpisanie umowy dodatkowej z PRE, bez wypowiedzenia umowy głównemu operatorowi.
6. Brak możliwości magazynowania wytwarzanej energii powoduje, że KSE musi funkcjonować w sposób racjonalny i uwzględniający wszelkie wahania cenowe pojawiające się na rynku energii.
7. Ograniczenie kompetencji, odpowiedzialności i samorządności władz lokalnych w powiecie stanowi problem energetyki na poziomie lokalnym, ponieważ obecnie starosta jedynie zatwierdza plan zapotrzebowania na energię.

[29] W. Dołęga, *Stacje elektroenergetyczne*, Wrocław 2007, s. 11.

8. Zwiększenie działań proekologicznych przyczyni się do powstania ekologicznych przedsiębiorstw energetycznych, będzie to spowodowane wzrostem cen zużycia energii, który zmusi rynek energii do inwestycji w OZE.
9. Technologia geotermalna będzie w przyszłości jednym z dominujących obszarów energetyki, gdyż jest to stabilne i niezależne źródło wytwarzania energii, które nie powoduje zanieczyszczeń środowiska naturalnego.
10. Rozwój w Polsce systemów mikro na poziomie lokalnym rozpocznie proces transformacji energetycznej, czego przykładem jest (…) *niemiecki plan przejścia na gospodarkę niskowęglową, poparty skutecznymi instrumentami promocji odnawialnych źródeł energii, efektywności energetycznej i redukcji emisji gazów cieplarnianych*[30]. (…)

**Komentarz**

Wydaje się, że właściwym kierunkiem rozwoju systemu elektroenergetycznego powiatu jest budowa systemów mikro, gdzie wszystkie te elementy, skorelowane i współpracujące ze sobą, mogą rozwiązać obecne problemy systemu produkcji i przesyłu energii w powiecie będzińskim. W Polsce zastosowanie tej metody na skalę całego kraju jest przedmiotem dyskusji w kręgach naukowych ze względu na opłacalność i wpływ na bezpieczeństwo energetyczne Polski. Zastosowanie jej w skali mikro można zaobserwować na przykładzie działania Spółdzielni Nasza Energia w województwie lubelskim.

Mimo rozwoju nowych technologii i rozwoju elektromobilności, KSE nie przewiduje budowy systemów mikro. Jednak lokalne spółdzielnie energetyczne będą rozwijane na przestrzeni kolejnych lat, zwłaszcza że kraje wysoko rozwinięte stawiają na te systemy, które umożliwiają poszczególnym miejscowościom samowystarczalność.

**Bibliografia:**

Apanowicz J., *Zarys metodologii prac dyplomowych i magisterskich z organizacji i zarządzania*, Gdynia 1997, WSAiB.

*Aktualizacja Programu Ochrony Środowiska dla Powiatu Będzińskiego na lata 2008–2020*, Będzin 2008, Starostwo Powiatu Będzińskiego, AGOS-MEGES Sp. z o.o.

*Aktualizacja Strategii Rozwoju Powiatu Będzińskiego na lata 2009–2020*, Będzin 2014, Starostwo Powiatu Będzińskiego, IRT Wrocław.

Bartodziej G., Tomaszewski M., *Polityka energetyczna i bezpieczeństwo energetyczne,* Racibórz–Warszawa 2009, Nowa Energia.

Bogdańska B., *Mapa energii słonecznej,* Warszawa 2002, Zespół Aktynometrii Instytutu Meteorologii i Gospodarki Wodnej.

[30] K. Jankowska, *Spółdzielnie energetyczne – przykład niemieckiej energetyki obywatelskiej*, „Czysta Energia" 2014, nr 9; https://www.cire.pl/pliki/2/edukacja_jankowska_iii_wersja_poadpo_kor.pdf. [dostęp: 23 XII 2016].

Dołęga W., *Stacje elektroenergetyczne,* Wrocław 2007, Oficyna Wydawnicza Politechniki Wrocławskiej.

*Geotermia w Polsce*, Polska Geotermalna Asocjacja, http://www.pga.org.pl/geotermia-zasoby-polskie.html [dostęp: 23 XII 2016].

Gradziuk A. i in., *Co to jest bezpieczeństwo energetyczne państwa?*, Warszawa 2002, „Biuletyn PISM" 2002, nr 103, s. 705–708.

Jankowska K., *Spółdzielnie energetyczne – przykład niemieckiej energetyki obywatelskiej*, „Czysta Energia" 2014, nr 9; https://www.cire.pl/pliki/2/edukacja_jankowska_iii_wersja_poadpo_kor.pdf [dostęp: 23 XII 2016].

Jankowski A., *Aktualizacja założeń do planu zaopatrzenia w ciepło, energię elektryczną i paliwa gazowe na obszarze miasta Będzin*, Katowice–Będzin 2013, Energoekspert.

Kowalski J., Kozera J., *Mapa zagrożeń bezpieczeństwa energetycznego RP w sektorach ropy naftowej i gazu ziemnego*, „Bezpieczeństwo Narodowe" 2009, nr 1–2, s. 301–324.

Liedel K., Piasecka P.*, Wojna cybernetyczna – wyzwanie XXI wieku,* Warszawa 2011, BBN, s. 15–28.

*Nowy słownik języka polskiego*, Warszawa 2001, Wilga.

Phillip F., *Preventing blackouts: Building a smarter power grid*, http://www.scientificamerican.com/article/preventing-blackouts-power-grid/ [dostęp: 5 VIII 2016].

*Plan zapotrzebowania w ciepło, energię elektryczną i paliwa gazowe na obszarze miasta Będzin,* Katowice 2013, Urząd Miasta Będzin, Energoekspert, s. 22.

Rabiega A., *Lokalny system zasilania odbiorców terenowych*, Warszawa 2014, SNE.

Solarz J., Michailiuk B., Kołodziejczak M., *Energetyka jądrowa w aspekcie wyboru najlepszego źródła energii*, Warszawa 2014, AON.

Strzoda J., Skrzypiec M., *Czy jesteśmy przygotowani na blackout?*, Wrocław 2007, CIRE.

Szewczyk J., Gientka D., *Mapa gęstości ziemskiego strumienia cieplnego dla obszaru Polski*, Warszawa 2009, Państwowy Instytut Geologiczny.

Wrocławski M., *Lokalne obszary bilansowania*, „Energia Elektryczna" 2012, październik, Energia – Operator SA.

**Akty prawne:**

*Ustawa z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze* (t.j.: Dz.U. z 2017 r. poz. 2126, ze zm.).

*Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym* (t.j: Dz.U. z 2018 r. poz. 995, ze zm.).

*Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne* (t.j.: Dz.U. z 2018 r. poz. 755, ze zm.).

*Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym* (t.j.: Dz.U. z 2018 r. poz. 994, ze zm.).

**Źródła internetowe:**

http://mkuliczkowski.pl/static/pdf/slownik.pdf [dostęp: 12 XI 2016].

Iceland Energy, http://wayback.vefsafn.is/wayback/20041109123743/www.os.is/page/english/ [dostęp: 29 XII 2016].

Spółdzielnia Nasza Energia, http://nasza-energia.com/opis-projektu/ [dostęp: 17 XII 2016].

www.um.jelcz-laskowice.finn.pl [dostęp: 1 XI 2016].

**Słowa kluczowe**: Krajowy System Elektroenergetyczny, Powiatowa Rezerwa Energetyczna, bezpieczeństwo energetyczne, system przesyłu energii, infrastruktura techniczna.

**Keywords:** National Grid System, Local Energy Reserve, energy security, electricity transmission system, technical infrastructure.

**Aleksandra Tołczyk (Gołaś)**

# Specyfika i uwarunkowania procesu radykalizacji muzułmanów w zakładach karnych. Studium przypadku Wielkiej Brytanii[1]

## Wstęp

Unia Europejska zmaga się z problemem wzrastającego systematycznie zagrożenia terrorystycznego, zarówno islamskiego, jak i rodzimego, rozumianego jako akt przemocy wymierzony głównie w społeczeństwa państw zachodnich, w których terroryści urodzili się lub wychowali. Po zamachach z 11 września 2001 r. w Stanach Zjednoczonych i serii ataków przeprowadzanych po dziś dzień na terenie Europy, masowo zaczęły pojawiać się na rynku wydawniczym publikacje na temat terroryzmu i radykalizacji. Zachodni decydenci polityczni uznali, że skrajne interpretacje religii są głównym bodźcem współczesnego ekstremizmu. Stany Zjednoczone, Australia, Wielka Brytania oraz inne państwa Europy Zachodniej skupiają się w swoich strategiach walki z terroryzmem na społecznościach muzułmańskich, próbując zrozumieć przyczyny ich podatności na radykalizację i adaptację ekstremistycznej ideologii. Miejscami stwarzającymi podatny grunt dla rozwoju skrajnych poglądów i zachowań, określanymi jako „uniwersytety" lub „inkubatory" terroryzmu, są zakłady karne. To tutaj drobny przestępca niemający nigdy wcześniej związku z działalnością terrorystyczną przyjmuje często ekstremalny system poglądów i wierzeń, za które jest gotowy zabijać innych ludzi. Warto też zaznaczyć, że ideologia współczesnego radykalnego islamu zrodziła się i rozwijała właśnie w więzieniach.

Radykalizacja, do której dochodzi w więzieniach, jej przebieg i uwarunkowania zależą pod wieloma względami od specyfiki i podejścia każdego państwa do tego problemu. W Wielkiej Brytanii w oficjalnych strategiach rządowych dotyczących walki z terroryzmem i ekstremizmem akcentuje się konieczność zwrócenia szczególnej uwagi na zakłady karne i zagrożenia, jakie niesie za sobą radykalizacja. Odnotowano również znaczny wzrost liczby muzułmanów w populacji więziennej Anglii i Walii, a także wiele przypadków konwersji na islam.

Opracowanie ma na celu odpowiedź na pytanie: jakie są przyczyny kształtujące specyfikę zakładu karnego jako miejsca sprzyjającego radykalizacji muzułmanów? Autorka podjęła też próbę zidentyfikowania charakteru tego problemu, odwołując się do

[1] Fragment pracy magisterskiej pt. *Specyfika i uwarunkowania procesu radykalizacji muzułmanów w zakładach karnych. Studium przypadków* (Uniwersytet Warszawski, Wydział Nauk Politycznych i Studiów Międzynarodowych). Praca została wyróżniona w siódmej edycji *Ogólnopolskiego konkursu Szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa* (edycja 2016/2017).

konkretnego przypadku, a mianowicie do aktualnej sytuacji w Wielkiej Brytanii. Hipotezą, którą autorka postara się zweryfikować, jest twierdzenie, że niewłaściwe zarządzanie systemem penitencjarnym połączone z doświadczeniami indywidualnymi i społecznymi muzułmanów sprzyjają szerzeniu się fanatyzmu w więzieniach. Treść opracowania powstała na podstawie oficjalnych statystyk, licznych raportów (m.in. przygotowanych przez RAND Corporation, Brytyjską Radę Muzułmańską, Królewski Inspektorat Więziennictwa), analiz poszczególnych przypadków radykalizacji i literatury fachowej.

## 1. Ujęcie teoretyczne i funkcjonalne badań nad radykalizacją

Ataki z 11 września 2001 r. na World Trade Center oraz obiekty Pentagonu miały podstawowe znaczenie w rozwoju badań nad szeroko rozumianym problemem współczesnego terroryzmu. Te wydarzenia, mające zdecydowanie bezprecedensowy charakter, doprowadziły do przeobrażenia sposobu postrzegania bezpieczeństwa w XXI wieku, wyrażonego w Stanach Zjednoczonych terminem „wojna z terroryzmem”[2]. Początek tego stulecia to również seria ataków terrorystycznych w Europie, określanych przez brytyjskich badaczy pojęciem Europlot. Rozumie się pod nim: ataki z 11 marca 2004 r. w Madrycie i z 7 lipca 2005 r. w Londynie, zabójstwo holenderskiego reżysera Theo Van Gogha 2 listopada 2004 r., strzelaninę na lotnisku we Frankfurcie 2 marca 2011 r. (jej celem byli amerykańscy żołnierze) i wiele innych zdarzeń będących elementem wykrytego w 2010 r. planu Al-Kaidy[3].

Wszystkie te przypadki doprowadziły do intensyfikacji współpracy międzynarodowej nie tylko związanej z przeciwdziałaniem i zwalczaniem terroryzmu. Coraz większe zainteresowanie przejawiano problemem radykalizacji i jej źródeł, zwłaszcza tych, które skłaniały do przeprowadzania aktów przemocy. Warto w tym miejscu zaznaczyć, że zamachowcy odpowiedzialni za ataki z 11 września 2001 r. mieszkali i studiowali w Niemczech i właśnie tam się zradykalizowali, tworząc tak zwaną komórkę hamburską (ang. *Hamburg cell*). Mohamed Atta, lider grupy, a zarazem jeden z pilotów-zamachowców, w chwili przyjazdu do Niemiec w 1992 r. był odbierany jako osoba religijna, ale nie fanatyk religijny[4]. Jak zauważa Olivier Roy, terrorystów w Europie Zachodniej łączą zazwyczaj podobne wzorce zachowania: są obywatelami europejskiego kraju, „normalnymi” zachodnimi nastolatkami, którzy nie uzewnętrzniają swoich przekonań i praktyk religijnych[5]. Zaczęto więc stawiać pytanie, dlaczego młodzi ludzie wychowani w krajach zachodnich radykalizują swoje poglądy i są gotowi zabijać innych? To pytanie przybrało na sile wraz z początkiem syryjskiej wojny domowej i napływem do Syrii bojowników z europejskimi paszportami, a także z kolejną falą zamachów w Europie Zachodniej, inspirowanych lub przeprowadzanych przez Państwo Islamskie (ISIS).

[2] Zob. szerzej na temat wojny George’a Busha z terroryzmem: *The Bush doctrine and the war on terrorism: global responses*, *global consequences*, M. Buckley, R. Singh (red.), London–New York 2006.

[3] Zob. A. Rabasa, Ch. Benard, *Eurojihad. Patterns of Islamist Radicalization and Terrorism in Europe*, New York 2015, s. IX–X.

[4] Zob. szerzej *The 9/11 Commission Report*, National Commission on Terrorist Attacks, http://govinfo.library.unt.edu/911/report/911Re port.pdf, s. 145–174 [dostęp: 27 XII 2016].

[5] O. Roy, *Islamic Terrorist Radicalisation in Europe*, w: *European Islam – Challenges for Society and Public Policy*, S. Amghar, A. Boubekeur, M. Emerson (red.), Brussels 2007, s. 52–60.

Warto zwrócić uwagę na to, że choć fanatyzm nie jest nowym fenomenem, w debacie międzynarodowej wciąż nie osiągnięto porozumienia co do kwestii definicyjnych. Środowiska akademickie, politycy oraz przedstawiciele organizacji odpowiadających za bezpieczeństwo zgadzają się, że radykalizacja w świecie zachodnim jest problemem, jednak nie mogą wspólnie jednoznacznie określić, co właściwie oznacza ten niezwykle popularny w ostatnich latach termin. Uniwersalna definicja ułatwiłaby tworzenie zarówno programów przeciwdziałania terroryzmowi, jak i deradykalizacji, a także wpłynęłaby na jakość i skuteczność współpracy międzynarodowej w omawianym obszarze. W piśmiennictwie, szczególnie anglosaskim, widoczny jest bałagan terminologiczny, przejawiający się stosowaniem przez autorów terminów: „radykalizacja" (ang. *radicalisation*) oraz „radykalizacja do przemocy" (ang. *violent radicalisation*). Oba terminy są zazwyczaj definiowane podobnie, jednak to drugie jest zdecydowanie węższe i utożsamia proces radykalizacji z zastosowaniem różnych form agresji, podobnie jak termin „socjalizacja do przemocy" (ang. *socialisation into violence*). Rozróżnienie tych pojęć jest pod wieloma względami mylące i mało praktyczne. Nie wszyscy badacze identyfikują radykalizację wyłącznie ze stosowaniem przemocy, podkreślając jej dwojaką naturę objawiającą się również przyjmowaniem skrajnych poglądów, przekonań, uczuć. Aleksandra Zięba i Damian Szlachter rozumieją radykalizację jako socjalizację do ekstremizmu, która manifestuje się (…) *w negacji istniejącego systemu/porządku politycznego przez użycie lub groźbę użycia przemocy politycznej (terroryzm)*[6]. Podkreślają jednak, że radykalizacja nie musi prowadzić do zaangażowania się w działalność terrorystyczną. W literaturze przedmiotu przedstawia się również radykalizację jako (…) *proces przyjmowania ekstremistycznego systemu wartości, połączonego z wyrażaniem aprobaty, wsparcia bądź wykorzystaniem przemocy i zastraszenia jako sposobu osiągania zmian w społeczeństwie*[7]. Dlatego też w niniejszej pracy stosuje się termin „radykalizacja" jako pewien czynnik ryzyka mogący, choć niekoniecznie, prowadzić do aktu przemocy politycznej. W tym podejściu należy wyróżnić dwa wymiary radykalizacji: postaw oraz zachowań, które choć są ściśle ze sobą powiązanie, to nie muszą od siebie zależeć. A zatem skrajne postawy nie muszą prowadzić do przemocy i odwrotnie – dołączenie do ekstremistycznej grupy nie musi być motywowane radykalnymi celami (tylko na przykład chęcią osiągnięcia jakichś korzyści). (…)

## 2. Proces radykalizacji w warunkach izolacji więziennej

Zjawisko radykalizacji w więzieniach nie jest wytworem ostatnich lat czy nawet dekad, a mimo to jego fenomen wciąż pozostaje obszarem w niewielkim stopniu zbadanym empirycznie. Zdaniem Andrew Silke dziwne jest, że po 11 września 2001 r. znacznemu,

[6] A. Zięba, D. Szlachter, *Zwalczanie terroryzmu – walka z radykalizacją postaw i werbowaniem terrorystów na obszarze Unii Europejskiej. Studium przypadku społeczności muzułmańskich,* w: *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego. Uwarunkowania – realizacja – wyzwania w drugiej dekadzie XXI wieku*, W. Fehler, K. Marczuk (red.), Warszawa 2015, s. 145–146.

[7] *Radykalizacja poglądów religijnych w społecznościach muzułmańskich wybranych państw Unii Europejskiej: Polska – Holandia – Wielka Brytania*, D. Szlachter, P. Potejko i inni (red.), Szczytno 2011, s. 7.

a wręcz przytłaczającemu, wzrostowi literatury dotyczącej terroryzmu, nie towarzyszył rozwój zainteresowania badaczy tematyką penitencjarną[8]. Zakłady karne mogą pełnić wiele funkcji wspomagających działanie organizacji terrorystycznej. Wśród nich warto wskazać: rekrutację nowych członków wśród współwięźniów, przygotowywanie ataku terrorystycznego, który zostanie popełniony po zwolnieniu z więzienia, a nawet udzielanie wsparcia grupie, pomimo pozostawania w izolacji od jej członków. Silke wysuwa tezę, że to, co dzieje się za więziennymi kratami, było przez wiele lat ignorowane i lekceważone, zauważa również, że ostatecznie większość terrorystów czy ekstremistów kończy w więzieniach, dlatego tym bardziej zaskakuje ubogość publikacji w tej dziedzinie.

Departament Sprawiedliwości Stanów Zjednoczonych definiuje radykalizację w więzieniach (ang. *prison radicalization*) jako proces, w którym więźniowie, początkowo nieplanujący ataku terrorystycznego ani do tego nie zachęcani, przyjmują skrajne poglądy, w tym przekonanie, że należy zastosować przemoc dla osiągnięcia celów politycznych lub religijnych[9]. Odseparowanie od świata zewnętrznego, negatywne skutki kary pozbawiania wolności i przystosowywania się do nowego sposobu życia połączone z dysfunkcjami emocjonalnymi i społecznymi jednostki zaburzają percepcję rzeczywistości, ułatwiając przyswajanie radykalnych treści i uczuć.

Dyskusja nad problemem radykalizacji muzułmanów w zakładach karnych na terenie Unii Europejskiej i Stanów Zjednoczonych pojawiała się po wydarzeniach z 11 września 2001 r. i w związku z działalnością Al-Kaidy, a następnie wraz z zamachami z 11 marca 2004 r. w Madrycie. Obecnie podkreśla się, że nie ma wątpliwości co do tego, że więzienia stwarzają podatny grunt dla radykalizacji muzułmanów i rekrutacji do organizacji terrorystycznych, co sprawia, że zwykły kryminalista popełniający do tej pory drobne przestępstwa staje się dżihadystą. Przebieg radykalizacji, jej przyczyny i uwarunkowania są specyficzną cechą każdego państwa, na którą wpływają: ramy prawne, sposób organizacji więzień, liczebność ekstremistów i terrorystów w zakładach karnych oraz podejście danego państwa do walki z radykalizacją. Niezależnie od tych uwarunkowań można jednak wyróżnić uniwersalne czynniki przyczyniające się do radykalizacji więziennej, takie jak oddziaływanie środowiska więziennego, podatność więźniów oraz rozwój radykalnego islamu. W 2006 r. dyrektor Federalnego Biura Śledczego Robert Mueller stwierdził, że więźniowie mogą przyjmować fanatyczną wizję islamu, ponieważ usprawiedliwia on skłonność do stosowania przemocy[10]. Więźniowie ci stanowią szczególnie duże zagrożenie ze względu na swoją kryminalną przeszłość i wcześniejsze przejawy agresji. Amedy Coulibaly, zamachowiec z marketu koszernego w Paryżu, stwierdził: (…) *więzienie jest najlepszą pieprzoną szkołą przestępczości*[11].

[8] Zob. A. Silke, *Terrorists, extremists and prison. An introduction to the critical issues*, w: *Prisons, Terrorism and Extremism. Critical Issues in Management, Radicalization and Reform*, A. Silke (red.), New York 2014, s. 5.

[9] *A Review of the Federal Bureau of Prisons' Selection of Muslim Religious Services Providers*, U.S. Department of Justice, 2004, https://oig.justice.gov/special/0404/final.pdf, s. 6 [dostęp: 6 IV 2017].

[10] R. Mueller, *Przemowa z Cleveland z 2006 r.*, https://archives.fbi.gov/archives /news/speeches/the-threat-of-homegrown-terrorism [dostęp: 4 V 2017].

[11] F. Gaub, J. Lisiecka, *The crime-terrorism nexus*, http://www.iss.europa.eu/publications/detail/article/the-crime-terrorism-nexus/, s. 2 [dostęp: 5 V 2017].

Dodał również, że w jednym miejscu mógł poznać Basków, muzułmanów, morderców, drobnych dealerów narkotyków, mógł więc uczyć się na podstawie gromadzonych przez lata doświadczeń innych osób. Zakłady karne mają znaczenie dla współczesnego terroryzmu islamskiego z trzech zasadniczych powodów:

1) są miejscami, gdzie ekstremiści mogą znaleźć wielu młodych, rozczarowanych życiem mężczyzn z kryminalną przeszłością, otwartych na poznawanie świata na nowo, gotowych na przyjęcie ekstremistycznych treści, a tym samym i na rekrutację,
2) umożliwiają współpracę znajdującym się tam terrorystom i zwykłym kryminalistom,
3) proponuje się tam osobom skazanym, które mają małą szansę na powrót i ponowną integrację ze społeczeństwem, aby po opuszczeniu więzienia dołączyły do ekstremistycznej grupy, co nadaje ich życiu sens i stwarza poczucie bycia potrzebnym.

Środowisko więzienne w szczególny sposób sprawia, że osoby przebywające w więzieniu są bardziej narażone na wpływ, a tym samym na odkrywanie i przyswajanie nowych systemów przekonań, uczuć, idei. Tak więc osoba znajdująca się w trudnej dla niej sytuacji pozbawienia wolności, borykająca się z problemami egzystencjalnymi i odseparowaniem od społeczeństwa, która nigdy wcześniej nie była zaangażowana w przemoc polityczną, staje się podatna na radykalizację, a nawet rekrutację do organizacji terrorystycznej. Więzienia są miejscami, gdzie nowe osoby są poddawane presji psychicznej i doświadczają otwarcia poznawczego – chęci i potrzeby identyfikacji z nowymi wierzeniami, uczuciami i grupami społecznymi. W 1961 r. w klasycznej już pracy *Asylums* Erving Goffman wprowadził pojęcie i n s t y t u c j a  t o t a l n a służące określeniu organizacji (instytucji) społecznych, które można wyróżnić od pozostałych ze względu na fizyczną izolację od świata zewnętrznego i tworzenie ograniczeń dla jej członków[12]. Autor podzielił te instytucje na pięć grup, jedna z nich (…) *obejmuje ten typ instytucji totalnych, których zadaniem jest ochrona społeczeństwa przed szkodzeniem mu w sposób świadomy. W tym przypadku nie dobro osób poddanych ograniczeniom jest bezpośrednim celem działania instytucji*[13]. Jako przykład Goffman wskazuje zakłady karne, będące specyficzną formą systemu społecznego, w którym pozbawia wolności, kontroluje i izoluje więźniów w imieniu społeczeństwa. Zrozumienie procesu radykalizacji w zakładach karnych wymaga scharakteryzowania wpływu tej szczególnej i unikalnej instytucji na osoby w niej przebywające.

Warto w tym miejscu zwrócić uwagę na zjawisko podatności w społeczeństwie, które wydaje się mieć dość istotne znaczenie w analizie procesu radykalizacji w warunkach izolacji więziennej. Zdaniem Wilheminy Wosińskiej: (…) *wpłynąć na innych ludzi oznacza spowodować, by działali oni/lub myśleli tak, jak życzy sobie jednostka (lub grupa) na nich oddziałująca*[14]. Z kolei Robert Cialdini wyjaśnia: (…) *większość członków naszej kultury wykształca w sobie w trakcie życia pewien zbiór czynników wyzwalających automatyczne uleganie wpływowi społecznemu, to znaczy zbiór pewnych*

[12] Zob. E. Goffman, *Asylums. Essays on the Social Situation of Mental Patients and Other Inmates*, Garden City 1961.
[13] Tenże, *Charakterystyka instytucji totalnych*, w: *Elementy teorii socjologicznych*, W. Derczyński, A. Jasińska-Kania, J. Szacki (red.), Warszawa 1973, s. 150.
[14] W. Wosińska, *Psychologia życia społecznego*, Gdańsk 2004, s. 982.

*cech czy informacji, których pojawienie się w otoczeniu jest sygnałem, że poddanie się wpływowi będzie dla człowieka dobroczynne i korzystne*[15]. To zjawisko znajduje oczywiście odzwierciedlenie nie tylko w normalnych warunkach społecznych, lecz także dotyczy sytuacji więziennej. Jednak, jak słusznie zauważa Henryk Machel, zakład karny jest z natury aspołeczny[16]. Argumentuje on swoją tezę w następujący sposób: (…) *społeczność więźniów pozostaje w stałej styczności osobistej ze sobą i mimo selekcji klasyfikacyjnej, wpływa na siebie wzajemnie na poziomie swoich możliwości* ***intelektualnych, moralnych, kulturowych i predyspozycji osobistych***[17]. *Ten wzajemny wpływ jest przeważnie ujemny*[18]. Dołączenie do nieformalnej grupy funkcjonującej w więziennych murach może zaspokoić potrzebę przynależności i wpłynąć na poczucie bezpieczeństwa jednostki, jednak kontakty z tą grupą mogą być również bodźcem do zainicjowania procesu radykalizacji osoby o pewnych predyspozycjach. Uleganie wpływowi następuje więc w sposób automatyczny, uproszczony i bezrefleksyjny. (…)

### 3. Problemy organizacyjne więzień a radykalizacja

Więzienia stały się obecnie obiektem debaty dotyczącej nowych rozwiązań organizacyjnych, gdyż w swoim dotychczasowym kształcie zostały uznane za sprzyjające radykalizacji[19]. Szczególnie na zachodzie Europy, w takich krajach jak Wielka Brytania, Francja oraz Belgia, podkreśla się konieczność reformy systemu penitencjarnego i wskazuje na negatywne tendencje obserwowane w więziennictwie[20]. W 2016 r. Komisja Europejska zapowiedziała pomoc dla państw członkowskich UE w zwalczaniu radykalizacji prowadzącej do terroryzmu. Współpraca w przeciwdziałaniu radykalizacji w więzieniach polegałaby na wymianie doświadczeń w celu stworzenia mechanizmów i programów zapobiegających problemowi, a także wspierających rehabilitację i resocjalizację[21]. Sposób zarządzania zakładem karnym, jego organizacja oraz zachowanie porządku i wynikającego z niego podziału zadań i obowiązków może istotnie wpłynąć na radykalizację osób w nim przebywających. Jak już wcześniej wspomniano, pobyt w zakładzie karnym negatywnie wpływa na psychikę człowieka i może prowadzić do radykalizacji lub dalszej kryminalizacji zachowań. Więzień często odczuwa bezradność i niemoc, przez co

[15] R. Cialdini, *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańsk 1994, s. 30–31.

[16] H. Machel, *Resocjalizacja penitencjarna: trzy uwarunkowania procesu*, „Resocjalizacja Polska" 2011, nr 2, s. 98.

[17] Wszystkie wyróżnienia pochodzą od autorki (przyp. red.).

[18] H. Machel, *Resocjalizacja penitencjarna*...

[19] Państwem zachodnim, które już na początku lat 90. XX w. opracowało programy monitorowania więzień, zwłaszcza w odniesieniu do radykalizmu islamskiego, była Francja. Powstałe wówczas praktyki przejęły inne państwa, większość z nich jest stosowana do dziś. Zob. szerzej: F. Khosrokhavar, *Radicalization in Prison: The French Case*, „Politics, Religion & Ideology" 2013, nr 14, s. 284–305.

[20] Przeglądu systemu więziennictwa dokonano również we Włoszech, gdzie mimo mniejszego zagrożenia radykalizacją w zakładach karnych w porównaniu z innymi państwami europejskimi, podkreśla się konieczność ciągłej analizy zjawiska i wyklucza się jego bagatelizowanie. Por. A. Cinelli, *Italy aims to combat radicalisation in jails, deport more illegal migrants*, http://uk.reuters.com/article/uk-europe-migrants-italy-prison-idUKKBN14P209 [dostęp: 5 IV 2017].

[21] Zob. szerzej *UE podejmuje bardziej zdecydowane działania, aby zwalczać radykalizację postaw prowadzącą do terroryzmu*, Komisja Europejska – komunikat prasowy, http://europa.eu/rapid/press-release_IP-16-2177_pl.htm [dostęp: 4 IV 2017].

ma poczucie, że to on stał się ofiarą (wiktymizacja). Sandra Musioł wśród przyczyn niezadowolenia z efektów resocjalizacji więziennej wymienia:

1) brak lub niedostatek środków, metod i technik oddziaływania resocjalizacyjnego,
2) wadliwe koncepcje organizacyjne zakładów oraz sposobów zarządzania i kierowania nimi,
3) niedoskonała społeczna organizacja placówki,
4) dezintegracja pionów służb zakładowych,
5) stosowanie autorytarnego stylu zarządzania,
6) stosowanie izolacyjno-represyjnej funkcji kary[22].

Przez długi czas nauki penitencjarne obejmowały swoim zainteresowaniem wyłącznie osoby skazane. Współcześnie nastąpił wzrost świadomości konieczności przebadania również personelu więziennego. Administracja zakładu karnego może – nawet w sposób nieświadomy – wspomagać proces radykalizacji, między innymi przez stosowanie środków nieproporcjonalnych do zachowań. Użycie siły i środków przymusu powinno być współmierne do zagrożeń i zakłóceń bezpieczeństwa czy porządku w danym ośrodku, w odwrotnym przypadku może zostać zakłócona relacja zaufania pomiędzy personelem a osadzonymi. Zarządzanie zakładem karnym polegające na milczącym zezwoleniu na występowanie na terenie więzienia takich zjawisk, jak przemoc, rasizm, islamofobia czy dyskryminacja, może spowodować u osób, których te urazy i przykrości dotykają, zainicjowanie procesu radykalizacji.

Stabilnie funkcjonujące więzienie wymaga przestrzeni dla osadzonych oraz zapewnienia im odpowiednich warunków mieszkaniowych. Z trudnym do rozwiązania problemem przeludnienia w więzieniach boryka się współcześnie większość państw Unii Europejskiej. Nagromadzenie zbyt dużej liczby osób w jednym miejscu utrudnia proces nadzorowania i gromadzenia informacji o osadzonych, a tym samym opóźnia podjęcie działania w przypadku wystąpienia ryzyka radykalizacji. Również przeludnienie nie sprzyja skuteczności resocjalizacji, a brak prywatności z nim związany może powodować problemy ze zdrowiem psychicznym lub nasilać już istniejące, może też zwiększać ryzyko występowania przemocy, samookaleczeń i samobójstw[23]. Ten problem narasta w przypadku niewystarczającej liczby personelu więziennego. Należy podkreślić, że przepełnienie więzień jest wynikiem złej polityki karnej, a nie rosnącego wskaźnika przestępczości. Pod koniec 2016 r. we Francji zapowiedziano budowę 33 nowych więzień oraz modernizację starych, co ma być elementem walki z radykalizacją muzułmanów. Francuskie zakłady karne są jednymi z najbardziej przepełnionych na świecie. Ówczesny premier alarmował: *Sytuacja jest krytyczna, zwłaszcza w więzieniach dla osób z wyrokami do dwóch lat, gdzie*

[22] S. Musioł, *Negatywne aspekty kary pozbawienia wolności*, https://ms.gov.pl/pl/probacja/2013/download,2691,9.html [dostęp: 2 V 2017].
[23] Zob. *Overcrowding*, Penal Reform International, https://www.penalreform.org/ priorities/prison-conditions/key-facts/overcrowding/ [dostęp: 13 V 2017].

*przepełnienie wynosi 140 procent*[24]. Co ciekawe, we Francji zauważono, że radykalizacja dotyczy również strażników więziennych, choć to zjawisko występuje w niewielkim stopniu. Mimo że nie nawoływali oni do stosowania przemocy, wprowadzono kroki w postaci zwolnienia z pracy (nieoficjalnie mówi się o 10–30 takich przypadkach na 27 tys. strażników zatrudnionych w całym kraju)[25].

Muzułmanie przebywający w więzieniach zazwyczaj niewiele wiedzą o islamie, mają również braki w edukacji. Dlatego ich rozumienie religii jest oparte głównie na informacjach zebranych w więzieniu. Istotnym problemem w Europie pozostaje więc duża liczba muzułmańskich więźniów, przy niewielkiej liczbie imamów więziennych. Imam Husamuddin Meyer, świadczący posługę duchową dla muzułmańskich więźniów w zakładach karnych w niemieckiej Hesji, zaznacza, że niejednokrotnie usłyszał pytania napawające go niepokojem: *„Panie imam, kto się nie modli, tego trzeba zabić, czyż nie?" lub „Państwo Islamskie to przecież prawdziwe państwo, takie samo jak inne?"*[26]. Według niego imamowie mogliby odegrać istotną rolę w przeciwdziałaniu radykalizacji w więzieniach i dodaje: (…) *mogą oni prowadzić rzeczową dyskusję z więźniami muzułmanami oraz służyć im poradą duszpasterską* oraz: (...) *kiedy imam mówi wierzącemu muzułmanowi, że postępuje niewłaściwie, to jego słowa wiele znaczą*[27]. Imam Meyer pracuje jednak tylko 15 godzin tygodniowo, świadcząc posługę dla ponad stu osadzonym. Dla porównania, katoliccy księża pracują w niemieckich więzieniach zazwyczaj na pełny etat, a na każdego przypada zdecydowanie niższa liczba osadzonych. Podobnie problem wygląda w innych krajach Europy. We Francji w 2008 r. w więzieniach w pobliżu Paryża na 20 tys. muzułmanów przypadało tylko ośmiu imamów[28].

Przykładem, w jaki sposób ingerencja państwa i problemy z zarządzaniem i organizacją zakładami karnymi mogą przyczynić się do wzrostu zagrożenia radykalizacją, może być sytuacja, do której doszło w Belgii w 2016 r.[29] W związku z przygotowywanymi wówczas przez belgijski rząd zmianami w warunkach zatrudnienia pracowników więziennictwa (oszczędności w kosztach zatrudnienia i wprowadzenie nieelastycznych godzin pracy) w więzieniach na terenie kraju wybuchły strajki, a znaczna część osób zrezygnowała z pracy, co spowodowało drastyczny wzrost liczby więźniów przypadających na jednego strażnika. W wyniku strajku obniżył się standard życia osadzonych, zwłaszcza przestrzeganie norm sanitarnych. Zaniepokojenie sytuacją wyraził komisarz ds. praw człowieka Rady Europy Nils Muiżnieks, który zauważył, że więźniowie od tygodni nie

[24] Cyt. za: *Powstaną 33 nowe więzienia. Między innymi w celu walki z islamską radykalizacją*, RMF24.pl, http://www.rmf24.pl/fakty/swiat/news-powstana-33-nowe-wiezienia-miedzy-innymi-w-celu-walki-z-isla,-nId,2286604 [dostęp: 13 V 2017].

[25] Tamże.

[26] *Więzienia są wylęgarnią radykałów*, onet.pl, http://wiadomosci.onet.pl/swiat/niemcy-wiezienia-sa-wylegarnia-radykalow/vc4df6 [dostęp: 14 V 2017].

[27] Tamże.

[28] A. Pargeret, *The New Frontiers of Jihad: Radical Islam In Europe*, Philadelphia 2008, s. 184.

[29] Zob. *Strażnicy więzienni strajkują, wysłano wojsko*, www.TVN24.pl, http://www.tvn24.pl/ wiadomosci-ze-swiata,2/belgia-strajk-straznikow-wieziennych-zolnierze-zastepuja-straznikow,642313.html [dostęp: 3 V 2017].

opuszczali swoich cel, nie mieli dostępu do podstawowych obiektów sanitarnych, do leków i służby zdrowia, a także nie mieli możliwości kontaktowania się z adwokatami i rodziną[30]. Pojawiły się wówczas obawy, że opisana sytuacja, wynikająca m.in. z niedoboru pracowników, uniemożliwi skuteczną resocjalizację, tym samym wzrośnie również prawdopodobieństwo radykalizacji postaw i zachowań wśród więźniów.

**4. Islam w zakładach karnych: religia, gangi i radykalizacja**

Zaangażowanie religijne więźniów jest zjawiskiem złożonym, motywowanym czynnikami społecznymi i psychologicznymi. Uważa się, że zakłady karne stanowią podatny grunt dla radykalizacji muzułmanów. Więzienia określa się również jako „inkubatory" dla dżihadystów, ponieważ dochodzi w nich do tworzenia sieci powiązań pomiędzy drobnymi przestępcami a osobami próbującymi przekazać ekstremistyczną ideologię dżihadu, które przypominają komórki organizacji terrorystycznej. Owemu łączeniu sieciowemu sprzyjają także złe warunki panujące w więzieniu (np. wspomniane przeludnienie) oraz braki perspektyw po zwolnieniu z niego. W polskiej literaturze przedmiotu nieformalne grupy funkcjonujące w obrębie zakładów karnych (subkultury lub inaczej – podkultury) nazywa się drugim życiem więzienia. Przez to pojęcie rozumie się: (…) *pozaregulaminowe formy postępowania wychowanków zakładów poprawczych związane z wartościami narzuconymi nie przez reguły formalne, lecz wyznaczone w procesie interakcji między wychowankami zakładu a przyjętymi oficjalnie zasadami funkcjonowania instytucji, jej celów i porządku*[31]. Cherif Kouachi, odpowiedzialny za zamach na redakcję francuskiego tygodnika satyrycznego „Charlie Hebdo" w 2007 r., podczas pobytu w największym więzieniu w Europie poznał Amedy'ego Coulibaly'ego. Ich mentorem był Djamel Baghdal, rekrutujący nowych członków do Al-Kaidy. Grupa kontynuowała spotkania po zakończeniu odbywania kary, była również zamieszana w organizację ucieczki z więzienia innego dżihadysty.

Muzułmanie bardzo często stosują przymus i zastraszenie w celu wprowadzenia norm islamu do codziennego życia w zakładzie karnym (np. wymuszanie porannych i wieczornych modlitw). Znęcanie się nad słabszymi współwięźniami i zmuszanie do zmiany wyznania na islam stało się również podstawą twierdzenia, że wyznawcy radykalnego islamu zaczęli w więzieniu tworzyć nie tylko małe grupy czy podkultury, ale całe gangi oparte na religii i kulturze islamu. Mają one zazwyczaj swojego lidera, strukturę hierarchiczną, styl kierowania, sposób komunikacji i zbiorową tożsamość. W Hiszpanii ogólna populacja więźniów w 2015 r. wynosiła 71 tys. osób, z czego ponad 7 tys. pochodziło z Afryki Północnej[32]. Często mówią oni jednym językiem, nierzadko pochodzą z Maroka, a nawet z tego samego miasta. Sami wybierają swojego imama, którym zostaje osoba najlepiej znająca *Koran*. Mimo że prawie połowa populacji

[30] Zob. *Komisarz Rady Europy krytykuje belgijskie więzienia*, TVN24.pl, http://www.tvn24.pl/wiadomosci-ze-swiata,2/belgia-strajk-straznikow-wieziennych-zolnierze-zastepuja-straznikow,642313.html [dostęp: 3 V 2017].
[31] M. Pyska, *Drugie życie więzienia*, www.wspia.eu/file/21412/16-PYSKA.pdf [dostęp: 5 V 2017].
[32] A. Rabasa, Ch. Benard, *Eurojihad. Patterns of Islamist*…, s. 112.

muzułmanów w hiszpańskich więzieniach to Marokańczycy, ich liderem zostaje zazwyczaj Algierczyk. Przypuszcza się, że dzieje się tak dlatego, że Algierczycy cieszą się uznaniem i prestiżem ze względu na największe doświadczenie w dżihadzie. (...)

Zaznacza się, że nie ma związku między terroryzmem a pogłębianiem wiary przez muzułmanów bądź zmianą religii przez więźniów na islam, przy jednoczesnym podkreśleniu istotnego znaczenia religii w codziennym życiu więziennym. Jedną z głównych przyczyn powrotu do islamu bądź zmiany wyznania na islam jest zdecydowanie strach i próba przetrwania w niesprzyjającym i wrogo nastawionym środowisku więziennym. Dla innych nawrócenie jest wyznacznikiem początku nowego życia. Islam nadaje sens życiu, zapewnia oczyszczenie i rehabilitację. W tym miejscu należy rozróżnić religijność od radykalizacji. Niektórzy powracają do islamu bądź zmieniają wyznanie szczerze, z powodów osobistych, niemających związku z radykalnymi i ekstremistycznymi poglądami. Mimo że islam (szczególnie salafizm[33]) stał się obecnie najpopularniejszą religią w Unii Europejskiej pod względem konwersji, nie można żadnego „na nowo narodzonego muzułmanina" ani osoby zmieniającej wyznanie automatycznie posądzać o wspieranie terroryzmu, chociaż może to być krok poprzedzający radykalizację. Jak się okazuje, trudno jest odróżnić symptomy mogące świadczyć o radykalizowaniu się więźnia od jego religijności. Przykładem może być Harry Sarfo, który wyjechał z Niemiec walczyć dla ISIS w 2015 r. Zradykalizował się on podczas pobytu w więzieniu, o którym mówił, że był to dla niego okres myślenia o Allahu, czytania *Koranu* i modlitwy – *Czas w więzieniu zbliżył mnie jako muzułmanina do mojego stwórcy*[34].

## 5. Tło radykalizacji więziennej w Wielkiej Brytanii: zakłady karne w strategiach i statystykach

Wielka Brytania jest jednym z państw Unii Europejskiej, które doświadczyło poważnego zagrożenia ze strony rodzimego terroryzmu islamskiego i wciąż tego doświadcza. Dowodem tego jest atak bombowy przeprowadzony w Manchesterze 22 maja 2017 r., w którym zginęły 22 osoby[35]. Szacuje się, że nawet 800 osób związanych z tym krajem wyjechało od początku trwania konfliktu do Syrii i Iraku, aby tam walczyć. Prawdopodobnie 50 proc. z nich już powróciło do kraju[36]. Roczne wydatki rządu brytyjskiego

[33] K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, s. 534.

[34] R. Basra, P. Neumann, *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus*, „Perspectives on Terrorism" 2016, nr 6, s. 31.

[35] Warto zauważyć, że Wielka Brytania ma kilkudziesięcioletnie doświadczenie związane z pobytem terrorystów w więzieniach, które były zdominowane w XX wieku nie przez islamistów, a przez członków IRA. Jednak nie wszystkie ugrupowania odnoszą się do radykalizacji i rekrutacji w więzieniach w ten sam sposób. „IRA, dla przykładu, nie chciała mieć nic wspólnego ze 'zwykłymi' przestępcami, którzy byli postrzegani jako nierzetelni, pozbawieni dyscypliny i potencjalnie szkodzący dla grupowego wizerunku armii wyzwoleńczej, zmierzającej do osiągnięcia celów politycznych", za: *Prisons and Terrorism. Radicalisation and De-radicalisation in 15 Countries*, The International Centre for the Study of Radicalisation and Political Violence, http://icsr.info/wpcontent/uploads/2012/10/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf, s. 6 [dostęp: 23 V 2017].

[36] *Letter from Rt Hon John Hayes MP, Minister of State for Security, to the Chair of the Committee, 6 February 2016*, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/countering-extremism/written/28921.pdf [dostęp: 19 V 2017].

przeznaczone w budżecie na walkę z terroryzmem wzrosły z 594 mln funtów w latach 2015–2016 do 670 mln funtów zaplanowanych na lata 2016–2017[37].

Problem radykalizacji w więzieniach w Wielkiej Brytanii jest akcentowany w dokumentach strategicznych, znajduje się także w zainteresowaniu pierwszoplanowych polityków. *Ustawa o Terroryzmie* (*The Terrorism Act* 2006[38]), uchwalona w odpowiedzi na zamachy z 7 lipca 2005 r., zawiera zapis o możliwości zatrzymania osoby podejrzanej o terroryzm do 90 dni bez postawienia zarzutów, co doprowadziło do wzrostu liczby wyroków za taką działalność. Pomiędzy wrześniem 2001 r. a wrześniem 2014 r. skazano 432 osoby za działalność powiązaną z terroryzmem (statystka wyłącza Irlandię Północną)[39]. Ustawa kryminalizuje również zachowania gloryfikujące terroryzm, czyli przygotowanie do przeprowadzenia ataku oraz jego popieranie bez osobistego bezpośredniego zaangażowania. Statystyki wskazują, że w brytyjskim systemie wymiaru sprawiedliwości stopniowo przybywa muzułmanów, którzy wraz z niemuzułmanami są narażeni na radykalizację prowadzoną przez islamskich ekstremistów.

Nacisk na walkę z ekstremizmem i radykalizacją w zakładach karnych został poruszony w zaktualizowanej w 2011 r. Strategii Walki z Terroryzmem (znanej pod nazwą CONTEST). Składają się na nią cztery filary, tzw. 4P, czyli: zapobieganie (ang. *prevent*), ściganie (ang. *pursue*), ochrona (ang. *protect*) i przygotowanie (ang. *prepare*)[40]. W ramach zapobiegania są realizowane działania mające na celu udaremnienie radykalizacji i wspieranie instytucji, m.in. zakładów karnych, w których ideologia ekstremistyczna może się rozwijać i może być szerzona[41]. W Strategii Zapobiegania (*PREVENT Strategy*), będącej częścią Strategii CONTEST, autorzy jasno wskazują: *Wiemy, że niektórzy ludzie, którzy zostali skazani i uwięzieni za działania związane z terroryzmem, dążą do zradykalizowania i rekrutacji innych więźniów. Wiemy również, że niektóre osoby skazane za działania niezwiązane z terroryzmem, ale utożsamiające się wcześniej ze środowiskami ekstremistycznymi i sieciami terrorystycznymi, aktywnie zaangażowały się w radykalizację i rekrutację podczas pobytu w więzieniu*[42].

W 2015 r. rząd brytyjski opublikował *Strategię Walki z Ekstremizmem* (*Counter-Extremism Strategy*), a w jej wstępie ówczesny premier David Cameron przekonywał,

[37] *Radicalisation: the counter narrative and identifying the tipping point*, House of Commons, Home Affairs Committee, https://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/ 135/135.pdf, s. 3 [dostęp: 19 V 2017].

[38] Tekst ustawy dostępny online: http://www.legislation.gov.uk/ukpga/2006/11 [dostęp: 23 V 2017].

[39] D. Anderson, *A question of trust. Report of the Investigatory Powers Review*, https:// terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf, s. 42 [dostęp: 19 V 2017].

[40] Zob. szerzej I. Jankowska-Czyż, *Przygotowanie Wielkiej Brytanii do przeciwdziałania terroryzmowi*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 6; A. Furgała, D. Szlachter, A. Tulej, P. Chomentowski, *System antyterrorystyczny Wielkiej Brytanii. Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2.

[41] Zob. *Prevent Strategy*, HM Government, https://www.gov.uk/government/uploads /system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf [dostęp: 20 V 2017].

[42] Tamże, s. 87.

że jednym z największych zagrożeń, któremu musi stawić czoła współczesne społeczeństwo brytyjskie, jest plaga ekstremizmu. Dostrzegał ją zarówno w działalności neonazistowskiej, islamofobii, jak i w antysemityzmie[43]. Jego zdaniem walka z islamistycznym ekstremizmem jest jednym z największych wyzwań obecnego pokolenia. Cameron oskarżył poprzednie rządy o dokonywanie złych wyborów, nadmierną pobłażliwość i „tolerancję wobec nietolerancji"[44]. W *Strategii* poruszono też wątek radykalizacji w zakładach karnych, wskazując, że specyficznym problemem jest wzajemne nakłanianie się więźniów do przemocy.

Na system penitencjarny Wielkiej Brytanii składa się wiele rodzajów zakładów karnych zarządzanych zarówno publicznie, jak i – od 1990 r. – przez firmy zewnętrzne, prywatne (na przykład Sodexo Justice Services)[45]. Zasadniczy podział w Anglii i Walii polega na stworzeniu oddzielnych więzień dla mężczyzn, kobiet, dzieci i młodych (ośrodki dla osób pomiędzy 12 a 18 rokiem życia) oraz zakłady dla młodocianych przestępców w wieku od 18 do 21 lat (*Young Offender Institutions*). Mężczyźni zostają przyporządkowani do czterech kategorii bezpieczeństwa:

1) kategoria A – więźniowie, których ucieczka mogłaby nieść za sobą zagrożenie dla społeczeństwa, porządku lub bezpieczeństwa narodowego, ich bezprawne opuszczenie więzienia musi zatem zostać uniemożliwione,
2) kategoria B – więźniowie, którzy nie potrzebują najwyższego poziomu i środków bezpieczeństwa, jednakże ucieczka musi być dla nich trudna do zrealizowania,
3) kategoria C – więźniowie, co do których nie ma pełnego zaufania, że mogą przebywać w otwartych warunkach, ale ze względu na brak środków lub zdolności organizacyjnych nie mogliby uciec z więzienia,
4) kategoria D – więźniowie, co do których istnieje rozsądny poziom zaufania, że mogą odbywać swoją karę w otwartych więzieniach[46].

Przy przyporządkowywaniu więźnia do konkretnej kategorii bierze się pod uwagę przede wszystkim prawdopodobieństwo ucieczki (włączając w to zarówno planowane, jak i rzeczywiste próby ucieczki) oraz zagrożenie, jakie niosłoby dla społeczeństwa i bezpieczeństwa państwa bezprawne opuszczenie więzienia przez te osoby. Do kategorii A zostają przydzieleni mężczyźni skazani za przestępstwa związane między innymi z terroryzmem, narkotykami, rabunkami, morderstwami. Ryzyko ich ucieczki jest podzielone na trzy kategorie: standardowe, wysokie oraz wyjątkowe, z czym jest związane ograniczenie wolności i jeszcze bardziej zaostrzona kontrola nad więźniem, większa niż w pozostałych więzieniach. W przypadku kobiet również stosuje się klasyfikację do czterech kategorii, jednak różnią się one od tych, według których są rozdzielani

[43] *Counter-Extremism Strategy*, HM Government, https://www.gov.uk /government/publications/counter-extremism-strategy, s. 5 [dostęp: 20 V 2017].
[44] Tamże.
[45] *Contracted-out prisons*, UK Justice, https://www.justice.gov.uk/about/hmps/contracted-out [dostęp: 20 V 2017].
[46] Zob. H. Gavin, *Criminological and Forensic Psychology*, London 2014, s. 320; G. Grimwood, *Categorisation of prisoners in the UK*, http://researchbriefings.files.parliament.uk/documents/.../CBP-7437.pdf [dostęp: 21 V 2017].

mężczyźni. W Szkocji wprowadzono trzy kategorie nadzoru: wysoki, średni i niski, a w Irlandii Północnej pięć kategorii bezpieczeństwa[47].

Zgodnie z oficjalnymi statystykami pod koniec 2016 r. niemal połowa osób osadzonych w zakładach karnych Anglii i Walii była chrześcijanami (48,5 proc.), co oznacza prawie 10-procentowy spadek w porównaniu z 2002 r.[48] W sytuacji więźniów deklarujących się jako muzułmanie tendencja jest odwrotna – w 2002 r. stanowili oni 8 proc. ogółu całej więziennej populacji, a niecałe 15 lat później ten odsetek wzrósł do 15 proc. Przyczyny zwiększenia się liczby osób w zakładach karnych Wielkiej Brytanii, które oświadczają, że są muzułmanami, można ująć w trzech punktach:

1) wzrost liczby wyznawców islamu w ogólnej populacji Zjednoczonego Królestwa,
2) niekorzystna pozycja społeczno-ekonomiczna brytyjskiej społeczności muzułmańskiej, która pod względem wieku jest zdecydowanie młodsza od reszty mieszkańców Wysp Brytyjskich,
3) obserwowana od lat tendencja wzrostowa zmiany religii na islam podczas odbywania kary pozbawienia wolności.

Najwięcej wyznawców islamu (47 proc. ogółu) znajduje się obecnie w więzieniu Whitemoor, będącym zakładem karnym o zaostrzonym rygorze, w którym przebywają osoby przydzielone do kategorii A i B[49].

## 6. Frustracje i kryzysy a radykalizacja w brytyjskich więzieniach

Jak już wcześniej wspomniano, radykalizacja jest złożonym procesem, na który oddziałują różne czynniki. Jednym z nich, sprawiającym, że więźniowie są podatni na radykalizację, jest przede wszystkim **kryzys tożsamości**, którego doświadczyły kolejne pokolenia brytyjskich muzułmanów. Dotyczy on zwłaszcza młodych mężczyzn pochodzących z Pakistanu i Bangladeszu. Dzieje się tak, ponieważ nie czują oni związku i nie identyfikują się ani z krajem „przyjmującym" (czyli obecnym miejscem zamieszkania – Wielką Brytanią), ani z miejscem swojego pochodzenia, co czyni ich tożsamość w pewien sposób osłabioną i niepełną. Brak przywiązania kulturowego oraz izolacja, zarówno od społeczeństwa Wielkiej Brytanii, jak i kraju pochodzenia ich rodzin, doprowadziła wielu brytyjskich muzułmanów do utożsamiania się z globalną wspólnotą islamską (arab. *umma*), która wyraża się m.in. w solidarności z muzułmańskimi ofiarami wojen i konfliktów na całym świecie. Jak zauważa Zdzisław Mach: (…) *kryzysy tożsamości mogą powodować negatywne nastawienie wobec innych i wobec wszystkiego, co jednostka ludzka lub grupa definiuje jako obce i wrogie*[50]. Dlatego też młodzi muzułmanie stali się obiektem zainteresowania brytyjskiej polityki wewnętrznej dotyczącej walki z terroryzmem. Istotny pozostaje również konflikt pomiędzy młodymi muzułmanami wychowywanymi i dorastającymi

[47] Tamże.
[48] G. Watson, *UK Prison Population Statistics*, researchbriefings.files.parliament.uk/ documents/.../SN04334.pdf [dostęp: 21 V 2017].
[49] *HMP Whitemoor. Annual Report 2016*, Independent Monitoring Boards, http://www.imb.org.uk/wp-content/uploads/2016/09/Whitemoor-2015-16.pdf, s. 3 [dostęp: 22 V 2017].
[50] Z. Mach, *Przedmowa*, w: *Socjologia tożsamości*, T. Paleczny (red.), Kraków 2008, s. 10.

w Wielkiej Brytanii a ich rodzicami. Młodzież dąży do uzyskania większej wolności i swobody, która jest charakterystyczna dla świata zachodniego, podczas gdy starsze pokolenia niechętnie akceptują coraz większy wpływ kultury zachodniej. Istnieje również teoria, że młodzi ludzie wybierają „tożsamość muzułmańską" jako formę buntu przeciwko pokoleniu swoich rodziców i przypisanemu im statusowi imigranta w brytyjskiej społeczności[51].

Radykalny islam, z jakim brytyjscy muzułmanie spotykają się w zakładach karnych, jest postrzegany przez nich jako szansa na „nowy początek", zarówno w sensie duchowym, jak i w związku z określeniem własnej tożsamości. Ekstremiści pomagają im uporać się z trudami uwięzienia, zazwyczaj sami zaczynają rozmowę z nowo przybyłymi, zagubionymi osobami i oferują wsparcie. „Abu Abdullah"[52] opisuje swoje pierwsze spotkanie z ekstremistami w brytyjskim więzieniu Belmarsh w następujący sposób: *Tego samego dnia [którego przybyłem do więzienia], poszedłem na spacerniak. Miałem tyle myśli w głowie: Co mam robić? Czy ktoś będzie się nade mną znęcał? Nie wiem, czego się spodziewać. Alhamdulillah* (chwała Allahowi – dop. aut.) *miałem szczęście. Tego dnia paru braci zbliżyło się do mnie i powiedzieli, że mnie się spodziewali.* (…) *Ci bracia byli bardzo przyjacielscy. Na początku miałem pewne obawy, czy powinienem im ufać… Ale potem poczułem się komfortowo*[53].

Powodem radykalizacji brytyjskich muzułmanów może być też poczucie żalu, mającego swoje źródła w niesprzyjającej sytuacji ekonomicznej, dyskryminacji (z badań przeprowadzonych w 2015 r. przez Islamską Komisję Praw Człowieka wynika, że 60 proc.brytyjskich muzułmanów doświadczyło lub było świadkiem islamofobii lub dyskryminacji, co oznacza wzrost o 40 proc. w porównaniu z 2010 r.[54]), a także w problemach rodzinnych. Jednym ze źródeł może być również niezadowolenie z polityki zagranicznej Wielkiej Brytanii (będącej elementem ogólnych pretensji politycznych dotyczących postrzeganej hegemonii Zachodu i niezadowolenia z sytuacji międzynarodowej muzułmanów), które może przerodzić się nawet w próbę zemsty. Warto przyjrzeć się ostatniemu z wymienionych czynników, często pojawiającemu się w oficjalnych raportach na temat więziennej radykalizacji.

W 2013 r. nawróceni na islam Brytyjczycy nigeryjskiego pochodzenia Michael Adebolajo i Michael Adebowale najpierw potrącili samochodem, a następnie brutalnie zamordowali rzeźniczym tasakiem brytyjskiego żołnierza, 25-letniego Lee Rigby'ego, który przez jedną zmianę służył w Afganistanie. Sprawcy wykrzykiwali „Allahu akbar", nie zbiegli również z miejsca przestępstwa, lecz tłumaczyli przechodniom swoje poglądy: *Przysięgamy na wszechmogącego Allaha, że nigdy nie przestaniemy z wami walczyć. Zabiliśmy tego mężczyznę tylko dlatego, że* ***muzułmanie codziennie giną z rąk***

[51] O. Lynch, *British Muslim youth: radicalisation, terrorism and the construction of the „other"*, „Critical Studies on Terrorism" 2013, nr 2, s. 244.

[52] Autor ujął imię i nazwisko w cudzysłowie, co sugeruje, że nie są to prawdziwe dane tej osoby, zob. J. Brandon, *Unlocking Al-Quaeda. Islamist Extremism in British Prisons*, London 2009, s. 27.

[53] Cyt. za: tamże.

[54] *Majority of British Muslims have witnessed Islamophobia*, „The Guardian", https://www.theguardian.com/world/2015/nov/11/majority-of-british-muslims-have-witnessed-islamophobia-study [dostęp: 19 V 2017].

***brytyjskich żołnierzy***, dodawali również: *Oko za oko, ząb za ząb*[55]. Adebolajo rok po osadzeniu w zakładzie karnym Belmarsh został przeniesiony do Frankland w związku z podejrzeniami o próby zradykalizowania innych więźniów. Biorąc pod uwagę motyw zabójstwa Rigby'ego można wysnuć przypuszczenie, że Adebolajo szerzył w Belmarsh swoje poglądy i namawiał współwięźniów do zemsty na Brytyjczykach.

Źródłem gniewu i frustracji brytyjskich muzułmanów jest również powszechne odczucie traktowania ich jako „obywateli drugiej kategorii", co jest przyczyną ich separowania się od reszty brytyjskiego społeczeństwa. Warto zaznaczyć, że od wielu lat występowały napięcia pomiędzy Brytyjczykami a muzułmanami, którzy mieli odmienne opinie w wielu sferach życia społecznego. Wyznawcy islamu dużo stracili w oczach opinii publicznej po tym, jak publicznie spalili *Szatańskie wersety* Salmana Rushdiego w odpowiedzi na fatwę ajatollaha Chomeiniego, wzywającego do zabicia autora książki[56]. W kolejnych latach pojawił się problem wojny w Zatoce Perskiej i zarzuty braku lojalności stawiane brytyjskim muzułmanom. W latach 90. XX w. wraz z rozwojem ekstremizmu islamskiego w Wielkiej Brytanii zaczęła szerzyć się islamofobia, która miała swoje apogeum po wydarzeniach z 11 września 2001 r., a następnie po zamachach londyńskich z 7 lipca 2005 r. Również współcześnie brytyjscy muzułmanie stają się ofiarami tak zwanych *hate crimes*. Wszystko to sprawia, że czują się prześladowani w brytyjskim społeczeństwie, a szczególnie w zakładach karnych.

## 7. Organizacyjne uwarunkowania radykalizacji w brytyjskich więzieniach

Brytyjski system więzienny przez przeszło 50 lat, do 2017 r., radził sobie z ekstremistami stanowiącymi największe zagrożenie, rozpraszając ich po sześciu więzieniach oraz regularnie przenosząc z jednego miejsca do drugiego. Miało to na celu zapobieganie zawiązywania się między nimi bliższej relacji i zmniejszenie prawdopodobieństwa radykalizacji innych osób. Stosowana jest również metoda koncentracji większości najgroźniejszych radykalnych islamistów w londyńskim więzieniu Belmarsh, będącym zakładem karnym o zaostrzonym rygorze (kategoria A), która – jak się okazuje – nie spełnia swojego założenia. Jeden z byłych więźniów londyńskiego Belmarsh (absolwent muzułmańskiego uniwersytetu, zwolniony w 2016 r. po odbyciu kary za oszustwa bankowe), stwierdził, że (…) *jest ono jak obóz treningowy dla dżihadystów*, dodał również: (…) *ekstremiści dokonują prania mózgów młodocianym osadzonym, aby szerzyć przekaz terroru na cały system więzienny*[57]. Jego zdaniem w więzieniu funkcjonuje gang nazywający siebie „Bracia", który kieruje drugim życiem więzienia, a o jego funkcjonowaniu wiedzą zarządzający więzieniem, służba więzienna i imamowie.

[55] Cyt. za: *Dożywocie i 45 lat więzienia dla „rzeźników z Londynu" za zabójstwo żołnierza*, TVN24.pl, http://www.tvn24.pl/wiadomosci-ze-swiata,2/dozywocie-i-45-lat-wiezienia-dla-rzeznikow-z-londynu-za-zabojstwo-zolnierza,402449.html [dostęp: 24 V 2017].

[56] J. Balicki, *Imigranci z krajów muzułmańskich w UE. Wyzwania dla polityki integracyjnej. Wybrane zagadnienia*, Warszawa 2010, s. 56.

[57] Cyt. za: S. Tonkin, *Belmarsh maximum security jail is „like jihadi trainig camp" where extremists „brainwash young prisoners to spread terror message across whole prison system"*, http://www.dailymail.co.uk/news/article-3594987/Belmarsh-maximum-security-jail-like-jihadi-training-camp-extremists-brainwash-young-prisoners-spread-terror-message-prison-system.html [dostęp: 20 V 2017].

W kwietniu 2017 r. brytyjskie Ministerstwo Sprawiedliwości (Ministry of Justice) zapowiedziało utworzenie specjalnych jednostek penitencjarnych, do których zostaną przeniesieni ekstremiści stanowiący największe zagrożenie. To rozwiązanie jest wzorowane na holenderskim więzieniu De Schie w Rotterdamie, w którym już od 2006 r. oddziela się ekstremistów od reszty współwięźniów[58]. Jak podkreślił brytyjski podsekretarz stanu w Ministerstwie Sprawiedliwości Sam Gyimah: *Każda forma ekstremizmu musi być pokonana gdziekolwiek się znajduje, zatem słuszne jest odseparowywanie tych, którzy stwarzają największe ryzyko w celu ograniczenia ich wpływu na innych więźniów*[59]. Trzy tzw. centra separacji mają zostać utworzone przy funkcjonujących już zakładach karnych („więzienia w więzieniu") i będą obowiązywać w nich nowe, szczególne zasady. W tych jednostkach będą umieszczane osoby, których zachowanie w czasie odbywania kary pozbawienia wolności będzie zakwalifikowane jako podejrzane, a obniżenie poziomu zagrożenia, jaki stwarzają, będzie możliwe wyłącznie dzięki odseparowania od reszty osadzonych oraz zastosowaniu szczególnego sposobu oddziaływania, zwłaszcza indywidualnych cel i oddzielnego zaplecza resocjalizacyjnego. W ten sposób będzie to dotyczyć więźniów podejrzewanych przede wszystkim o planowanie ataku terrorystycznego oraz tych, którzy sami stanowią zagrożenie dla bezpieczeństwa narodowego lub radykalizują innych.

Co trzy miesiące eksperci będą poddawać ocenie zachowanie tych osób, a na podstawie zebranych informacji mogą postanowić o powrocie danej osoby do reszty społeczeństwa. Ten sposób wydaje się być skuteczny, aby przeciwdziałać radykalizacji i rozszerzaniu ekstremistycznych ideologii w zakładach karnych. Co jest równie ważne, dla każdej osoby osadzonej w nowej formie „więzienia w więzieniu" będzie przygotowywany **indywidualny program deradykalizacji**. Ian Acheson zauważa, że odosobnienie ekstremistów nie może służyć wyłącznie ich ukaraniu, ponieważ wtedy wszystkie starania zawiodą[60]. Dlatego też najważniejsze jest odpowiednie podejście do każdego przypadku. W Rzymskim Memorandum dotyczącym dobrych praktyk w zakresie resocjalizacji i reintegracji ekstremistów podkreśla się konieczność dopasowania programu resocjalizacyjnego do unikalnych cech każdego więźnia (przykładowo, odmiennie należy podejść do osoby skazanej za przewodzenie organizacji terrorystycznej, jak do osoby wspierającej to ugrupowanie; inaczej też powinni być traktowani więźniowie długoterminowi, a inaczej krótkoterminowi)[61].

Pomysł koncentracji ekstremistów w specjalnych jednostkach zyskał zarówno zwolenników, jak i przeciwników. Jednym z argumentów przeciwko nowemu rozwiązaniu jest przedstawianie tego typu więzień jako „brytyjskie Guantanamo". Oznacza to, że wraz

[58] C. Vallance, *The prison wing housing only terrorists*, http://www.bbc.com/news/uk-36336011 [dostęp: 20 V 2017].

[59] *Dangerous extremists to be separated from mainstream prison population*, Ministry of Justice, https://www.gov.uk/government/news/dangerous-extremists-to-be-separated-from-mainstream-prisonpopulation [dostęp: 20 V 2017].

[60] A. Travis, *Islamist extremists in prison „should be in isolated units"*, https://www.thegu ardian.com/society/2016/jul/13/extreme-islamists-in-prisons-should-be-in-isolated-units-england-wales [dostęp: 24 V 2017].

[61] Zob. *Rome Memorandum od Good Practices for Rehabilitation and Reintegration of Violent Extremist Offenders*, Global Counterterrorism Forum, http://www.unicri.it/topics/counter_terrorism /Rome_Memorandum.pdf [dostęp: 24 V 2017].

z przeniesieniem do tej jednostki ekstremiści zdobędą wyższy status w hierarchii więziennej. Może to spowodować próby celowego dostania się do części przeznaczonej „tylko dla terrorystów". Zauważa się również, że w „brytyjskim Guantanamo" mogą zacząć powstawać struktury terrorystyczne. Z kolei zwolennicy twierdzą, że fizyczne oddzielenie ekstremistów od reszty populacji więziennej może w istotny sposób ograniczyć rozprzestrzenianie się radykalnej ideologii islamistycznej.

W przeciwieństwie do sytuacji zaobserwowanych w z wielu państwach Unii Europejskiej (między innymi w Hiszpanii, Belgii czy Francji), więzienia w Wielkiej Brytanii nie są tak bardzo przeludnione, a znajdującym się w nich osobom zapewnia się odpowiednią przestrzeń. Więźniowie wskazują jednak na niesprzyjające warunki życia i brak komfortu, skarżą się na brud (zwłaszcza w toaletach) i wszechobecne graffiti. Co więcej, w kwietniu 2017 r. były szef Narodowego Urzędu ds. Ochrony Antyterrorystycznej (National Counter Terrorism Security Office) Chris Phillips podkreślił, że problemem organizacyjnym sprzyjającym radykalizacji w brytyjskich zakładach karnych jest niedobór pracowników służby więziennej[62]. Ekstremiści z większą swobodą mogą szerzyć radykalną wizję islamu i rekrutować nowych członków do organizacji terrorystycznych, gdy czują, że nie są nieustannie obserwowani. Ponadto im mniej pracowników, którzy są obarczeni licznymi obowiązkami, tym bardziej utrudnione jest zbieranie informacji i późniejsza analiza sytuacji w zakładzie karnym. Zbyt mała liczba strażników powoduje ponadto, że więźniowie są zmuszeni do spędzania więcej czasu w swoich celach, co czyni izolację więzienną jeszcze bardziej dokuczliwą i frustrującą. W rezultacie więzienie nie spełnia jednej ze swoich najważniejszych funkcji, czyli przygotowania osadzonych do powrotu do społeczeństwa, ponieważ więźniowie nie mogą uczestniczyć we wszystkich warsztatach czy zajęciach.

Jesienią 2016 r. oficerowie więziennictwa Anglii i Walii pod przewodnictwem Stowarzyszenia Oficerów Więziennych (Prison Officers' Association, POA) strajkowali przeciwko brakom kadrowym i systematycznej redukcji etatów, sprzeciwiali się eskalacji przemocy oraz przypadkom samookaleczeń, do których dochodzi w brytyjskich więzieniach. Obawy strajkujących były podparte danymi Ministerstwa Sprawiedliwości, z których wynikało, że następuje wzrost liczby napadów na personel więzienny, przy jednoczesnym stopniowym zmniejszaniu liczby pracowników[63]. Pod koniec 2015 r. na jednego pracownika więziennictwa przypadało 3,6 więźnia, co oznacza wzrost o 1,1 w porównaniu z 2010 r. W 2016 r. Mile Rolfe, szef POA, również podkreślał, że w ostatnich pięciu latach liczba pracowników w najważniejszych obszarach działalności więzień zmniejszyła się w przybliżeniu o 28 proc., co jest ściśle związane z **cięciami finansowymi**[64].

[62] *Warnings over increase in Islamic radicalisation in prison*, BBC News, http://www.bbc.com /news/av/uk-32200457/warnings-over-increase-in-islamic-radicalisation-in-prisons [dostęp: 23 V 2017].

[63] H. Munzinger, *Fewer prison officers and more assaults: how UK prison staffing has changed*, https://www.theguardian.com/society/datablog/2016/nov/18/fewer-prison-officers-and-more-assaults-how-uk-prison-staffing-has-changed [dostęp: 23 V 2017].

[64] POA, komunikat prasowy z 18 maja 2016 r., http://www.poauk.org.uk/index.php?press-releases&newsdetail=20160518-10prisons-bill [dostęp: 23 V 2017].

Warto zauważyć, że owi pracownicy brytyjskiego systemu penitencjarnego najczęściej rezygnują z pracy z własnej woli. W 2015 r. aż 39 proc. wszystkich przypadków odejścia z pracy kadry więziennej (oprócz przejścia na emeryturę, z powodów zdrowotnych, zwolnień) było podyktowanych właśnie nieprzymuszonym ustąpieniem z funkcji (dla porównania – rok wcześniej było to 27 proc.)[65]. Rezygnacja z pracy jest często spowodowana obawą o własne zdrowie i wspomnianym wzrostem ataków agresji więźniów wobec personelu więziennego. Zdaniem POA zaistniałą sytuację wykorzystują ekstremiści. Znajdują się oni w więzieniach nie tylko z powodu odbywania wyroku skazującego za popełnione przestępstwa, lecz także aktywnie próbują dostać się do zakładów karnych, np. starają się o otrzymanie tam pracy. Ich celem jest sprawniejsze dotarcie do więźniów, którzy są szczególnie podatni na indoktrynację[66].

Oczywiście nie tylko braki kadrowe są problemem leżącym u podstaw więziennej radykalizacji muzułmanów. Przyczynia się do tego również niewłaściwe kształtowanie relacji pomiędzy osadzonymi a personelem. Podatności na islamistyczną ideologię sprzyja szczególnie poczucie dyskryminacji i nieuczciwości, doświadczane właśnie ze strony pracowników zakładu karnego, co może ponadto kształtować przekonanie o wrogości niemuzułmanów do islamu. W raporcie Królewskiego Inspektoratu Więziennictwa (HM Inspectorate of Prisons, HMIP) zawarto statystykę, zgodnie z którą 43 proc. z 922 muzułmanów biorących udział w badaniu wskazało, że było ofiarą prześladowania ze strony pracowników więzienia (w przypadku niemuzułmanów było to 30 proc.)[67]. Przyczyn tej sytuacji należy upatrywać nie tylko w osobistych uprzedzeniach pracowników więzień, lecz także w ich nieodpowiednim lub niekompletnym wyszkoleniu, pociągającym za sobą jeszcze inne konsekwencje. Przykładowo, niektórzy strażnicy więzienni zajmujący się młodocianymi przestępcami w londyńskim więzieniu Isis nie byli przygotowani do identyfikacji zachowań radykalnych i zgłaszania podejrzeń o radykalizację i szerzenie ekstremizmu wśród współwięźniów. Zdaniem Petera Clarka, szefa HMIP, większość strażników ma wiedzę na temat zarządzania ryzykiem radykalizacji, są jednak i takie osoby, które zdają się ignorować swoje obowiązki w tym zakresie[68]. Praca strażników więziennych jest w niektórych przypadkach utrudniona również ze względu na tak zwaną wrażliwość kulturową. Polityczna poprawność zdaje się wspierać szerzenie się ekstremizmu i utrudnia lub nawet uniemożliwia reakcję adekwatną do przejawów nieodpowiedniego zachowania. Radykalni muzułmanie wywierają presję na personel więzienny, między innymi domagając się opuszczenia przez nich sal modlitewnych podczas praktykowania kultu religijnego czy nie godząc się na przeszukania z powodu

[65] *Prison safety*, House of Commons, Justice Committee, https://www.publications.parliament.uk/pa/cm201516/cmselect/cmjust/625/625.pdf, s. 13 [dostęp: 23 V 2017].

[66] G. Grimwood, *Radicalisation in prisons in England and Wales*, http://researchbriefings .parliament.uk/ResearchBriefing/Summary/CBP-7487, s. 22 [dostęp: 24 V 2017].

[67] *Annual Report 2015-2016*, HM Chief Inspector of Prisons for England and Wales, https://www.justiceinspectorates.gov.uk/hmiprisons/wp-content/uploads/sites/4/2016/07/HMIP-AR_2015-16_web.pdf, s. 115 [dostęp: 24 V 2017].

[68] M. Bentham, *Guards at London prison „unable to identify suspected extremists"*, http://www.standard.co.uk/news/politics/guards-at-london-prison-unable-to-identify-suspected-extremists-a3362481.html [dostęp: 24 V 2017].

stroju. Pracownicy więzień często ustępują muzułmanom, bo nie chcą być posądzeni o rasizm[69].

## 8. Gangi, przemoc i wymuszenia konwersji na islam

Jak już niejednokrotnie sygnalizowano, więzień wraz z rozpoczęciem odbywania kary zaczyna aktywnie poszukiwać sensu i celu istnienia, nadziei, własnej tożsamości i znajomości w nowym środowisku. Konwersja na islam i późniejsze praktykowanie tej religii ze współwięźniami jest częstym sposobem przez brytyjskich więźniów na zaspokojenie potrzeb przynależności i zawiązanie „braterskiej" relacji z innymi. Zmiana wyznania na islam jest jedną z przyczyn wzrostu populacji muzułmanów w zakładach karnych Wielkiej Brytanii. Analizy, które zostały przeprowadzone przez Instytut Kryminologii Uniwersytetu w Cambridge w więzieniu Whitemoor, wykazały, że w przebadanej próbie 23 muzułmanów ponad połowa zadeklarowała zmianę wyznania w trakcie odbywania kary pozbawienia wolności[70].

W 2001 r. aresztowano Richarda Reida, głównego podejrzanego o próbę wysadzenia samolotu amerykańskich linii lotniczych, lecącego z Paryża do Miami. Materiały wybuchowe próbował on ukryć w butach, dlatego został nazwany „*Shoe Bomber"*. W wieku 22 lat Reid zmienił wyznanie na islam podczas 6-letniego pobytu w zakładzie dla młodocianych przestępców Feltham, do którego został skierowany za drobne przestępstwa. Były strażnik więzienny opisuje: *Richard Reid – rozmawiałem z nim każdego dnia. Czy stał się radykałem – radykalnym islamistą – podczas pobytu w brytyjskim więzieniu? Moim zdaniem tak. Wystarczy spojrzeć na charakter jego konwersji, miał kryzys osobisty, nie mógł poradzić sobie z otoczeniem więziennym i szukał swojej tożsamości… Gdybym ja zamierzał kogoś zrekrutować, Richard Reid był osobą, którą chciałbym mieć*[71].

Zdaniem Jamesa Brandona doświadczenia więzienne związane z tożsamością i lojalnością grupową stają się dla „nowych muzułmanów" zdecydowanie bardziej istotne, niż dla osób, które urodziły się i wychowały w wierze islamu[72]. Ten autor zaznacza też, że to oni właśnie w większości przypadków są podatni na radykalizację w wyniku nieumiejętnej interpretacji *Koranu*, przez co dużo łatwiej przyswajają ideologię dżihadu. Również z badań przygotowanych w 2010 r., dotyczących doświadczeń więziennych brytyjskich muzułmanów, wynika, że osoby, które podczas pobytu w zakładzie karnym zmieniły wyznanie na islam, mają tendencję do silniejszego odczuwania swojej tożsamości religijnej, ponadto mają głębsze pragnienie i potrzebę przewodnictwa duchowego[73]. Przyczyny nawrócenia na islam podzielono na trzy główne kategorie:

[69] *„Political correctness" allowing Islamist extremism to flourish in British prisons, report warns*, „The Telegraph", http://www.telegraph.co.uk/news/2016/08/21/political-correctness-allowing-islamist-extremism-to-flourish-in/ [dostęp: 24 V 2017].

[70] A. Liebling, H. Arnold, C. Straub, *An exploration of staff – prisoner relationships at HMP Whitemoor*, Cambridge 2011, s. 3.

[71] M. Hamm, *The Spectacular Few. Prisoner Radicalization and the Evolving Terrorist Threat*, New York–London 2013, s. 47.

[72] J. Brandon, *Unlocking Al-Quaeda*…, s. 19–20.

[73] *Muslim prisoners' experiences: A thematic review*, HM Chief Inspector of Prisons, http://www.ohrn.nhs.uk/resource/policy/MuslimPrisonersThematic.pdf, s. 7 [dostęp: 21 V 2017].

1) pierwsza dotyczy osób, które zostały przyciągnięte do islamu ze względu na dyscyplinę, strukturę i komfort związany z wyznawaniem tej religii,
2) druga dotyczy osób, które poczuły, że przynależność do silnej muzułmańskiej grupy zapewni im ochronę i wsparcie,
3) trzecia to osoby, które dostrzegły materialne korzyści wynikające z identyfikowania siebie jako muzułmanina.

Zauważono, że istnieje prawdopodobieństwo (zwłaszcza w placówkach o zaostrzonym rygorze i dla młodocianych przestępców), że zmiana wyznania może być w niektórych przypadkach rezultatem zastraszania lub wymuszenia siłą. W wywiadzie przeprowadzonym przez brytyjską stację radiową BBC Radio 5 Live były strażnik pracujący w więzieniu Long Lartin stwierdził, że w tym zakładzie nieprzyłączenie się do gangu może być źródłem problemów i trudności, podobnie jak ma to miejsce w więzieniach amerykańskich. Dlatego też więźniowie często zmieniają wyznanie na islam wyłącznie po to, aby siebie chronić, nie identyfikują się i nie przyjmują systemu wartości tej wiary z własnych duchowych potrzeb. Często na cel są obierani młodzi mężczyźni poszukujący wsparcia, które uzyskują od radykalnych muzułmanów, w zamian za co stają się od nich zależni i przez nich kontrolowani. W przypadku niektórych więzień pojawiają się nawet głosy, że zarządcy do tego stopnia stracili kontrolę nad muzułmańskimi gangami zastraszającymi współwięźniów i zmuszającymi ich do zmiany wyznania na islam, że ci więźniowie obawiają się wyjść z celi, próbując się w ten sposób uchronić się przed koniecznością dostosowywania się do narzucanych poglądów. W 2006 r. w więzieniu Belmarsh odkryto działalność gangu nazywającego siebie Muzułmańscy Chłopcy, zajmującego się aktywnym poszukiwaniem rekrutów dla Al-Kaidy. Zmuszali oni więźniów do przyjmowania islamu, atakowali brutalnie osoby, które się im sprzeciwiły i odmówiały konwersji. Ofiary były okaleczane żyletkami i parzone wrzącą wodą.

Radykalizacji sprzyja też studiowanie literatury ekstremistycznej (książek, broszur). Istnieją dowody, że brytyjscy więźniowie mają dostęp do materiałów, w których interpretacji chętnie pomagają islamiści. Ci zaś zachęcają ich (i oczywiście zmuszają) do indywidualnego studiowania. Babar Ahmed, więzień Long Lartin, opisywał: *Tutaj nie ma czasu na odpoczynek, na to przyjdzie czas później. Więzienie nie jest miejscem odpoczynku*. Dodał również: (…) *teraz rozumiem, dlaczego więzienia znane są jako Uniwersytety Wiedzy Islamskiej*[74]. Książki, do których więźniowie mają dostęp, kształtują ich wiedzę o islamie oraz poglądy o otaczającym świecie, w tym o środowisku więziennym. Wspomniany Babar Ahmed przyznał, że odbywając po raz pierwszy karę pozbawienia wolności, miał okazję zapoznać się z dziełami Sayida Kutba (jednego z najważniejszych ideologów ugrupowań dżihadystycznych), które odpowiadały na wiele nurtujących go pytań dotyczących więzienia[75]. Książki zazwyczaj dostarczają muzułmańskie organizację charytatywne sprzeciwiające się ekstremizmowi. Odnotowano jednak sytuację,

[74] J. Brandon, *Unlocking Al-Quaeda*…, s. 50.
[75] Tamże.

że jedna z takich instytucji była do 2009 r. kierowana przez osobę, którą podejrzewano o kontakty z Al-Kaidą.

Może również zdarzyć się sytuacja odwrotna. Muzułmanie mogą tworzyć gangi, aby chronić samych siebie przed wrogo nastawionymi współwięźniami. Ze względu na swoją wiarę stają się również celem przemocy i prześladowań. Badania wskazują, że wyznawcy islamu (w tym ekstremiści) czują się zdecydowanie mniej bezpiecznie w brytyjskich więzieniach niż niemuzułmanie[76]. Z tego też względu przyłączają się do islamistycznych gangów lub takie tworzą, zapewniając sobie bezpieczeństwo. Te grupy przyjmują ideologię, zgodnie z którą przemoc jest dowodem na wrogość niemuzułmanów wobec islamu. Warto zaznaczyć, że agresja i niechęć wobec wyznawców Allaha jest pospolitym zjawiskiem w brytyjskich zakładach karnych, w których ekstremiści odbywający tam karę są w szczególny sposób piętnowani. Przykładem mogą być słowa Mahmouda Abu Rideha: *Moje zatrzymanie w Belmarsh charakteryzuje się ciągłymi nadużyciami, rytualnymi upokorzeniami, obraźliwymi uwagami na temat stroju mojej żony i drwinami na tle rasistowskim*[77]. Sposób, w jaki Abu Rideh był traktowany przez współwięźniów, oraz przetrzymywanie go w zakładzie karnym ponad rok bez procesu doprowadziło go do przekonania, że wszyscy muzułmanie w Wielkiej Brytanii są prześladowani.

Z badań przeprowadzanych we wszystkich typach brytyjskich więzień wynika, że choć dostęp do posługi religijnej jest dość łatwy, to jednak duchowni przeznaczają zbyt mało czasu na przebywanie z więźniami i nie mogą zaspokoić potrzeb religijnych stale rosnącej populacji wyznawców islamu[78]. Zdaniem niektórych muzułmanów kapelani są zbyt mocno utożsamiani z systemem więziennym, przez co nie mogą zostać obdarzeni pełnym zaufaniem. Zidentyfikowano również cztery najbardziej problematyczne okoliczności, sygnalizowane zarówno przez duchownych muzułmańskich, jak i więźniów, mogące wpływać na proces radykalizacji w brytyjskich więzieniach. Są nimi:

1) brak zrozumienia islamu przez pracowników więzień – niemal wszyscy kapelani więzienni uważają, że personel ma negatywne wyobrażenie o islamie i potrzebuje szkoleń na temat wiary i kultury islamu,
2) brak zaufania w kontaktach z muzułmanami ze strony pracowników więzienia i zbyt mocne skupianie się na zagrożeniach bezpieczeństwa,
3) niemożność wypełniania przez kapelanów swoich obowiązków ze względu na brak czasu, przez co jest utrudnione skuteczne wykrywanie oznak radykalizacji,
4) problemy z dostarczaniem muzułmanom odpowiedniej dla nich żywności (w 2013 r. skandal wywołało odnalezienie śladów wieprzowiny w podawanej więźniom żywności halal, co muzułmanie potraktowali jako naruszenie praw człowieka[79])[80].

Choć większość kapelanów więziennych wykonuje użyteczną pracę, są również

[76] *Muslim prisoners' experiences*…, s. 15.
[77] Cyt. za: J. Brandon, *Unlocking Al-Quaeda*…, s. 55.
[78] *Muslim prisoners' experiences*…, s. 8.
[79] *Muslim prisoners sue over contaminated halal pies*, „The Telegraph", http://www.telegr aph.co.uk/news/10341373/Muslim-prisoners-sue-over-contaminated-halal-pies.html [dostęp: 24 V 2017].
[80] *Muslim prisoners' experiences*…, s. 8.

dowody, że niektórzy imamowie promują w zakładach karnych radykalną wizję islamu. Rząd brytyjski zapowiedział nawet wzmocnienie procedur weryfikacji i kontroli duchownych, którym zezwala się na dostęp do więźniów w związku z wykrytą w wielu więzieniach literaturą ekstremistyczną, broszurami i płytami CD[81].

Wzrost zainteresowania radykalnymi imamami nastąpił za sprawą Anjema Choudary, który w 2016 r. został skazany za wspieranie Państwa Islamskiego. Jak zauważa „The Guardian": *Choudary to jeden z najbardziej osławionych kaznodziei nienawiści w Wielkiej Brytanii* (...)*, któremu przez wiele lat udawało się uniknąć aresztu mimo manifestowanej sympatii dla ekstremistów i powiązań z niektórymi z najgroźniejszych brytyjskich terrorystów*[82]. Choudary sam siebie uważa za zwykłego „wykładowcę szariatu", ponadto złożył przysięgę wierności ISIS i za pośrednictwem serwisu YouTube zachęcał do tego również innych muzułmanów. Wraz ze skazaniem radykalnego imama na karę więzienia brytyjskie mediach wyraziły obawy, czy charyzmatyczny Choudary nie będzie wykorzystywał swojej sytuacji i nie zacznie radykalizować współwięźniów[83].

## Zakończenie

Celem artykułu była odpowiedź na pytanie, jakie są przyczyny kształtujące specyfikę zakładu karnego jako miejsca sprzyjającego radykalizacji muzułmanów. W pracy podjęto też próbę zidentyfikowania charakteru problemu w kontekście aktualnej sytuacji w Wielkiej Brytanii. Wskazano, że izolacja od świata zewnętrznego, negatywne skutki kary pozbawiania wolności i trudności z przystosowaniem się do nowego sposobu życia, razem z wieloma dysfunkcjami emocjonalnymi i społecznymi jednostki ułatwiają przyswajanie radykalnych treści i uczuć. Środowisko więzienne bezsprzecznie oddziałuje na człowieka, jednak niektórzy więźniowie wykazują szczególną podatność i wrażliwość na potencjalne radykalne wpływy ze względu na wcześniejsze doświadczenia zdobyte przed skazaniem na pozbawienie wolności (kryzysy tożsamości, potrzeby, uprzednie stosowanie przemocy i inne). Co więcej, więzienia stały się obecnie obiektem debaty dotyczącej nowych rozwiązań organizacyjnych, które w swoim dotychczasowym kształcie zostały uznane za sprzyjające radykalizacji. Dotyczy to niewątpliwie przeludnień, niedoboru pracowników, stosowania przemocy i tortur oraz niewystarczającej liczby imamów dostępnych więźniom. Zasygnalizowano również problem islamistycznych gangów funkcjonujących w obrębie więzień.

W odniesieniu do Wielkiej Brytanii wskazano, że wśród przyczyn mogących zainicjować lub ułatwić proces radykalizacji są przede wszystkim kryzysy tożsamości,

[81] *Summary of the main findings of the review of Islamist extremism in prisons, probation and youth justice*, Ministry of Justice, https://www.gov.uk/government/publications/islamist- extremism-in-prisons-probation-and-youth-justice/summary-of-the-main-findings-of-the-review-of-islamist-extremism-in-prisons-probation-and-youth-justice [dostęp: 24 V 2017].

[82] *„Kaznodzieja nienawiści" może trafić za kraty nawet na 10 lat*, TVN24.pl, http://www.tvn24.pl/wiadomosci-ze-swiata,2/imam-anjem-choudary-uznany-winnym-wspierania-is,6688 48.html [dostęp: 24 V 2017].

[83] Zob. m.in. *How safe is it to lock up Anjem Choudary in prison with Muslim he could radicalise?*, „The Telegraph", http://www.telegraph.co.uk/news/2016/08/17/how-safe-is-it-to-lock-up-anjem-choudary-in-prison-with-muslims/ [dostęp: 24 V 2017].

z jakimi borykają się brytyjscy muzułmanie, niezadowolenie z polityki Zjednoczonego Królestwa wobec wyznawców islamu, dyskryminacja i islamofobia. Zdaniem niektórych badaczy system penitencjarny Wielkiej Brytanii od lat zmaga się z kryzysem, co – zdaniem autorki niniejszej pracy – świadczy właśnie o specyfice problemu radykalizacji w brytyjskich więzieniach. Objawia się on przede wszystkim wzrostem przemocy w zakładach karnych (zarówno w relacjach personelu z więźniami, jak i pomiędzy więźniami), stopniowym pomniejszaniu liczby pracowników w wyniku cięć finansowych lub rezygnacji strażników z pracy, a także z trudnym do opanowania rozwojem gangów wymuszających przemocą zmiany wyznania na islam.

Ujęte powyżej wnioski potwierdzają postawioną na wstępie hipotezę, że niewłaściwe zarządzanie systemem penitencjarnym, połączone z doświadczeniami indywidualnymi i społecznymi muzułmanów sprzyjają radykalizacji więziennej. Zasadne wydają się być następujące uwagi i rekomendacje, odnoszące się do Wielkiej Brytanii, ale mogące znaleźć również zastosowanie w innych państwach. Na podstawie zebranych informacji uzasadnione jest stwierdzenie, że próby walki z więzienną radykalizacją należy rozpocząć od gruntownych reform samego więziennictwa. Szczególnie należy rozwiązać problem przeludnienia w więzieniach, powodujący konsekwencje w postaci między innymi trudności w nadzorowaniu dużych skupisk osób. Niedobór personelu jest jednym z najpoważniejszych wyzwań, jakim musi sprostać system penitencjarny Wielkiej Brytanii, dlatego koniecznie należy stworzyć odpowiednie i sprzyjające warunki pracy. Trzeba również zadbać o to, aby osoby mające kontakt z muzułmanami miały odpowiednią wiedzę na temat islamu, radykalizacji i integracji tego środowiska, aby zminimalizować ryzyko odczuwania przez osadzone osoby niesprawiedliwości, dyskryminacji, niezrozumienia, łamania praw. Osoby zarządzające zakładami karnymi powinny również zdać sobie sprawę, że kapelani muzułmańscy mogą być pomocni w rozwiązywaniu problemów i mogą skutecznie przeciwdziałać radykalizacji. Należy jednak wprowadzić weryfikację, aby dostęp do więzień mieli tylko sprawdzeni i zaufani imamowie. W ramach wyzwań organizacyjnych warto również skupić się na resocjalizacji i reintegracji więźniów, stosując indywidualne programy deradykalizacji. Pozbawienie wolności nie powinno zatem być tylko karą, ale również powinno przygotowywać do powrotu do społeczeństwa. Brytyjscy muzułmanie są grupą silnie odczuwającą różne problemy, które również w ramach odbywania kary powinno się zidentyfikować, aby zmniejszyć ryzyko radykalizacji.

**Bibliografia:**

Anderson D., *A question of trust. Report of the Investigatory Powers Review*, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf [dostęp: 19 V 2017].

*Annual Report 2015–2016*, HM Chief Inspector of Prisons for England and Wales, https://www.justiceinspectorates.gov.uk/hmiprisons/wp-content/uploads/sites/4/2016/07/HMIP-AR_2015-16_web.pdf [dostęp: 24 V 2017].

Balicki J., *Imigranci z krajów muzułmańskich w UE. Wyzwania dla polityki integracyjnej. Wybrane zagadnienia*, Warszawa 2010, Wydawnictwo UKSW.

Basra R., Neumann P., *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus*, „Perspectives on Terrorism" 2016, nr 6, s. 25–40.

Bentham M., *Guards at London prison „unable to identify suspected extremists"*, http://www.standard.co.uk/news/politics/guards-at-london-prison-unable-to-identify-suspected-extremists-a3362481.html [dostęp: 24 V 2017].

Brandon J., *Unlocking Al-Quaeda. Islamist Extremism in British Prisons*, London 2009, (b.w.).

Cialdini R., *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańsk 1994, Gdańskie Wydawnictwo Psychologiczne.

*Contracted-out prisons*, UK Justice, https://www.justice.gov.uk/about/hmps/contracted-out [dostęp: 20 V 2017].

*Counter-Extremism Strategy*, HM Government, https://www.gov.uk /government/publications/counter-extremism-strategy [dostęp: 20 V 2017].

*Dangerous extremists to be separated from mainstream prison population*, Ministry of Justice, https://www.gov.uk/government/news/dangerous-extremists-to-be-separated-from-mainstream-prisonpopulation [dostęp: 20 V 2017].

*Dożywocie i 45 lat więzienia dla „rzeźników z Londynu" za zabójstwo żołnierza*, TVN24.pl, http://www.tvn24.pl/wiadomosci-ze-swiata,2/dozywocie-i-45-lat-wiezienia-dla-rzeznikow-z-londynu -za-zabojstwo-zolnierza,402449.html [dostęp: 24 V 2017].

Gaub F., Lisiecka J., *The crime-terrorism nexus*, http://www.iss.europa.eu/publications/detail/article/the-crime-terrorism-nexus/ [dostęp: 5 V 2017].

Gavin H., *Criminological and Forensic Psychology*, London 2014, (b.w.).

Gilligan A., *Muslim gangs imposing sharia law in British prisons*, http://www.telegraph.co.uk/news /uknews/law-and-order/7428933/Muslim-gangs-imposing-sharia-law-in-British-prisons.html [dostęp: 22 V 2017].

Goffman E., *Asylums. Essays on the Social Situation of Mental Patients and Other Inmates*, Garden City 1961, (b.w.).

Goffman E., *Charakterystyka instytucji totalnych*, w: *Elementy teorii socjologicznych*, W. Derczyński, A. Jasińska-Kania, J. Szacki (red.), Warszawa 1973, PWN.

Grimwood G., *Categorisation of prisoners in the UK*, http://researchbriefings.files.parliament.uk/documents/.../CBP-7437.pdf [dostęp: 21 V 2017].

Grimwood G., *Radicalisation in prisons in England and Wales*, http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7487 [dostęp: 24 V 2017].

Hamm M., *The Spectacular Few. Prisoner Radicalization and the Evolving Terrorist Threat*, New York–London 2013, (b.w.).

*HMP Whitemoor. Annual Report 2016*, Independent Monitoring Boards, http://www.imb.org.uk/wp-content/uploads/2016/09/Whitemoor-2015-16.pdf [dostęp: 22 V 2017].

*How safe is it to lock up Anjem Choudary in prison with Muslim he could radicalise?*, „The Telegraph", http://www.telegraph.co.uk/news/2016/08/17/how-safe-is-it-to-lock-up-anjem-choudary-in-prison-with-muslims/ [dostęp: 24 V 2017].

Izak K., *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, ABW.

*„Kaznodzieja nienawiści" może trafić za kraty nawet na 10 lat*, TVN24, http://www.tvn24.pl/wiadomosci-ze-swiata,2/imam-anjem-choudary-uznany-winnym-wspierania-is,6688 48.html [dostęp: 24 V 2017].

Khosrokhavar F., *Radicalization in Prison: The French Case*, „Politics, Religion & Ideology" 2013, nr 14, s. 284–305.

*Komisarz Rady Europy krytykuje belgijskie więzienia*, TVN24, http://www.tvn24.pl/wiadomosci-ze-swiata,2/belgia-strajk-straznikow-wieziennych-zolnierze-zastepuja-straznikow,642313.html [dostęp: 3 V 2017].

*Letter from Rt Hon John Hayes MP, Minister of State for Security, to the Chair of the Committee, 6 February 2016*, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/countering-extremism/written/28921.pdf [dostęp: 19 V 2017].

Liebling A., Arnold H., Straub C., *An exploration of staff – prisoner relationships at HMP Whitemoor*, Cambridge 2011, Cambridge Institute of Criminology – Prisons Research Centre.

Lynch O., *British Muslim youth: radicalisation, terrorism and the construction of the „other"*, „Critical Studies on Terrorism" 2013, nr 2, s. 241–261.

Mach Z., *Przedmowa*, w: *Socjologia tożsamości*, T. Paleczny (red.), Kraków 2008, Oficyna Wydawnicza AFM, s. 7–16.

Machel H., *Resocjalizacja penitencjarna: trzy uwarunkowania procesu*, „Resocjalizacja Polska" 2011, nr 2, s. 91–107.

*Majority of British Muslims have witnessed Islamophobia*, „The Guardian", https://www.theguardian.com/world/2015/nov/11/majority-of-british-muslims-have-witnessed-islamophobia-study [dostęp: 19 V 2017].

Munzinger H., *Fewer prison officers and more assaults: how UK prison staffing has changed*, https://www.theguardian.com/society/datablog/2016/nov/18/fewer-prison-officers-and-more-assaults -how-uk-prison-staffing-has-changed [dostęp: 23 V 2017].

Musioł S., *Negatywne aspekty kary pozbawienia wolności*, https://ms.gov.pl/pl/probacja/2013/download,2691,9.html [dostęp: 2 V 2017].

*Muslim prisoners' experiences: A thematic review*, HM Chief Inspector of Prisons, http://www.ohrn.nhs.uk/resource/policy/MuslimPrisonersThematic.pdf [dostęp: 21 V 2017].

*Muslim prisoners sue over contaminated halal pies*, „The Telegraph", http://www.telegraph.co.uk/news/10341373/Muslim-prisoners-sue-over-contaminated-halal-pies.html [dostęp: 24 V 2017].

*Overcrowding*, Penal Reform International, https://www.penalreform.org/ priorities/ prison-conditions/key-facts/overcrowding/ [dostęp: 13 V 2017].

Pargeret A., *The New Frontiers of Jihad: Radical Islam In Europe*, Philadelphia 2008, (b.w.).

POA, Komunikat prasowy z 18 maja 2016 r., http://www.poauk.org.uk/index.php?press-releases&newsdetail=20160518-10prisons-bill [dostęp: 23 V 2017].

*„Political correctness" allowing Islamist extremism to flourish in British prisons, report warns*, „The Telegraph", http://www.telegraph.co.uk/news/2016/08/21/political-correctness-allowing-islamist-extremism-to-flourish-in/ [dostęp: 24 V 2017].

*Powstaną 33 nowe więzienia. Między innymi w celu walki z islamską radykalizacją*, RMF24.pl, http://www.rmf24.pl/fakty/swiat/news-powstana-33-nowe-wiezienia-miedzy-innymi-w-celu-walki-z-isla,nId,2286604 [dostęp: 13 V 2017].

*Prevent Strategy*, HM Government, https://www.gov.uk/government/uploads /system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf [dostęp: 20 V 2017].

*Prison safety*, House of Commons, Justice Committee, https://www.publications .parliament.uk/pa/cm201516/cmselect/cmjust/625/625.pdf [dostęp: 23 V 2017].

*Prisons and Terrorism. Radicalisation and De-radicalisation in 15 Countries*, The International Centre for the Study of Radicalisation and Political Violence, http://icsr.info/wpcontent/uploads/2012/10/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf [dostęp: 24 V 2017].

Pyska M., *Drugie życie więzienia*, www.wspia.eu/file/21412/16-PYSKA.pdf [dostęp: 5 V2017].

Rabasa A., Benard Ch., *Eurojihad. Patterns of Islamist Radicalization and Terrorism in Europe*, New York 2015, Cambridge University Press.

*Radicalisation: the counter narrative and identifying the tipping point*, House of Commons, Home Affairs Committee, https://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/ 135/135.pdf [dostęp: 23 V 2017].

*Radykalizacja poglądów religijnych w społecznościach muzułmańskich wybranych państw Unii Europejskiej: Polska – Holandia – Wielka Brytania*, D. Szlachter, P. Potejko i inni (red.), Szczytno 2011, WSPol.

*Rome Memorandum od Good Practices for Rehabilitation and Reintegration of Violent Extremist Offenders*, Global Counterterrorism Forum, http://www.unicri.it/topics/counter_terrorism /Rome_Memorandum.pdf [dostęp: 24 V 2017].

Roy O., *Islamic Terrorist Radicalisation in Europe,* w: *European Islam – Challenges for Society and Public Policy*, S. Amghar, A. Boubekeur, M. Emerson (red.), Brussels 2007, Center for European Policy Studies, s. 52–60.

*Strażnicy więzienni strajkują, wysłano wojsko*, TVN24, http://www.tvn24.pl/ wiadomosci-ze-swiata,2/belgia-strajk-straznikow-wieziennych-zolnierze-zastepuja-straznikow,642313.html [dostęp: 3 V 2017].

*Summary of the main findings of the review of Islamist extremism in prisons, probation and youth justice*, Ministry of Justice, https://www.gov.uk/government/publications/islamist-extremism-in-prisons-probation-and-youth-justice/summary-of-the-main-findings-of-the-review-of-islamist-extremism-in-prisons-probation-and-youth-justice [dostęp: 24 V 2017].

Tonkin S., *Belmarsh maximum security jail is „like jihadi trainig camp" where extremists „brainwash young prisoners to spread terror message across whole prison system"*, http://www.dailymail.co.uk/news/article-3594987/Belmarsh-maximum-security-jail-like-jihadi-training-camp-extremists-brainwash-young-prisoners-spread-terror-message-prison-system.html [dostęp: 20 V 2017].

Travis A., *Islamist extremists in prison „should be in isolated units"*, https://www.theguardian.com/society/2016/jul/13/extreme-islamists-in-prisons-should-be-in-isolated-units-england-wales [dostęp: 24 V 2017].

*The 9/11 Commission Report*, National Commission on Terrorist Attacks, http://govinfo.library.unt.edu/911/report/911Re port.pdf [dostęp: 27 XII 2016].

*The Bush doctrine and the war on terrorism: global responses, global consequences*, M. Buckley, R. Singh (red.), London–New York 2006, Routledge.

*UE podejmuje bardziej zdecydowane działania, aby zwalczać radykalizację postaw prowadzącą do terroryzmu*, Komisja Europejska, komunikat prasowy, http://europa.eu/rapid/press-release_IP-16-2177_pl.htm [dostęp: 4 IV 2017].

Vallance C., *The prison wing housing only terrorists*, http://www.bbc.com/news/uk-36336011 [dostęp: 20 V 2017].

*Warnings over increase in Islamic radicalisation in prison*, BBC News, http://www.bbc.com/news/av/uk-32200457/warnings-over-increase-in-islamic-radicalisation-in-prisons [dostęp: 23 V 2017].

Watson G., *UK Prison Population Statistics*, researchbriefings.files.parliament.uk/ documents/.../SN04334.pdf [dostęp: 21 V 2017].

*Więzienia są wylęgarnią radykałów*, onet.pl, http://wiadomosci.onet.pl/swiat/niemcy-wiezienia-sa-wylegarnia-radykalow/vc4df6 [dostęp: 14 V 2017].

Wosińska W., *Psychologia życia społecznego*, Gdańsk 2004, Gdańskie Wydawnictwo Psychologiczne.

Zięba A., Szlachter D., *Zwalczanie terroryzmu – walka z radykalizacją postaw i werbowaniem terrorystów na obszarze Unii Europejskiej. Studium przypadku społeczności muzułmańskich*, w: *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego. Uwarunkowania – realizacja – wyzwania w drugiej dekadzie XXI wieku*, W. Fehler, K. Marczuk (red.), Warszawa 2015, s. 143–170.

**Słowa kluczowe:** radykalizacja, zakład karny, Wielka Brytania, terroryzm, ekstremizm.

**Keywords:** radicalization, prison, Great Britain, terrorism, extremism.

**Rafał Podolak**

# Dopuszczalny zakres kontroli operacyjnej w systemie praw człowieka[1]

Z początkiem lat 90. XX w. w wyniku transformacji ustrojowej nastąpił w Polsce dynamiczny rozwój przestępczości, w tym przestępczości zorganizowanej, na nieznaną wcześniej skalę. Tradycyjne metody zwalczania przestępczości okazały się w tamtej rzeczywistości niewystarczające, zaszła więc potrzeba stworzenia narzędzia o dużej skuteczności, które dałoby przewagę organom ścigania. Takim narzędziem stała się kontrola operacyjna – pozaprocesowy środek uzyskiwania informacji o przestępstwach i przestępcach, polegający na kontroli niejawnej m.in. treści korespondencji, rozmów, zawartości przesyłek, bez wiedzy osób kontrolowanych. Co warto podkreślić, kontrola operacyjna stała się narzędziem równie skutecznym, jak niebezpiecznym z punktu widzenia państwa prawa. Kontrola operacyjna zakłada bowiem głęboką ingerencję w podstawowe prawa człowieka, jakimi są: prawo do prywatności, wolność, a także tajemnica korespondencji, podlegające ochronie zarówno w krajowym, jak i międzynarodowym porządku prawnym. Istnieje więc ryzyko, że przy nieprawidłowej prawnej regulacji i niedostatecznej ostrożności w korzystaniu z tego narzędzia może dochodzić do zaistnienia stanu zagrożenia praw człowieka. Należy jednak pamiętać, że podczas prowadzenia kontroli operacyjnej uprawnione służby są w stanie uzyskać informacje o przestępstwach, które najprawdopodobniej nie byłyby możliwe do zdobycia w inny sposób. Chodzi o przestępstwa najbardziej szkodliwe z punktu widzenia interesu społecznego. Istotne jest zatem odpowiedzenie na pytanie: co jest ważniejsze – interes ogółu czy interes jednostki? Jak znaleźć równowagę między tymi wartościami? Jaki powinien być dopuszczalny zakres ingerencji państwa w życie prywatne jednostki podczas stosowania kontroli operacyjnej z punktu widzenia ochrony praw człowieka?

## 1. Systemy ochrony praw człowieka

Prawa człowieka jako doniosłe prawa wyrastające wprost z godności człowieka potrzebują skutecznej ochrony. Ochrona praw człowieka zachodzi w ramach tzw. systemów praw

[1] Fragment pracy magisterskiej pt. *Dopuszczalny zakres kontroli operacyjnej w systemie praw człowieka* (Katolicki Uniwersytet Lubelski Jana Pawła II, Wydział Prawa, Prawa Kanonicznego i Administracji). Praca została wyróżniona w siódmej edycji Ogólnopolskiego konkursu Szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2016/2017). Autor wykorzystał fragmenty pochodzące ze wstępu, rozdziału I pt. *Prawa człowieka i systemy ich ochrony – zagadnienia wstępne*; podrozdziały – *Kluczowe pojęcia z zakresu praw człowieka*, *Wnioski*, rozdziału II pt. *Kontrola operacyjna w polskim porządku prawnym*, rozdziału III pt. *Prawo do prywatności i jego dopuszczalne ograniczenia*, rozdziału IV pt. *Zagrożenia dla praw człowieka ze strony kontroli operacyjnej*, podrozdziały – *Kontrola operacyjna w świetle polskiego standardu konstytucyjnego*, *Środki niejawnej kontroli jednostki w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka*, *Wnioski* oraz fragmenty zakończenia.

człowieka. Przez pojęcie system praw człowieka należy rozumieć ogół środków i działań mających na celu zapewnienie i realizację praw człowieka[2]. Wyróżnia się trzy systemy ochrony praw człowieka: system wewnątrzpaństwowy, system ponadnarodowy, jakim jest system Unii Europejskiej, a także system międzynarodowy, w którego ramach można wyróżnić system uniwersalny, czyli system Organizacji Narodów Zjednoczonych, i systemy regionalne. W ramach europejskiego systemu regionalnego działają przede wszystkim Rada Europy i Organizacja Bezpieczeństwa i Współpracy w Europie. Między tymi systemami zachodzi wzajemne oddziaływanie. Prawo międzynarodowe wywiera wpływ na krajowe akty normatywne dotyczące praw człowieka w zakresie ich kierunku i treści. Prawo wewnętrzne z kolei oddziałuje na prawo międzynarodowe w ten sposób, że państwa w procesie stanowienia prawa międzynarodowego często forsują przyjmowanie tych rozwiązań, które już się sprawdziły na płaszczyźnie krajowej.

System ochrony praw człowieka ONZ charakteryzują uniwersalność i unikalność. Uniwersalność wyraża się w wypracowaniu pewnego powszechnego systemu wartości, wspólnego dla wszystkich narodów, niezależnie od ich rozwoju cywilizacyjnego i kultury. Unikalność natomiast wyraża się w globalnym zakresie terytorialnym systemu ochrony praw człowieka ONZ, co czyni go jedynym o tak dużym zasięgu. W ramach systemu ONZ funkcjonują dwa podsystemy: oparty na Karcie Narodów Zjednoczonych[3] i traktatowe, których podstawą są wielostronne umowy międzynarodowe, zawierane pod auspicjami ONZ (głównie *Międzynarodowy Pakt Praw Obywatelskich i Politycznych*[4], MPPOiP). System Rady Europy (europejska Konwencja o ochronie praw człowieka[5], EKPCz) jest regionalnym systemem ochrony praw człowieka.

Krajowy system ochrony praw człowieka jest z reguły oparty na ustawie zasadniczej danego państwa. W przypadku Polski jest to naturalnie Konstytucja RP[6]. To właśnie w Konstytucji RP znajduje się katalog chronionych praw i wolności, a także ogół środków zapewniających realizację praw człowieka. Należy zauważyć, że to właśnie system wewnętrzny odgrywa decydującą rolę, gdyż to on, będąc najbliżej ofiar naruszeń i tym samym będąc najbardziej dla nich dostępny, daje gwarancję najskuteczniejszego dochodzenia przez nie swoich praw. Oczywiście pod warunkiem, że nie jest to system dysfunkcyjny. Z tego też względu systemy międzynarodowe, regionalne i uniwersalny pełnią dwojakie funkcje – kontrolną i korygującą wobec systemów krajowych, a także rolę mechanizmu umożliwiającego dochodzenie naruszonych praw w sytuacji, kiedy system krajowy nie działa prawidłowo.

---

[2] R. Wieruszewski, *ONZ-owski system ochrony praw człowieka*, w: B. Banaszak i in., *System ochrony praw człowieka*, Kraków 2005, s. 57.

[3] *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. z 1947 r. nr 23 poz. 90). Dokument podpisany 26 czerwca 1945 r.

[4] *Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.* (Dz.U. z 1977 r. nr 38 poz. 167).

[5] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2* (Dz.U. z 1993 r. nr 61 poz. 284).

[6] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r. nr 78 poz. 483, ze zm.).

## 2. Kontrola operacyjna i zarys jej prawnej regulacji

Kontrola operacyjna jest metodą pracy operacyjnej stosowaną poza procesem karnym przez odpowiednie, uprawnione do tego służby. Zarówno w mediach, jak i mowie potocznej przyjęło się określanie kontroli operacyjnej mianem „podsłuch". Jest to znaczne uproszczenie, aczkolwiek trudno się dziwić używaniu takiego określenia przez „niewtajemniczonych". Wynika to między innymi z różnorodności sposobów jej prowadzenia, przez co przeciętnemu człowiekowi dużo łatwiej jest przyswoić termin „podsłuch", w którym na dobrą sprawę zamyka się istotę tej czynności. Podsłuch implikuje bowiem ingerencję w prywatność osoby podsłuchiwanej bez jej wiedzy, w celu uzyskania informacji, niekoniecznie ujawnianych z własnej woli.

W obecnie obowiązujących aktach prawnych nie sposób znaleźć definicję legalną kontroli operacyjnej. Jej brak wynika między innymi z różnorodności sposobów prowadzenia kontroli, a także celów, którym ma służyć. Samo pojęcie „kontrola operacyjna" można jednak przybliżyć dzięki odniesieniu się do znaczenia w języku polskim słowa k o n t r o l a, co oznacza sprawdzanie czegoś, zestawianie stanu faktycznego ze stanem wymaganym[7], a także odniesienie się do zadań podmiotów uprawnionych do przeprowadzania kontroli wynikających z aktów normatywnych i do pojęcia „czynności operacyjno-rozpoznawczych". C z y n n o ś c i o p e r a c y j n o - r o z p o z n a w c z e to niejawne działania uprawnionych służb państwa prowadzone poza procesem karnym, mające za zadanie służyć celom obecnym lub przyszłym tego procesu, oraz wykonywane w celu zapobiegania i zwalczania przestępczości. Czynności operacyjno-rozpoznawcze są osadzone w naukach kryminalistycznych, a ramy działań organów ścigania wyznacza prawo[8].

Kontrola operacyjna jest zatem metodą pracy operacyjnej podejmowaną przez uprawnione służby w celu zapobieżenia, wykrycia, ustalenia sprawców, uzyskania i utrwalenia dowodów niektórych umyślnych przestępstw ściganych z oskarżenia publicznego, a także w celu spełniania innych ustawowych zadań, powierzonych tym podmiotom. Jest ona prowadzona niejawnie i zgodnie z obowiązującym stanem prawnym i polega na: uzyskiwaniu i utrwalaniu treści rozmów przy wykorzystaniu środków technicznych, w tym sieci telekomunikacyjnych; uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; uzyskiwaniu dostępu i kontroli zawartości przesyłek. Nie jest to więc jedynie „podsłuchiwanie", jakim to terminem często posługują się media. Od instytucji kontroli operacyjnej należy odróżnić

[7] Hasło: k o n t r o l a, w: *Słownik Języka Polskiego PWN*, http://sjp.pwn.pl/sjp/kontrola;2473611.html [dostęp: 7 XI 2016].

[8] K. Ożóg-Wróbel, *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, nr 4, s. 116.

tzw. podsłuch procesowy, uregulowany w rozdziale 26 kpk[9], mający zastosowanie już po wszczęciu postępowania karnego.

Każda z ustaw, w której dla określonej instytucji przewidziano możliwość prowadzenia kontroli operacyjnej, zawiera katalog spraw lub zadań stanowiących podstawę dopuszczenia takiego środka. Służby bowiem nie mogą gromadzić w ten sposób informacji na temat wszystkich przestępstw. Gdyby tak było, pozwoliłoby to w konsekwencji na wykorzystanie podsłuchu operacyjnego, obarczonego ograniczeniami konstytucyjnymi, nawet w przypadku popełnienia tzw. drobnych przestępstw, co w dobie europeizacji prawa wydaje się być nie do zaakceptowania[10]. Katalog przestępstw jest zamknięty w tym sensie, że uzyskane w ramach takiej kontroli dowody są dowodami pozwalającymi na wszczęcie postępowania karnego lub mają znaczenie dla toczącego się postępowania karnego tylko wtedy, gdy są dowodami popełnienia przestępstw określonych w ustawie formułującej zadania i kompetencje tych organów[11]. Należy jednak zwrócić szczególną uwagę na art. 168b kpk, dodany ostatnimi nowelizacjami, który daje możliwość dowodowego wykorzystania materiałów uzyskanych w drodze kontroli operacyjnej w odniesieniu do przestępstw innych niż katalogowe, a nawet w odniesieniu do osób nieobjętych kontrolą operacyjną, co budzi wątpliwości z punktu widzenia ochrony praw człowieka (o czym w dalszej części niniejszego artykułu). Należy podkreślić również, że tzw. ustawa antyterrorystyczna[12] z 2016 r. poszerzyła możliwości Agencji Bezpieczeństwa Wewnętrznego w zakresie przeprowadzania kontroli operacyjnej. Artykuł 9 tej ustawy daje bowiem możliwość przeprowadzania kontroli operacyjnej w celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym wobec cudzoziemców, w stosunku do których istnieje obawa o prowadzenie przez nich działalności terrorystycznej. Zastosowanie kontroli operacyjnej jest możliwe również w odniesieniu do najpoważniejszych przestępstw, których zwalczanie jest związane z ustawowymi zadaniami uprawnionych do tego służb. Te przestępstwa zazwyczaj charakteryzują się dużą szkodliwością społeczną i z racji „ciężaru gatunkowego" – także większą trudnością w wykryciu, ustaleniu sprawców oraz uzyskaniu i utrwaleniu dowodów dotyczących tych przestępstw. Służby, posługując się narzędziem kontroli operacyjnej, są w tych przypadkach w stanie uzyskać znacznie więcej informacji niezbędnych do prowadzenia postępowania, niż gdyby wykonywały jedynie podstawowe czynności pracy operacyjnej.

Kontrola operacyjna jest obwarowana ustawowo określonym zbiorem zasad dotyczących jej prowadzenia. Te zasady mają zastosowanie od samego momentu jej wszczęcia aż do zakończenia i ewentualnego wykorzystania materiałów z niej pochodzących do procesu karnego. Każda z ustaw zawierających uprawnienia danej służby do prowadzenia kontroli operacyjnej zawiera formułę dotyczącą podstawowego

[9] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: Dz.U. z 2018 r. poz. 1987).
[10] J. Kudła, *Przestępstwa katalogowe w kontroli operacyjnej*, LEX 2016.
[11] K. Woźniewski, *Dopuszczalność wykorzystywania środków dowodowych uzyskanych za pomocą wadliwych czynności dowodowych*, „Gdańskie Studia Prawnicze – Przegląd Orzecznictwa" 2009, nr 3, LEX 2009.
[12] *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

warunku, koniecznego do prowadzenia kontroli. Tym warunkiem jest sytuacja, w której przy wykonywaniu czynności operacyjno-rozpoznawczych inne środki okazały się bezskuteczne albo będą nieprzydatne. Ten warunek określa się inaczej zasadą subsydiarności. Zgodnie z nią nie wolno stosować kontroli operacyjnej na dowolnym etapie czynności prowadzonych przez służby. Aby można było zastosować tę zasadę, musi wcześniej wystąpić bezskuteczność uprzednio stosowanych w danej sprawie środków albo wysokie prawdopodobieństwo, że planowane użycie innych niż kontrola operacyjna środków może być nieprzydatne w konkretnej sytuacji[13]. Ustawodawca używa w omawianych aktach prawnych spójnika „albo", odnosząc się do elementu bezskuteczności albo nieprzydatności innych środków. Do spełnienia zasady subsydiarności wystarczy więc wystąpienie jednej z tych przesłanek[14]. W razie uprzedniego niepodjęcia bezskutecznych działań w ramach czynności operacyjno-rozpoznawczych lub też w razie braku wykazania nieprzydatności innych środków, zastosowanie kontroli operacyjnej będzie sprzeczne z prawem. Jest to szczególnie ważne z praktycznego punktu widzenia, gdyż decyzję o zarządzeniu kontroli operacyjnej podejmuje sąd. Sąd musi być pewien, że opisany wcześniej warunek został spełniony, co wymaga odpowiedniego uzasadniania wniosków o zastosowanie kontroli operacyjnej. Zarządzenie przez sąd kontroli operacyjnej nie tylko może nastąpić na czas ściśle określony w ustawie, lecz także musi dokładnie precyzować, w jakim zakresie i na czym ma polegać zarządzona kontrola[15]. Informacje uzyskane i utrwalone zgodnie z prawem mogą stać się następnie istotnym materiałem dowodowym w procesie karnym.

Kontrola operacyjna jako metoda pracy operacyjnej stosowana poza procesem karnym ma bardzo szeroką i szczegółową regulację. Z powodu swojej skuteczności, poziomu ingerencji w życie prywatne i nadzwyczajnego charakteru jest ona narzędziem podatnym na nadużycia. Tak szczegółowa regulacja jest konieczna ze względu na doniosłość praw i wolności jednostki, w których sferę wkracza się przez stosowanie kontroli operacyjnej. Dotyczy to przede wszystkim prawa do prywatności i wolności korespondencji. Państwo nie może ingerować w te prawa bez przyczyny, na nadmierną skalę, na podstawie prawa o zbyt małej szczegółowości. Może to bowiem prowadzić do nadużyć ze strony państwa, które nie są dopuszczalne w państwie prawa.

### 3. Prawo do prywatności i jego dopuszczalne ograniczenia

Życie prywatne i prawo do jego poszanowania należy rozumieć w sposób szeroki, tzn. uwzględniający takie elementy, jak np. tajemnica korespondencji czy nienaruszalność mieszkania. Prawo do prywatności nie jest jednak wartością absolutną, podlega ograniczeniom ze względu na dobro ogółu. Niczym nieskrępowany zakres praw i wolności człowieka nieuchronnie prowadziłby do kolizji z interesem społeczeństwa.

[13] P. Pochodyła, S. Franc, *Kontrola operacyjna oraz zakres jej stosowania*, „Zeszyty Naukowe WSEI", seria: „Administracja" 2011, nr 1, s. 205.
[14] S. Hoc, P. Szustakiewicz, *Ustawa o CBA. Komentarz*, LEX 2012.
[15] Postanowienie Sądu Apelacyjnego w Lublinie z 21 grudnia 2011 r., sygn. akt II AKz 611/11.

W międzynarodowych i krajowych aktach prawnych rolę przepisów ograniczających odgrywają tzw. klauzule limitacyjne, inaczej ograniczające. Przewidują one wiele wymogów stawianych okrojeniu praw i wolności człowieka, po których spełnieniu dopiero można mówić o ograniczeniu dopuszczalnym.

Prywatność jest ściśle związana z pojęciem „interes własny jednostki", z jej dobrem oraz z aktywnością podejmowaną przez jednostkę na rzecz ochrony tego dobra, w przeciwieństwie do aktywności podejmowanej dla dobra wszystkich[16]. W ramach sfery prywatności to jednostka decyduje o informacjach jej dotyczących udostępnianych innym osobom. Nie podlega ona również w swoim działaniu ingerencji ze strony osób trzecich, jest autonomiczna. Samo prawo do prywatności jako dobro chronione prawem zostało jednak dostrzeżone dopiero pod koniec XIX wieku. Pojęciem „prawo do prywatności" (ang. *right to privacy*) posłużyli się w 1890 r. w swoim artykule *The Right to Privacy*[17] dwaj amerykańscy prawnicy – Samuel D. Warren i Louis D. Brandeis. Autorzy wskazywali w nim przypadki, w których amerykańskie sądy przy wydawaniu wyroków w sprawach mogących być uznanymi za naruszenie sfery życia prywatnego, opierały się na takich podstawach prawnych, jak naruszenie własności, naruszenie tajemnicy. Dowodzili tym samym, że istnieje wspólna, niewyrażona expressis verbis podstawa, którą jest prawo do prywatności służące ochronie nienaruszalnej osobowości[18].

Pomimo fundamentalnego znaczenia tego prawa, problemem jest stworzenie jego definicji. Wspomniana wyżej koncepcja *right to privacy* obejmuje swoim zasięgiem bardzo szeroki zakres wartości chronionych. Z tego też względu doktryna prawa i orzecznictwo, zajmując się tą dziedziną, raczej nie podejmuje się definiowania prywatności. Skupia natomiast swoją uwagę na wyliczaniu sfer, które powinny być chronione za pomocą konstrukcji prawa do prywatności, albo też ustala listy działań, które godzą w sferę życia prywatnego jednostki[19]. Taka lista działań godzących w prawo do prywatności jednostki może obejmować np. ingerencję w życie prywatne, rodzinne lub domowe, naruszenie integralności psychofizycznej człowieka, naruszenie czci, honoru lub opinii, ujawnienie intymnych lub krępujących faktów odnoszących się do życia prywatnego osoby, niepokojenie osoby przez śledzenie, naruszanie korespondencji, nadużycie informacji uzyskanych prywatnie, ujawnienie informacji uzyskanych od zainteresowanego lub udzielonych w warunkach poufności[20]. Podczas stosowania kontroli operacyjnej szczególne znaczenie ma ingerencja w życie prywatne, naruszanie tajemnicy korespondencji, a także niezgodne z prawem gromadzenie informacji o obywatelach przez władze publiczne.

[16] J. Braciak, *Prawo do prywatności*, w: *Prawa i wolności obywatelskie w Konstytucji RP*, Warszawa 2002, s. 278.

[17] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, nr 5, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [dostęp: 24 III 2017].

[18] Z. Mielnik, *Prawo do prywatności (zagadnienia wybrane)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2, s. 29.

[19] K. Degórska, *Prawo do ochrony życia prywatnego i rodzinnego*, w: *Prawa i wolności I i II generacji*, A. Florczak, B. Bolechow (red.), Toruń 2006, s. 148.

[20] Zob. K. Kubiński, *Ochrona życia prywatnego człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1993, nr 1, s. 62.

### 3.1. Prawo do prywatności w systemach ochrony praw człowieka

Przed wejściem w życie obowiązującej obecnie Konstytucji RP ochronę prywatności, z braku norm konstytucyjnych w tym zakresie, wywodzono z zasady demokratycznego państwa prawa i obowiązujących Polskę umów międzynarodowych[21]. Uznanie ochrony życia prywatnego za element demokratycznego państwa prawa dało podstawę do uregulowania prawa do prywatności w obecnie obowiązującej Konstytucji RP. Zgodnie z art. 47 Konstytucji RP każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W art. 49 czytamy, że zapewnia się wolność i ochronę tajemnicy komunikowania się, a ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Ponadto art. 51 ust. 2 stanowi, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Wprowadzenie tych przepisów do Konstytucji RP spowodowało zaliczenie ich do konstytucyjnie chronionych praw jednostki, a to oznacza bezpośredniość ich stosowania, a więc możność zastosowania ich wprost, bez dodatkowej implementacji w ustawach zwykłych[22].

Na gruncie Konstytucji RP przyjmuje się, że prywatność odnosi się między innymi do ochrony informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu[23]. Trybunał Konstytucyjny (dalej: TK) już jakiś czas temu zauważył, że z powodu immanentnego związku prawa do prywatności z godnością człowieka naruszanie prawa do prywatności może prowadzić do zagrożenia godności jednostki[24]. Stąd należy stwierdzić, że podmiotowym zakresem prawa do prywatności są objęte osoby fizyczne, gdyż tylko one są zdolne do posiadania życia prywatnego, rodzinnego i czci[25]. Postanowienia konstytucyjne ustanawiające zasadę ochrony sfery życia prywatnego są ogólne i nieprecyzyjne, jest to jednak zabieg celowy i trafny, gdyż próba wyczerpującego wyliczenia sytuacji będących wyrazem korzystania z wolności i praw stwarza poważne ryzyko pozostawienia istotnych okoliczności faktycznych i prawnych poza zakresem regulacji[26]. Uściślenie zakresu prawa do prywatności, enumeratywne wyliczenie jego elementów składowych pozostawia się więc doktrynie i orzecznictwu.

Ochrona tajemnicy korespondencji oznacza prawo do zachowania w tajemnicy treści przekazu wysyłanego do oznaczonego adresata, jeśli taka jest wola nadawcy[27]. Tajemnica korespondencji podlega ochronie nie tylko w stosunkach wertykalnych, to znaczy

[21] Zob. Orzeczenie Trybunału Konstytucyjnego z 24 czerwca 1997 r., sygn. akt K 21/96.
[22] K. Degórska, *Prawo do ochrony*…, s. 154.
[23] *Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., sygn. akt U 5/97* (Dz.U. z 1988 r. nr 67 poz. 444).
[24] *Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r., sygn. akt K 32/04* (Dz.U. z 2005 r. nr 250 poz. 2116).
[25] J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych*, w: *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, M. Jabłoński (red.), Wrocław 2014, s. 159.
[26] Z. Zawadzka, *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną: Problem rozstrzygania konfliktu zasad*, LEX 2013.
[27] M. Balcerzak, *Prawo do poszanowania korespondencji*, w: B. Gronowska i in., *Prawa człowieka i ich ochrona*, Toruń 2010, s. 370.

w stosunkach państwo – jednostka, lecz także w relacjach horyzontalnych, czyli relacjach jednostka – jednostka[28]. Zgodnie z wyrokiem TK prywatność i wolność komunikowania się to sfery pozostające we wzajemnym związku[29]. Należąca do sfery prywatności tzw. autonomia informacyjna wiąże się nie tylko z prawem do wytyczenia zakresu „niedostępności" w odniesieniu do informacji osobistych, lecz także w odniesieniu do informacji o własnych poglądach politycznych, ideologicznych, światopoglądowych, ocenach zjawisk publicznych oraz innych osób, w tym pełniących funkcje publiczne.

Prawo człowieka do prywatności zostało uwzględnione już w 1948 r. w *Powszechnej Deklaracji Praw Człowieka*[30] z 1948 roku (dalej: PDPCz). W art. 12 PDPCz czytamy, że nikt nie będzie podlegać arbitralnemu wkraczaniu w jego życie prywatne, rodzinne, mieszkanie lub korespondencję ani też nie będzie podlegać zamachom na jego honor i reputację. Niemal identyczną regulację dotyczącą prawa do prywatności zawiera art. 17 MPPOiP.Twórcy *Deklaracji* oraz *Paktu* zapewne zdawali sobie sprawę z tego, że prywatność jest pojęciem bardzo ogólnym, toteż w art. 12 PDPCz i art. 17 MPPOiP oprócz „życia prywatnego" pojawiają się także takie jego składniki, jak „mieszkanie" czy „korespondencja". Obowiązki państwa, zgodnie z *Deklaracją* i *Paktem*, mają przede wszystkim charakter negatywny, to znaczy mają formę zakazu samowolnej ingerencji w sferę życia prywatnego jednostki.

Zgodnie z art. 8 EKPCz każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. W odróżnieniu od PDPCz i MPPOiP w *Konwencji* stylistyczny nacisk kładzie się na obowiązek poszanowania sfery prywatnej człowieka, a nie na zakaz ingerencji. Pojęciowo sprowadza się to do zakazu arbitralnej ingerencji ze strony władz publicznych, a także do obowiązku działania pozytywnego w postaci podejmowania środków mających na celu zapewnienie poszanowania życia prywatnego[31]. Ponieważ samo prawo do poszanowania życia prywatnego jest unormowane bardzo zwięźle w *Konwencji*, precyzowanie standardów jego ochrony następuje w orzecznictwie Europejskiego Trybunału Praw Człowieka (dalej: ETPCz).

### 3.2. Ograniczenie prawa do prywatności w systemach ochrony praw człowieka – klauzule limitacyjne

Klauzulami limitacyjnymi określa się postanowienia formułujące warunki dopuszczalności ingerencji w substancję chronioną uprawnień[32]. Klauzule limitacyjne odwołują się do pojęć bardzo ogólnych, takich jak „demokratyczne państwo" oraz „bezpieczeństwo państwa". Typowa klauzula limitacyjna składa się z trzech elementów:

[28] M. Bartoszewicz, *Komentarz do art. 49 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* M. Haczkowska (red.), LEX 2014.

[29] Zob. *Wyrok Trybunału Konstytucyjnego z dnia 11 października 2006 r., sygn. akt P 3/06* (Dz.U. z 2006 r. nr 190 poz. 1409).

[30] *Powszechna Deklaracja Praw Człowieka (rezolucja Zgromadzenia Ogólnego ONZ 217/III A w dniu 10 grudnia 1948 r.)*, http://www.bb.po.gov.pl/Prawa/PNZ/PDPCZ.pdf [dostęp: 2 III 2017].

[31] Wyrok ETPCz z 22 października 1996 r. w sprawie Stubbings i inni przeciwko Wielkiej Brytanii, skarga nr 22083/93, 22095/93, pkt 62.

[32] R. Mizerski, *Limitacja korzystania z praw człowieka*, w: B. Gronowska i in., *Prawa człowieka i ich ochrona*, Toruń 2010, s. 234.

zgodności ingerencji z prawem, realizowania przez ingerencję celu prawowitego, konieczności ingerencji w społeczeństwie demokratycznym[33]. Weryfikacja, czy ograniczenie wolności i praw było dopuszczalne, odbywa się za pomocą trzech testów nawiązujących do elementów klauzuli limitacyjnej. Test legalności służy sprawdzeniu, czy ograniczenie ma swoją podstawę w obowiązującym prawie. Test celowości określa, czy ograniczenie zaszło z uwagi na cel prawowity, np. bezpieczeństwo państwa, porządek publiczny. Test konieczności z kolei bada, czy ograniczenie było konieczne w demokratycznym społeczeństwie. Aby limitacja była dopuszczalna, wszystkie trzy testy muszą dawać wynik pozytywny[34].

Konstytucja RP w art. 31 ust. 3 zawiera tzw. ogólną klauzulę limitacyjną, to znaczy taką, która dotyczy wszystkich praw i wolności gwarantowanych tym aktem prawnym[35]. Zgodnie z klauzulą zawartą w art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą następować z zachowaniem trzech warunków: wyłączności ustawy, proporcjonalności oraz zachowania istoty wolności i praw, a także przy wystąpieniu materialnych przesłanek dopuszczalności ograniczeń, do których zalicza się: bezpieczeństwo państwa, porządek publiczny, ochronę środowiska, zdrowia i moralności publicznej, wolność i prawa innych osób[36]. Jeśli chodzi o wymienione wyżej przesłanki materialne, ich katalog jest katalogiem zamkniętym, a do dopuszczalności ograniczenia wystarczy wystąpienie nawet jednej z nich[37]. Ograniczenia praw i wolności można wprowadzić tylko w ustawie. Należy to pojmować dosłownie, z wykluczeniem dopuszczalności subdelegacji, tj. przekazania kompetencji normodawczej innemu organowi[38]. Unormowanie ustawowe musi cechować zupełność, co znaczy, że w żadnym wypadku, w sytuacji sporu pomiędzy jednostką a organem władzy publicznej o zakres czy sposób korzystania z wolności i praw, podstawa prawna rozstrzygnięcia tego sporu nie może być oderwana od unormowania konstytucyjnego ani mieć rangi niższej od ustawy[39]. Zasada proporcjonalności łączy się z wymogiem konieczności ograniczenia i wyraża się w trzech przesłankach: ograniczenie prowadzi do zamierzonych skutków, ograniczenie jest niezbędne do ochrony interesu publicznego, rezultaty ograniczenia pozostają w odpowiedniej proporcji do ciężarów nakładanych na obywatela[40]. Niezbędność wyraża się w tym, że środki, prowadzące do ograniczenia praw i wolności powinny chronić wartości określone w art. 31 ust. 3 Konstytucji RP, w sposób bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych

[33] Tamże, s. 235.
[34] Tamże.
[35] J. Zakolska, *Problem klauzuli ograniczającej korzystanie z praw i wolności człowieka w pracach konstytucyjnych, w poglądach doktryny i orzecznictwa Trybunału Konstytucyjnego*, „Przegląd Sejmowy" 2005, nr 5, s. 11.
[36] A. Łabno, *Ograniczenie wolności i praw człowieka na podstawie art. 31 Konstytucji III RP*, w: *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (red.), Warszawa 2002, s. 699.
[37] M. Piechowiak, *Klauzula limitacyjna a nienaruszalność praw i godności*, „Przegląd Sejmowy" 2009, nr 2, s. 56–57.
[38] *Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., sygn. akt U 5/97*…
[39] Tamże.
[40] Orzeczenie Trybunału Konstytucyjnego z dnia 26 kwietnia 1995 r., sygn. akt K 11/94.

środków[41]. Istota prawa lub wolności zostanie naruszona, gdy regulacje prawne, nie znosząc danego prawa lub wolności, w praktyce uniemożliwiają korzystanie z niego[42]. Ingerencja polskich organów władzy publicznej w sferę praw człowieka musi spełniać wymogi określone w klauzulach ograniczających, zamieszczonych w MPPOiP oraz EKPCz, co wynika z tego, że obie umowy międzynarodowe są częścią polskiego porządku prawnego, są stosowane bezpośrednio i mają pierwszeństwo przed ustawami, których nie da się z nimi pogodzić[43].

Europejska *Konwencja o ochronie praw człowieka* nie zawiera jednej, ogólnej klauzuli limitującej, podobnej do tej istniejącej w Konstytucji RP. Zawiera za to wiele szczegółowych klauzul ograniczających dotyczących gwarantowanych praw i wolności. Pozwala to na szczegółowe dostosowanie ograniczeń do specyfiki danego prawa bądź wolności. Taką klauzulę zawiera również prawo do poszanowania życia prywatnego. Zgodnie z art. 8 ust. 2 EKPCz niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do poszanowania życia prywatnego i rodzinnego jednostki, a także jej mieszkania i korespondencji, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób. Klauzula wyrażona w tym artykule zawiera więc typowe dla klauzuli limitującej wymienione wcześniej elementy, czyli zgodność ingerencji z prawem, realizowanie przez ingerencję celu prawowitego i konieczność ingerencji w społeczeństwie demokratycznym. ETPCz formułuje wymogi co do właściwości prawa. Musi być ono dostępne, precyzyjne i musi przewidywać efektywne środki kontroli. Dostępność wyraża się w możliwości orientacji jednostki w tym, jakiego zachowania prawo oczekuje od niej w danej sytuacji[44]. Precyzyjność natomiast wyraża się w możliwości przewidzenia przez jednostkę prawnych konsekwencji swojego zachowania[45]. Efektywne środki kontroli to środki chroniące jednostkę przed nieuprawnionym naruszeniem swoich praw ze strony państwa, a ich egzystencja wynika z samej zasady rządów prawa[46].

W artykule 8 ust. 2 EKPCz wśród celów prawowitych wymienia się bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności, ochronę

[41] A. Deryng, *Rzecznik Praw Obywatelskich jako wnioskodawca w postępowaniu przed Trybunałem Konstytucyjnym*, LEX 2014.

[42] B. Banaszak, *Prawa człowieka i obywatela w nowej Konstytucji Rzeczypospolitej Polskiej*, „Przegląd Sejmowy" 1997, nr 5, s. 57.

[43] K. Wojtyczek, *Zasada proporcjonalności*, w: *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (red.), Warszawa 2002, s. 680–681.

[44] Wyrok ETPCz z 26 kwietnia 1979 r. w sprawie Sunday Times przeciwko Wielkiej Brytanii, skarga nr 6538/74, pkt 49.

[45] Tamże.

[46] Wyrok ETPCz z 25 marca 1983 r. w sprawie Silver i inni przeciwko Wielkiej Brytanii, skarga nr 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, pkt 90.

praw i wolności osób. Znaczenie tych celów precyzują tzw. Zasady Syrakuskie[47], które są poświęcone wprawdzie MPPOiP, ale mają również znaczenie dla EKPCz. Zgodnie z nimi bezpieczeństwo państwowe uzasadnia ingerencję w prawa i wolności człowieka tylko w przypadku zagrożenia samego bytu narodu, jego integralności terytorialnej lub jego politycznej niezależności. Zasady Syrakuskie stanowią też, że ograniczanie praw i wolności ze względu na bezpieczeństwo publiczne może następować w przypadku zagrożenia bezpieczeństwa obywateli, ich życia lub integralności, lub ich własności – w postaci poważnego uszczerbku. W przypadku ochrony porządku publicznego limitacja może zachodzić w celu ochrony zespołu reguł zapewniających funkcjonowanie społeczeństwa lub też zespołu fundamentalnych zasad, na których jest zbudowane społeczeństwo. Przesłanka ochrony porządku publicznego powinna być interpretowana w świetle istoty danego prawa lub wolności podlegających ograniczeniu, a organy państwa stojące na straży porządku publicznego powinny być kontrolowane przez parlament, sądy i inne kompetentne i niezależne podmioty w trakcie pełnienia swoich zadań. Kontrola dotyczy więc także działalności policji i służb specjalnych. Ograniczenia praw i wolności muszą być także konieczne w demokratycznym społeczeństwie. Zasady Syrakuskie uznają za konieczne te ograniczenia, które są oparte na celu prawowitym, są do niego proporcjonalne i są odpowiedzią na pilną potrzebę społeczną. Ocena, czy ograniczenie spełnia przesłankę konieczności, jest powierzone władzom krajowym. Europejski Trybunał rozpatruje jedynie, czy państwo działało rozsądnie, ostrożnie i w dobrej wierze[48]. Państwo, które decyduje się ograniczyć prawa i wolności, musi wykazać, że te ograniczenia nie podważają funkcjonowania demokratycznego społeczeństwa.

Zgodnie z art. 17 MPPOiP nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję. W *Pakcie* nie występuje wyrażona wprost klauzula limitacyjna dotycząca tego artykułu. Informację o dopuszczalnych ograniczeniach tego prawa stanowią wymienione w tekście artykułu dwa przypadki, które przesądzają o niedopuszczalności ingerencji – taka ingerencja jest samowolna lub bezprawna. Klauzula bezprawnej ingerencji oznacza, że ingerencja, do której państwo jest upoważnione, może nastąpić wyłącznie na podstawie prawa. To prawo zaś musi być zgodne z postanowieniami, celami i zasadami *Paktu*. Natomiast samowolna, inaczej – arbitralna, ingerencja może również dotyczyć ingerencji dokonywanej na podstawie prawa. Nawet ingerencja, do której dochodzi na podstawie prawa, powinna następować w zgodzie z postanowieniami, celami i zasadami *Paktu* i w każdym przypadku powinna znajdować uzasadnienie w konkretnych okolicznościach. Specjalny Sprawozdawca ONZ do spraw promocji i ochrony wolności wyrażania opinii

[47] *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Commission on Human Rights, 28 IX 1984 r., E/CN.4/1985/4, http://www.refworld.org/docid/4672bc122.html [dostęp: 2 III 2017].

[48] Wyrok ETPCz z 26 września 1995 r. w sprawie Vogt przeciwko Niemcom, skarga nr 17851/91, pkt 52.

stwierdza w swoim raporcie z 2013 r.[49], że mimo że art. 17 nie zawiera wyrażonej wprost klauzuli limitacyjnej, to jednak podlega takiemu samemu testowi dopuszczalnej limitacji, jakiemu podlegają inne prawa i wolności wyrażone w *Pakcie* mające taką klauzulę, np. art. 12 ust. 3 *Paktu*. Test dopuszczalnej limitacji jest opisany między innymi w Komentarzu Ogólnym ONZ nr 27[50] z 1999 r., dotyczącym wolności poruszania się. Zgodnie z opinią Komitetu wyrażoną w tym Komentarzu ograniczanie wolności i praw musi następować między innymi na mocy prawa, nie może naruszać ich istoty, musi być konieczne w demokratycznym społeczeństwie ze względu na cele prawowite oraz musi być proporcjonalne do celu, który ma być osiągnięty. Wyjaśnienie terminów „demokratyczne społeczeństwo" i innych znajduje się w Zasadach Syrakuskich, o których była mowa wcześniej.

Kontrola operacyjna bez wątpienia jest narzędziem umożliwiającym wkroczenie w sferę prywatności jednostki. Wskazuje się w tym względzie na szczególne znaczenie np. ingerencji w wolność i tajemnicę korespondencji bądź niezgodnego z prawem gromadzenia danych o jednostkach przez władze publiczne. Regulacja kontroli operacyjnej jako regulacja instrumentu ograniczającego prawo do prywatności musi tym samym odpowiadać standardom i wymogom znajdującym zastosowanie w ramach funkcjonowania poszczególnych klauzul limitacyjnych. Jeśli nie będzie ona odpowiadać tym wymogom, to będzie wtedy limitacją niedopuszczalną, a to z kolei wiąże się z powstawaniem zagrożeń dla prawa do prywatności.

## 4. Kontrola operacyjna w świetle polskiego standardu konstytucyjnego

Dla obecnego kształtu prawnej regulacji kontroli operacyjnej podstawowe znaczenie miał wyrok w sprawie o sygn. akt K 23/11, wydany przez TK w 2014 r.[51] W tym wyroku Trybunał Konstytucyjny dokonał wskazania wymogów dotyczących prawnej regulacji kontroli operacyjnej. Te wymogi mają na celu zagwarantowanie, że naruszenie prawa do prywatności osoby objętej kontrolą odbędzie się zgodnie z obowiązującym prawem krajowym i międzynarodowym. Wykonanie tego wyroku doprowadziło do nowelizacji ustawy o Policji i innych ustaw przewidujących stosowanie kontroli operacyjnej, brak zastosowania się ustawodawcy do wymogów przedstawionych w wyroku TK prowadziłby bowiem nieuchronnie do zaistnienia stanu zagrożenia dla praw człowieka.

Po pierwsze gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek, a zwłaszcza sfery prywatności, jest dopuszczalne wyłącznie na podstawie wyraźnego i precyzyjnego przepisu ustawy. Konieczne jest także precyzyjne określenie w ustawie organów państwa upoważnionych do gromadzenia oraz przetwarzania

[49] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Human Rights Council, 17 IV 2013 r., A/HRC/23/40, http://www.refworld.org/docid/51a5ca5f4.html [dostęp: 2 III 2017].

[50] *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, UN Human Rights Committee (HRC), 2 XI 1999 r., CCPR/C/21/Rev.1/Add.9, http://www.refworld.org/docid/45139c394.html [dostęp: 2 III 2017].

[51] *Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11* (Dz.U. z 2014 r. poz. 1055).

danych o jednostce, w tym do stosowania czynności operacyjno-rozpoznawczych. W świetle obecnie obowiązujących przepisów dotyczących kontroli operacyjnej wydaje się, że ten standard jest realizowany.

W ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach, którymi są wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im, a ustawa powinna wskazywać rodzaje takich przestępstw. W przypadku kontroli operacyjnej przepisy przewidujące możliwość jej stosowania zawierają katalog przestępstw, przy których zwalczaniu można zarządzić kontrolę. Można byłoby więc mówić o realizacji tego standardu, gdyby nie dodany nowelizacją z 11 marca 2016 r. art. 168b kpk. Mowa jest w nim bowiem o tym, że:

> Jeżeli w wyniku kontroli operacyjnej zarządzonej na wniosek uprawnionego organu na podstawie przepisów szczególnych uzyskano dowód popełnienia przez osobę, wobec której kontrola operacyjna była stosowana, innego przestępstwa ściganego z urzędu lub przestępstwa skarbowego niż przestępstwo objęte zarządzeniem kontroli operacyjnej lub przestępstwa ściganego z urzędu lub przestępstwa skarbowego popełnionego przez inną osobę niż objętą zarządzeniem kontroli operacyjnej, prokurator podejmuje decyzję w przedmiocie wykorzystania tego dowodu w postępowaniu karnym.

W świetle powyższej regulacji te przestępstwa nie muszą więc być nawet przestępstwami katalogowymi. Prowadzi to do sytuacji, w której materiały pochodzące z kontroli operacyjnej mogą być wykorzystywane w sprawach dotyczących potencjalnie każdego przestępstwa. I to nie tylko popełnionego przez osobę, wobec której stosowano kontrolę. Nie jest to zgodne ze standardem konstytucyjnym i wydaje się, że narusza prawo do prywatności przez zbyt szeroki zakres możliwości ingerencji w sferę prywatności jednostki również w przypadkach niebędących przypadkami koniecznymi z punktu widzenia demokratycznego społeczeństwa. Wydaje się, że godzi to również w prawo do rzetelnego procesu sądowego wyrażone w art. 6 EKPCz. Wątpliwości wywołuje także art. 27 ust. 1 pkt 1 w zw. z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW oraz AW[52]. Na podstawie tych przepisów ABW może prowadzić kontrolę operacyjną w celu rozpoznawania, zapobiegania i wykrywania (…) *innych przestępstw godzących w bezpieczeństwo państwa*. W polskim porządku prawnym nie istnieje jednak żaden katalog przestępstw godzących w bezpieczeństwo państwa, nie formułuje go również doktryna ani orzecznictwo, przez co w danej sprawie interpretacji dotyczącej zaliczenia danego przestępstwa do przestępstw wyżej wymienionych dokonuje ABW. Jest to naruszenie wymogów co do jakości prawa, określonych w orzecznictwie ETPCz, zwłaszcza opisanego wcześniej wymogu precyzyjności i dostępności[53].

[52] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz.U. z 2017 r. poz. 1920, ze zm.).

[53] J. Podkowik, *Privacy in the digital era – Polish electronic surveillance law declared partially unconstitutional: Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11*, „European Constitutional Law Review" 2015, t. 11 (3), s. 590–591.

W ustawie muszą być określone kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze, w tym również kontrola operacyjna. W polskim ustawodawstwie przyjęło się regulować tę kwestię w sposób nieograniczony, co znaczy, że kontrolę operacyjną można stosować zarówno wobec osób fizycznych, jak i prawnych. Nie ma także żadnych generalnych wyłączeń dotyczących ograniczenia możliwości stosowania kontroli operacyjnej, np. wobec dziennikarzy czy obrońców[54]. Od 15 stycznia 2016 r. istnieje w ustawach zapis dotyczący mechanizmu niezwłocznego, komisyjnego i protokolarnego niszczenia materiałów stanowiących tajemnicę spowiedzi i tajemnicę obrończą, a także mechanizmu przekazywania prokuratorom przez szefów służb materiałów zawierających inne tajemnice określone w Kodeksie postępowania karnego, np. tajemnicę dziennikarską czy adwokacką. Prokuratorzy kierują te materiały do sądu z wnioskiem o dopuszczenie do ich wykorzystania w postępowaniu karnym, sąd zaś dopuszcza do wykorzystania te materiały, jeżeli jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Zmiany wprowadzone przez wykonanie wyroku TK to istotny krok naprzód, jeśli chodzi o poszanowanie tajemnic prawnie chronionych w toku kontroli operacyjnej. Wcześniej obowiązujące przepisy mogły podczas prowadzenia kontroli operacyjnej prowadzić do naruszania prawa do rzetelnego procesu, wyrażonego w art. 6 EKPCz, a nawet wolności religijnej w przypadku naruszenia tajemnicy spowiedzi, co znajduje uzasadnienie w art. 9 EKPCz i art. 53 Konstytucji RP.

Trybunał Konstytucyjny w wyroku K 23/11 stwierdził również, że jest pożądane określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków. Ustawodawca uszczegółowił wobec tego rodzaje środków stosowanych w ramach kontroli operacyjnej. Wcześniej obowiązujące przepisy wspominały jedynie ogólnie o kontrolowaniu przesyłek i treści korespondencji, a także o stosowaniu środków technicznych umożliwiających uzyskiwanie dostępu do treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.

Trybunał Konstytucyjny stoi na stanowisku, że czynności operacyjno-rozpoznawcze powinny być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie da się ich uzyskać w inny, mniej dolegliwy dla nich sposób. Problemem jest tu ponownie art. 168b kpk, ponieważ, jak już wspomniano, materiały pochodzące z kontroli operacyjnej teoretycznie mogą być obecnie wykorzystywane procesowo w każdej sprawie karnej, przez co zachodzi poważne zagrożenie nadużywania tego narzędzia przy zbieraniu materiałów niezwiązanych z pierwotną przyczyną stosowania kontroli niejako „przy okazji".

W ustawie należy określić maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek, który nie może przekraczać ram koniecznych

[54] B. Grabowska-Moroz, A. Pietryka, *Służby specjalne, policyjne i skarbowe a prawa człowieka – standardy konstytucyjne i międzynarodowe oraz kierunki niezbędnych zmian legislacyjnych*, „Raporty, Opinie, Sprawozdania", Warszawa 2016, s. 23–24.

obowiązujących w demokratycznym państwie prawa. Omawiane ustawy określają zakres czasowy kontroli, lecz pewnym wyjątkiem w tym względzie jest ustawa o ABW oraz AW, a także ustawa o SKW oraz SWW[55]. ABW i SKW nie są bowiem ograniczone czasowo w swojej działalności w ramach kontroli operacyjnej (w uzasadnionych przypadkach), w ustawach mowa jedynie o możliwości przedłużenia kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy. Takie rozwiązanie jest co prawda uzasadnione ciężarem gatunkowym spraw, w których ABW i SKW stosują kontrolę operacyjną, wydaje się jednak, że ustawodawca powinien posłużyć się w tym przypadku bardziej precyzyjnym określeniem granic czasowych stosowania kontroli. Idzie wszak o ochronę konstytucyjnie chronionego prawa do prywatności. Rzecznik Praw Obywatelskich we wniosku do TK o zbadanie zgodności regulacji dotyczących czasu stosowania kontroli operacyjnej z Konstytucją RP[56] zwrócił uwagę również na potencjalnie długi czas kontroli operacyjnej, który w wyniku ostatnich zmian może trwać nawet 18 miesięcy, co, jego zdaniem, może skutkować niedopuszczalnym ograniczeniem w zakresie korzystania z konstytucyjnych wolności i praw.

Trybunał Konstytucyjny stwierdza, że niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej zwłaszcza wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji. Na stosowanie kontroli operacyjnej zgodnie z ustawami zezwolenie wydaje sąd. Zgoda sądu na przeprowadzenie kontroli operacyjnej nie musi jednak obecnie zawierać uzasadnienia. Takie uzasadnienie sporządza się w przypadku odmowy zarządzenia lub przedłużenia kontroli operacyjnej[57]. Do wniosku skierowanego do sądu nie dołącza się także całego zgromadzonego w sprawie materiału, a jedynie materiały uzasadniające potrzebę zastosowania kontroli operacyjnej. Budzi to wątpliwości Rzecznika Praw Obywatelskich, który skierował do TK wniosek o zbadanie zgodności tejże regulacji z Konstytucją RP, a konkretnie z jej art. 45 ust.1 gwarantującym prawo do rzetelnego procesu[58]. Wątpliwości z punktu widzenia praw człowieka budzi też rozwiązanie zastosowane w tzw. ustawie antyterrorystycznej, zgodnie z którą kontrola operacyjna prowadzona wobec cudzoziemca w sprawach rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym nie wymaga zgody sądu na etapie wszczęcia. Kontrolę operacyjną zarządza tu samodzielnie szef ABW.

Konieczne jest również precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych. Obecnie

[55] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: Dz.U. z 2017 r. poz. 1978, ze zm.).

[56] Postępowanie toczy się pod sygnaturą K 9/16.

[57] Tak stanowi załącznik nr 1 do *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 czerwca 2011 r. w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów* (Dz.U. z 2011 r. nr 122 poz. 697). To rozporządzenie uznano wprawdzie za uchylone 15 stycznia 2016 r. wraz z uchwaleniem ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, jednak do tej pory nie wprowadzono nowej regulacji.

[58] Postępowanie toczy się pod sygnaturą K 32/15.

zbędne i niedopuszczalne dane niszczy się niezwłocznie, komisyjnie i protokolarnie, co wydaje się czynić zadość temu wymogowi. Ponadto TK zauważa, że należy zagwarantować bezpieczeństwo zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów. Odpowiednim rozwiązaniem w tym względzie może być np. ustanawianie przez służby specjalnych pełnomocników ds. przetwarzania danych osobowych.

Zdaniem TK niezbędne jest unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie – na wniosek zainteresowanego – poddania sądowej ocenie legalności zastosowania tych czynności, a odstępstwo jest tu dopuszczalne wyjątkowo. Obecnie ten standard w praktyce nie jest realizowany. Zasadą jest bowiem, że osobie, wobec której kontrola operacyjna była stosowana, nie udostępnia się materiałów zgromadzonych podczas trwania tej kontroli. Prawo do zaznajomienia się z tymi materiałami ma jedynie podejrzany w danej sprawie i jego obrońca, kiedy jest zamykane śledztwo, o czym mówi art. 321 kpk. Dopiero w tym momencie podejrzany może z całą pewnością uzmysłowić sobie, że był inwigilowany. Inne osoby, wobec których stosowano kontrolę operacyjną, nie mają obecnie nawet możliwości zasięgnięcia jakiejkolwiek oficjalnej informacji na ten temat, nie mówiąc już o możliwości poddania ocenie legalności zastosowanej kontroli sądowej. Jedynym instrumentem zakwestionowania legalności kontroli operacyjnej, leżącym w gestii inwigilowanych osób, pozostaje powództwo o ochronę dóbr osobistych, przy założeniu, że powód dysponuje informacjami uprawdopodobniającymi nielegalne pozyskiwanie danych[59].

Stosowanie czynności operacyjno-rozpoznawczych przez poszczególne organy władzy publicznej powinno odbywać się w sposób transparentny, co ma się przejawiać w publicznej jawności i dostępności zagregowanych danych statystycznych o liczbie i rodzaju stosowanych czynności operacyjno-rozpoznawczych. Obecnie sprowadza się to do przedstawiania Sejmowi i Senatowi przez prokuratora generalnego jawnej, rocznej informacji o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli, a także do corocznego przedstawiania Sejmowi i Senatowi przez ministra właściwego do spraw wewnętrznych informacji dotyczących stosowania kontroli operacyjnej przez Policję.

Trybunał Konstytucyjny nie wyklucza zróżnicowania intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się w zależności od tego, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne. Zróżnicowanie 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. Ma to obecnie miejsce na gruncie tzw. ustawy antyterrorystycznej, w której – w ramach walki z przestępstwami o charakterze terrorystycznym – kontrolę operacyjną w stosunku do cudzoziemca zarządza szef ABW i czyni

[59] B. Grabowska-Moroz, A. Pietryka, *Służby specjalne, policyjne i skarbowe*…, s. 26–27.

to bez weryfikacji przez sąd. Zdaniem TK to zróżnicowanie nie może jednak prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności oraz praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich. Założeniem wyjściowym jest także jednakowy standard ingerencji w konstytucyjne wolności oraz prawa bez względu na to, czy ich podmiot ma obywatelstwo polskie. Z tego też względu art. 37 ust. 2 Konstytucji RP, mówiący o możliwości różnicowania korzystania z konstytucyjnych wolności i praw w odniesieniu do cudzoziemców, nie wyłącza zastosowania omawianego już w niniejszej pracy art. 31 ust. 3 Konstytucji RP. W tym artykule zawarto ogólną podstawę do ograniczania konstytucyjnych wolności i praw. W świetle powyższego rozwiązanie, które znalazło się w tzw. ustawie antyterrorystycznej, wydaje się być nie do zaakceptowania.

## 5. Środki kontroli niejawnej jednostki w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka

Europejski Trybunał Praw Człowieka zawarł podstawowe zasady dotyczące stosowania podsłuchu w wyroku Valenzuela Contreras przeciwko Hiszpanii[60]. Odwołując się do swoich wcześniejszych orzeczeń, Trybunał wskazał, że przechwytywanie rozmów telefonicznych jest ingerencją w prawo jednostki do poszanowania życia prywatnego i korespondencji ze strony władzy publicznej. Taka ingerencja będzie naruszeniem art. 8 EKPCz, jeśli nie jest zgodna z prawem, nie realizuje celu prawowitego, a także nie jest konieczna w społeczeństwie demokratycznym. Zgodność z prawem oznacza przede wszystkim wymóg, aby kwestionowany środek kontroli miał podstawę w prawie krajowym. Nie oznacza to jedynie wymogu istnienia takiej podstawy w prawie krajowym, ale odnosi się także do jakości tego prawa, które musi być kompatybilne z zasadą rządów prawa. Implikuje to konieczność istnienia w prawie krajowym środka ochrony prawnej przeciw arbitralnej ingerencji władzy publicznej w prawa chronione przez art. 8 EKPCz.

Trybunał wskazał, że ryzyko arbitralnej ingerencji jest szczególnie wysokie, kiedy władza publiczna działa w sposób niejawny. W kontekście tajnych środków inwigilacji stosowanych przez władze publiczne wymóg przewidywalności wpływa na prawo krajowe w taki sposób, że musi ono być wystarczająco jasne, aby odpowiednio wskazywało obywatelom okoliczności i warunki, w jakich władze publiczne mogą zastosować wobec nich środki inwigilacji o charakterze niejawnym. Istotne jest, aby zasady w tej materii były jasne i szczegółowe, zwłaszcza gdy weźmie się pod uwagę zachodzący nieustannie postęp technologiczny. Polski ustawodawca dostosował się do tego postulatu i znowelizował ustawy w zakresie rodzajów środków stosowanych w ramach kontroli operacyjnej, uszczegóławiając ich katalog.

W celu uniknięcia nadużycia władzy w ustawie powinny znaleźć się gwarancje minimalne. Takimi gwarancjami jest po pierwsze zawarcie w ustawie definicji kategorii osób, wobec których można zastosować podsłuch. Polskie ustawy w odniesieniu do kontroli operacyjnej nie zawierają takiej definicji. Po drugie ustawa musi wymieniać

[60] Wyrok ETPCz z 30 lipca 1998 r. w sprawie Valenzuela Contreras przeciwko Hiszpanii, skarga nr 27671/95.

przestępstwa, które mogą być podstawą stosowania podsłuchu, regulować limit czasowy jego stosowania, a także procedurę sporządzania raportów dotyczących przechwyconych rozmów. Wątpliwości budzi omawiany wcześniej zakres czasowy stosowania kontroli operacyjnej przez ABW i SKW. Po trzecie muszą istnieć środki ostrożności podejmowane w celu przekazania sędziemu i obronie całości materiału pochodzącego z podsłuchu w stanie nienaruszonym. W Polsce sąd i obrona, niestety, mają dostęp tylko do części tego materiału. Dla przykładu sędzia na etapie przedłużania kontroli operacyjnej zapoznaje się jedynie z materiałami uzasadniającymi takie przedłużenie, obrona natomiast na etapie zamknięcia śledztwa ma do czynienia jedynie z materiałami wprowadzonymi do postępowania. Po czwarte zaś ustawa musi zawierać przesłanki, po których spełnieniu materiały pochodzące z podsłuchu muszą być zniszczone, szczególnie gdy doszło do umorzenia śledztwa lub uniewinnienia przez sąd. Polski ustawodawca ostatnią nowelizacją omawianych w pracy ustaw dodał przepisy nakazujące niezwłoczne, komisyjne i protokolarne niszczenie materiałów pochodzących z kontroli operacyjnej, w przypadku gdy zawierają informacje objęte bezwzględnymi zakazami dowodowym i nie zawierają dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania. Można w tym upatrywać realizację wyżej wymienionej zasady.

Trybunał w sprawie Ekimdzhiev przeciwko Bułgarii[61], odnosząc się do bułgarskiej ustawy o specjalnych środkach kontroli, wskazał, że nieinformowanie osób objętych takimi środkami, jak podsłuch, podczas prowadzenia kontroli niejawnej, a nawet po jej zakończeniu, nie może prowadzić do konkluzji, że ingerencja w życie prywatne jednostki nie była uzasadniona zgodnie z art. 8 ust. 2 EKPCz, ponieważ to właśnie nieświadomość danej osoby o zastosowaniu wobec niej podsłuchu gwarantuje jego skuteczność. Odpowiednia informacja o zastosowaniu podsłuchu powinna jednak zostać dostarczona zainteresowanym osobom z chwilą, gdy taka informacja nie narazi na szwank celu, dla którego zastosowano podsłuch. Taka informacja powinna być dostarczona już po zakończeniu kontroli niejawnej. Bułgarska ustawa, podobnie zresztą jak obecnie polskie ustawy, nie przewiduje wymogu informowania o tym właśnie fakcie osób objętych podsłuchem. Skutkuje to tym, że osoby objęte podsłuchem nie mają możliwości dowiedzenia się o stosowaniu wobec nich tego środka ani nie mogą dochodzić zadośćuczynienia za bezprawną ingerencję w ich życie prywatne ze strony władzy publicznej, chyba że te osoby są po takiej kontroli niejawnej stawiane w stan oskarżenia lub nastąpił wyciek informacji. Trybunał uznaje taki stan rzeczy za brak ważnego zabezpieczenia przed niewłaściwym wykorzystaniem środków kontroli niejawnej przez władzę publiczną.

W sprawie Drakšas przeciwko Litwie[62] Trybunał zwrócił uwagę na konieczność ochrony materiałów pochodzących z niejawnych podsłuchów przed wyciekiem na zewnątrz. Podmioty przetwarzające i przechowujące takie materiały są odpowiedzialne

[61] Wyrok ETPCz z 28 czerwca 2007 r. w sprawie Association for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii, skarga nr 62540/00.

[62] Wyrok ETPCz z 31 lipca 2012 r. w sprawie Drakšas przeciwko Litwie, skarga nr 36662/04.

za utrzymanie poufności informacji uzyskanych w drodze kontroli niejawnej. Brak ochrony poufności takich informacji i na przykład ich wyciek do mediów, a tym samym ich rozpowszechnienie, może skutkować naruszeniem art. 8 EKPCz.

W sprawie Dragojević przeciwko Chorwacji[63] ETPCz wskazał, że użycie środków kontroli niejawnej powinno ograniczać się do przypadków, w których istnieją rzeczywiste przypuszczania, że dana osoba dopuściła się planowania lub popełnienia poważnych przestępstw. Takie środki powinny też być zarządzane tylko wtedy, kiedy istotnych okoliczności w sprawie nie da się ustalić za pomocą innych metod albo jeśli byłoby to poważnie utrudnione. Wszystko to daje gwarancję istnienia odpowiedniej procedury zapewniającej brak możliwości użycia podsłuchu w sposób bezprawny i bez odpowiedniego uzasadnienia.

W sprawie Zakharov przeciwko Rosji[64] Trybunał poddał kompleksowemu badaniu rosyjskie przepisy dotyczące stosowania podsłuchu. Trybunał stwierdził, że na etapie zarządzania i prowadzenia kontroli niejawnej, kiedy osoba nią objęta nie ma o tym wiedzy, zasadnicze znaczenie powinno się przypisać temu, aby procedury dawały odpowiednie gwarancje ochrony praw tej osoby bez jej udziału. Taka osoba bowiem na tym etapie nie jest w stanie dochodzić żadnego skutecznego środka odwoławczego. Odnosząc się do charakteru przestępstw, w związku z którymi można prowadzić kontrolę niejawną, ETPCz stwierdził, że nie wymaga się wskazania w ustawie tych konkretnych przestępstw z nazwy. Wystarczy przedstawić odpowiednio szczegółowo charakter danych przestępstw, co np. na gruncie polskiej ustawy antyterrorystycznej sprowadza się do użycia sformułowania „przestępstwa o charakterze terrorystycznym", które jest wyjaśnione w polskim *Kodeksie karnym*[65] w art. 115 § 20. Kontrola niejawna może być zarządzona również w odniesieniu do osoby, która może mieć informacje o przestępstwie lub inne, istotne w sprawie. Z punktu widzenia *Konwencji* nie musi być nią objęty tylko podejrzany w danej sprawie. Skrytykowano brak wymogu natychmiastowego niszczenia danych nieistotnych dla celu, w którym je pozyskano, zdaniem Trybunału przechowywanie takich danych może naruszać art. 8 EKPCz. W Polsce wymóg natychmiastowego, komisyjnego i protokolarnego niszczenia materiałów niepozwalających na wszczęcie postępowania karnego lub niemających znaczenia dla postępowania karnego dodano nowelizacją ustaw z 2016 r. regulujących możliwość stosowania kontroli operacyjnej.

Wątpliwości Trybunału dotyczyły także rosyjskich wniosków o stosowanie kontroli niejawnej. Wykazano, że tamtejsze sądy nie otrzymywały wraz z wnioskiem żadnych materiałów uzasadniających zarządzenie takiego środka. Rosyjskie sądy zarządzały go wyłącznie na podstawie powołania we wniosku odpowiedniego czynu zabronionego, który był podstawą wszczęcia kontroli niejawnej, a jedynymi powodami nieuwzględniania takich wniosków był brak podpisu właściwej osoby, brak wskazania odpowiedniego

[63] Wyrok ETPCz z 15 I 2015 r. w sprawie Dragojević przeciwko Chorwacji, skarga nr 68955/11.
[64] Wyrok ETPCz z 4 XII 2015 r. w sprawie Zakharov przeciwko Rosji, skarga nr 47143/06.
[65] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: Dz.U. 2086 poz. 1600, ze zm.).

czynu zabronionego lub wskazanie czynu, który nie może być podstawą do wszczęcia kontroli niejawnej. Rosyjskie wnioski nie musiały także zawierać wskazania konkretnej osoby lub numeru telefonu, wobec których stosuje się podsłuch, co skutkowało przechwytywaniem wszelkiej komunikacji telefonicznej z obszaru popełnienia czynu zabronionego. Taki stan rzeczy Trybunał uznał za niedopuszczalny.

Trybunał zajął się również rolą dostawców usług telekomunikacyjnych w stosowaniu kontroli niejawnej. Zabezpieczeniem przed nadużyciami ze strony władzy publicznej jest wymóg przedstawienia takim dostawcom odpowiedniego sądowego zezwolenia na prowadzenie kontroli. W Rosji dostawcy usług telekomunikacyjnych zostali prawnie zobligowani do instalacji sprzętu dającego odpowiednim służbom bezpośredni dostęp do wszelkiej komunikacji prowadzonej za pomocą telefonu komórkowego. Dostawcy zostali również zobowiązani do tworzenia baz danych zawierających informacje na temat wszystkich subskrybentów i usług im świadczonych z okresu trzech ostatnich lat, do których to baz danych rosyjskie służby miały bezpośredni, zdalny dostęp. Wspominany sprzęt instalowany przez dostawców nie rejestrował informacji o prowadzeniu wobec danego abonenta kontroli niejawnej, co uniemożliwiało wykrycie nielegalnych kontroli. Pozwalało to na obchodzenie procedury uzyskania zezwolenia na prowadzenie podsłuchu i stwarzało warunki do poważnych nadużyć.

Trybunał zauważył, że powiadamianie osób o objęciu ich kontrolą niejawną po jej zakończeniu może być w praktyce niemożliwe. Wynika to z tego, że dana działalność lub niebezpieczeństwo będące powodem stosowania kontroli niejawnej może, już po zawieszeniu jej stosowania, utrzymywać się przez lata, a nawet dekady. Dlatego też powiadomienie każdej osoby dotkniętej zawieszonym środkiem może również zniweczyć długoterminowy cel, dla którego pierwotnie zastosowano kontrolę niejawną. Może to także służyć ujawnieniu metod i pól działania służb specjalnych, a nawet zdekonspirować ich funkcjonariuszy. Odpowiednia informacja o zastosowaniu podsłuchu powinna jednak zostać dostarczona zainteresowanym osobom z chwilą, gdy taka informacja nie narazi na szwank celu, dla którego zastosowano podsłuch, o czym już wcześniej była mowa. Zwrócono przy tym uwagę, że nieistnienie skutecznego sądowego środka odwoławczego od stosowania kontroli niejawnej, w sytuacji gdy nie wszczęto przeciw danej osobie postępowania karnego albo gdy dana osoba podejrzewa, że była inwigilowana, jest brakiem ważnego zabezpieczenia przed niewłaściwym stosowaniem tego narzędzia.

W sprawie Szabó i Vissy przeciwko Węgrom[66] Trybunał, odnosząc się do nowych zagrożeń ze strony terroryzmu, wskazał, że rozwojowi metod prowadzenia kontroli niejawnej powinien także towarzyszyć jednoczesny rozwój prawnych zabezpieczeń, mających na celu ochronę poszanowania praw obywateli zawartych w *Konwencji*. Wysiłki ze strony władzy państwowej, która dąży do ograniczenia terroryzmu, przywracałyby zaufanie obywateli do organów państwowych i ich zdolności do podtrzymania bezpieczeństwa publicznego. Zostałyby one jednak zniweczone, gdyby zagrożenie ze strony terroryzmu zostało paradoksalnie

[66] Wyrok ETPCz z 12 stycznia 2016 r. w sprawie Szabó i Vissy przeciwko Węgrom, skarga nr 37138/14.

zastąpione przez zagrożenie wywołane nieograniczonymi uprawnieniami władzy do wkraczania w sferę życia prywatnego obywateli za pomocą niekontrolowanych, a jednocześnie daleko idących technik i prerogatyw. Zdaniem ETPCz w demokratycznym społeczeństwie wymóg konieczności w odniesieniu do ograniczenia prawa do poszanowania życia prywatnego przez kontrolę niejawną należy interpretować wąsko jako ścisłą konieczność zastosowania tego środka do ochrony instytucji demokratycznych. Oznacza to, że środek kontroli niejawnej może zostać uznany za zgodny z *Konwencją* jedynie wtedy, gdy jest ściśle konieczny w ujęciu ogólnym, czyli służy ochronie instytucji demokratycznych, a ponadto wtedy, kiedy jest konieczny w ujęciu szczególnym, czyli służy uzyskaniu istotnych informacji w konkretnej sprawie. Każdy środek kontroli niejawnej, który nie odpowiada tym kryteriom, będzie groził nadużyciem ze strony władzy publicznej. Odnosząc się do kontroli niejawnej w niecierpiących zwłoki sytuacjach nadzwyczajnych, w których nie jest uzasadnione występowanie o zezwolenie sądowe na zastosowanie tego środka i zarządza go sam komendant danej służby, Trybunał uznał ją za zasadną i dopuszczalną, konieczną w demokratycznym społeczeństwie ze względu na interes bezpieczeństwa narodowego, a także ochronę porządku i zapobieganie przestępczości. Kontrola niejawna zarządzona w takim trybie musi jednak podlegać sądowemu nadzorowi post factum.

Trybunał powiększa nieustannie swój dorobek orzeczniczy w omawianej materii z godną odnotowania częstotliwością. Biorąc pod uwagę kilkanaście ostatnich lat, należy zauważyć, że ETPCz zdecydowanie coraz częściej zajmuje się zagadnieniem środków kontroli niejawnej jednostki i ewentualnych naruszeń praw człowieka w ramach ich prowadzenia. Jako możliwe przyczyny takiego stanu rzeczy bez wątpienia można podać zarówno rozwój technologiczny, powodujący znaczne zwiększenie ilości dostępnych pól prowadzenia inwigilacji, jak i zwiększenie zagrożenia, np. ze strony terroryzmu islamskiego, a tym samym zwiększenie liczby prowadzonych kontroli niejawnych, z równoczesnym poszerzeniem zakresu tych kontroli. Być może mamy do czynienia ze zwiększaniem się świadomości prawnej społeczeństwa, co powinno cieszyć. Brak odpowiedniej regulacji lub też niedostateczna jej jakość może w konsekwencji prowadzić do zaistnienia stanu zagrożeń praw człowieka, szczególnie prawa do poszanowania życia prywatnego i prawa do rzetelnego procesu. Nie można przy tym jednak tracić z oczu skuteczności podejmowania środków kontroli niejawnej, wszak to właśnie wysoka skuteczność tych środków decyduje o wprowadzaniu ich do porządku prawnego. Polski ustawodawca, w celu pogodzenia tych dwóch wartości: ochrony praw człowieka i skuteczności podsłuchów, powinien skorzystać ze wskazówek w postaci standardu konstytucyjnego wyznaczonego przez Trybunał Konstytucyjny, a także bogatego orzecznictwa Europejskiego Trybunału Praw Człowieka.

## Zakończenie

Wymogi dotyczące dopuszczalności stosowania środka kontroli niejawnej, jakim jest kontrola operacyjna, zostały w systemie ochrony praw człowieka określone w sposób

szczegółowy. Istnienie każdej z opisanych wyżej przesłanek ma na celu zapewnienie, że prawa i wolności jednostki gwarantowane konstytucyjnie i konwencyjnie nie zostaną bezprawnie naruszone. Brak spełnienia którejkolwiek z tych przesłanek może skutkować zaistnieniem nadużyć ze strony władzy publicznej, a co za tym idzie naruszeniem praw jednostki. A na to nie może być zgody w demokratycznym państwie prawa.

Trybunał Konstytucyjny wydając wyrok K 23/11, dostrzegł zagrożenia płynące ze stosowania kontroli operacyjnej – zarówno te stare, do których odnosił się Europejski Trybunał Praw Człowieka w ugruntowanym orzecznictwie, jak i nowe, wynikające z technologicznego rozwoju. Ustawodawca stosując się do orzeczenia Trybunału i nowelizując tym samym ustawę o Policji oraz wiele innych ustaw w zakresie uregulowania kontroli operacyjnej, bez wątpienia poczynił krok w dobrym kierunku. Nowa regulacja wymieniająca między innymi środki niejawnego pozyskiwania informacji wykorzystywanych podczas kontroli operacyjnej, określająca maksymalny okres stosowania tej kontroli na 18 miesięcy, a także wprowadzająca obowiązek niezwłocznego, komisyjnego i protokolarnego niszczenia materiałów zbędnych dla postępowania karnego lub zawierających dane objęte bezwzględnymi zakazami dowodowymi, to wyraźne zbliżenie się krajowej regulacji do europejskich standardów ochrony praw człowieka.

Jest to jednak w dalszym ciągu tylko zbliżenie się do standardów europejskich, gdyż na obecnym etapie nie można jeszcze mówić o ich pełnej realizacji. Nie sposób bowiem nie dostrzec, że na mocy obecnie obowiązujących przepisów nadal nie informuje się oficjalnie osoby poddanej kontroli operacyjnej o tym fakcie, co ma szczególne znaczenie, kiedy ta osoba nie została następnie postawiona w stan oskarżenia i nie mogła zapoznać się z aktami sprawy. Brakuje ponadto skutecznego instrumentu ochrony prawnej przysługującego osobom poddanym nielegalnej kontroli operacyjnej. Nie istnieje definicja kategorii osób mogących podlegać kontroli, przez co nie ma możliwości podsłuchiwania każdego, kto ma choćby najmniejszy związek ze sprawą, w tym np. adwokatów czy dziennikarzy, w związku z wykonywaniem ich pracy. Sąd i obrona nie mają możliwości zapoznania się z całością materiału zebranego podczas kontroli operacyjnej, a ABW i SKW mogą dalej stosować kontrolę operacyjną właściwie bez maksymalnej granicy czasowej. Z niepokojem należy odnotować także to, że ustawodawca oprócz regulacji potrzebnych i godnych pochwały wprowadził również w ostatnim czasie do porządku prawnego przepisy, które przy stosowaniu kontroli operacyjnej wywołują wiele wątpliwości z punktu widzenia ochrony praw człowieka. Mowa tu po pierwsze o art. 168b kpk umożliwiającym wykorzystanie materiałów pochodzących z kontroli operacyjnej, zawierających dowody popełnienia przez osobę przestępstw innych niż katalogowe. Po drugie należy wskazać na przepisy tzw. ustawy antyterrorystycznej, która nie wymaga zgody sądu na zastosowanie kontroli operacyjnej wobec cudzoziemca w sprawach zwalczania przestępstw o charakterze terrorystycznym na etapie wszczęcia. Nie uwzględniono w niej również, podobnie jak w ustawach regulujących działanie ABW i SKW, górnej granicy czasowej stosowania kontroli. *De lege ferenda* taki

stan rzeczy wymaga zmian, szczególnie w zakresie zagrożeń wymienionych powyżej. W przeciwnym wypadku nietrudno wyobrazić sobie sytuację, w której w najbliższym czasie wyżej wymienione regulacje staną się przedmiotem wyroku Trybunału Konstytucyjnego, stwierdzającego ich niezgodność z Konstytucją RP albo podstawą wydania wyroku przeciwko Rzeczypospolitej Polskiej przez Europejski Trybunał Praw Człowieka.

Wyważenie interesu publicznego i interesu prywatnego jest zadaniem bardzo trudnym. Kontrola operacyjna zyskuje na swej skuteczności, kiedy jest prowadzona w sposób jak najbardziej tajny i jak najmniej ingerujący w życie prywatne. Z kolei życie prywatne jednostki jest kategorią bardzo delikatną, wyczuloną na najmniejsze nawet naruszenie, i wymaga poszanowania. Ustawodawca staje przed wyzwaniem uregulowania kontroli operacyjnej w taki sposób, aby to narzędzie było jednocześnie skuteczne i gwarantowało zakaz nieuzasadnionej ingerencji w prywatność jednostki. Te wartości pozornie wydają się być niemożliwymi do pogodzenia, jednak przy zachowaniu odpowiednich warunków opisanych w niniejszym tekście, staje się to możliwe. Równowaga, jakkolwiek trudna do osiągnięcia i czasochłonna, nie jest kategorią z dziedziny *fantasy*. Nie jest to także wyłącznie polski problem. Analiza europejskiego orzecznictwa wskazuje, że z trudnościami odpowiedniej regulacji środków kontroli niejawnej borykają się również demokracje znacznie starsze od naszej. Ważne jest przede wszystkim takie zestawienie wymienionych wyżej wartości, aby się równoważyły. Przyznanie wyraźnego pierwszeństwa celowi ochrony praw i wolności spowoduje, że kontrola operacyjna będzie nieskuteczna, a to przecież skuteczność stanowi o jej wartości. Z kolei skupianie się jedynie na zapewnieniu maksymalnej skuteczności tego środka spowoduje, że na masową skalę będą naruszane prawa człowieka, szczególnie prawo do prywatności, co jest niedopuszczalne z punktu widzenia demokratycznego państwa prawa.

**Bibliografia:**

Balcerzak M., *Prawo do poszanowania korespondencji*, w: B. Gronowska i in., *Prawa człowieka i ich ochrona*, Toruń 2010, TNOiK.

Banaszak B., *Prawa człowieka i obywatela w nowej Konstytucji Rzeczypospolitej Polskiej*, „Przegląd Sejmowy" 1997, nr 5.

Bartoszewicz M., *Komentarz do art. 49 Konstytucji Rzeczypospolitej Polskiej*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, M. Haczkowska (red.), LEX 2014.

Braciak J., *Prawo do prywatności*, w: *Prawa i wolności obywatelskie w Konstytucji RP*, Warszawa 2002, C.H. Beck.

*CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, UN Human Rights Committee (HRC), 2 XI 1999 r., CCPR/C/21/Rev.1/Add.9, http://www.refworld.org/docid/45139c394.html [dostęp: 2 III 2017].

Degórska K., *Prawo do ochrony życia prywatnego i rodzinnego*, w: *Prawa i wolności I i II generacji*, A. Florczak, B. Bolechow (red.), Toruń 2006, Adam Marszałek.

Deryng A., *Rzecznik Praw Obywatelskich jako wnioskodawca w postępowaniu przed Trybunałem Konstytucyjnym*, LEX 2014.

Grabowska-Moroz B., Pietryka A., *Służby specjalne, policyjne i skarbowe a prawa człowieka – standardy konstytucyjne i międzynarodowe oraz kierunki niezbędnych zmian legislacyjnych*, „Raporty, Opinie, Sprawozdania", Warszawa 2016, Helsińska Fundacja Praw Człowieka.

Hoc S., Szustakiewicz P., *Ustawa o CBA. Komentarz*, LEX 2012.

Kubiński K., *Ochrona życia prywatnego człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1993, nr 1.

Kudła J., *Przestępstwa katalogowe w kontroli operacyjnej*, LEX 2016.

Łabno A., *Ograniczenie wolności i praw człowieka na podstawie art. 31 Konstytucji III RP*, w: *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak,A. Preisner (red.), Warszawa 2002, C.H. Beck.

Mielnik Z., *Prawo do prywatności (zagadnienia wybrane)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2.

Mizerski R., *Limitacja korzystania z praw człowieka*, w: Gronowska B. i in., *Prawa człowieka i ich ochrona*, Toruń 2010, TONIK.

Ożóg-Wróbel K., *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, nr 4.

Piechowiak M., *Klauzula limitacyjna a nienaruszalność praw i godności*, „Przegląd Sejmowy" 2009, nr 2.

Pochodyła P., Franc S., *Kontrola operacyjna oraz zakres jej stosowania*, „Zeszyty Naukowe WSEI, seria: Administracja" 2011, nr 1.

Podkowik J., *Privacy in the digital era – Polish electronic surveillance law declared partially unconstitutional: Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11*, „European Constitutional Law Review" 2015, t. 11.

*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* UN Human Rights Council, 17 IV 2013 r., A/HRC/23/40, http://www.refworld.org/docid/51a5ca5f4.html [dostęp: 2 III 2017].

Rzucidło J., *Prawo do prywatności i ochrona danych osobowych*, w: *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, M. Jabłoński (red.), Wrocław 2014, Uniwersytet Wrocławski.

*Słownik Języka Polskiego PWN*, http://sjp.pwn.pl/sjp/kontrola;2473611.html [dostęp: 7 XI 2016].

*The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Commission on Human Rights, 28 IX 1984 r., E/CN.4/1985/4, http://www.refworld.org/docid/4672bc122.html [dostęp: 2 III 2017].

Warren S.D., Brandeis L.D., *The Right to Privacy*, „Harvard Law Review" 1890, nr 5, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [dostęp: 24 III 2017].

Wieruszewski R., *ONZ-owski system ochrony praw człowieka*, w: B. Banaszak i in., *System ochrony praw człowieka*, Kraków 2005, Wolters Kluwer.

Wojtyczek K., *Zasada proporcjonalności*, w: *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (red.), Warszawa 2002, C.H. Beck.

Woźniewski K., *Dopuszczalność wykorzystywania środków dowodowych uzyskanych za pomocą wadliwych czynności dowodowych*, „Gdańskie Studia Prawnicze – Przegląd Orzecznictwa" 2009, nr 3, LEX 2009.

Zakolska J., *Problem klauzuli ograniczającej korzystanie z praw i wolności człowieka w pracach konstytucyjnych, w poglądach doktryny i orzecznictwa Trybunału Konstytucyjnego,* „Przegląd Sejmowy" 2005, nr 5.

Zawadzka Z., *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną: Problem rozstrzygania konfliktu zasad*, LEX 2013.

**Akty prawne:**

*Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r. nr 78 poz. 483, ze zm.).

*Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, podpisana w dniu 26 czerwca 1945 r.* (Dz.U. z 1947 r. nr 23 poz. 90).

*Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r.* (Dz.U. z 1993 r. nr 61 poz. 284, ze zm.).

*Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.* (Dz.U. z 1977 r. nr 38 poz. 167).

*Powszechna Deklaracja Praw Człowieka (rezolucja Zgromadzenia Ogólnego ONZ 217/III A w dniu 10 grudnia 1948 r.)*, http://www.bb.po.gov.pl/Prawa/PNZ/PDPCZ.pdf.

*Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

*Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: Dz.U. z 2017 r. poz. 1978, ze zm.).

Ustawa *z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz.U. z 2017 r. poz. 1920, ze zm.).

*Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: Dz.U. z 2018 poz. 1600, ze zm.).

*Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: Dz.U. z 2018 r. poz. 1987).

*Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 czerwca 2011 r. w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów* (Dz.U. z 2011 r. nr 122 poz. 697).

**Wykaz orzecznictwa:**

***Orzecznictwo Europejskiego Trybunału Praw Człowieka***

Wyrok ETPCz z 26 kwietnia 1979 r. w sprawie Sunday Times przeciwko Wielkiej Brytanii, skarga nr 6538/74.

Wyrok ETPCz z 25 marca 1983 r. w sprawie Silver i inni przeciwko Wielkiej Brytanii, skarga nr 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75.

Wyrok ETPCz z 26 września 1995 r. w sprawie Vogt przeciwko Niemcom, skarga nr 17851/91.

Wyrok ETPCz z 22 października 1996 r. w sprawie Stubbings i inni przeciwko Wielkiej Brytanii, skarga nr 22083/93, 22095/93.

Wyrok ETPCz z 30 lipca 1998 r. w sprawie Valenzuela Contreras przeciwko Hiszpanii, skarga nr 27671/95.

Wyrok ETPCz z 28 czerwca 2007 r. w sprawie Association for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii, skarga nr 62540/00.

Wyrok ETPCz z 31 lipca 2012 r. w sprawie Drakšas przeciwko Litwie, skarga nr 36662/04.

Wyrok ETPCz z 15 stycznia 2015 r. w sprawie Dragojević przeciwko Chorwacji, skarga nr 68955/11.

Wyrok ETPCz z 4 grudnia 2015 r. w sprawie Zakharov przeciwko Rosji, skarga nr 47143/06.

Wyrok ETPCz z 12 stycznia 2016 r. w sprawie Szabó i Vissy przeciwko Węgrom, skarga nr 37138/14.

***Orzecznictwo Trybunału Konstytucyjnego***

Orzeczenie Trybunału Konstytucyjnego z dnia 24 czerwca 1997 r., sygn. akt K 21/96.

Orzeczenie Trybunału Konstytucyjnego z dnia 26 kwietnia 1995 r., sygn. akt K 11/94.

*Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11* (Dz.U. z 2014 r. poz. 1055).

*Wyrok Trybunału Konstytucyjnego z dnia 11 października 2006 r., sygn. akt P 3/06* (Dz.U. z 2006 r. nr 190 poz. 1409).

*Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r., sygn. akt K 32/04* (Dz.U. z 2005 r. nr 250 poz. 2116).

*Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., sygn. akt U 5/97* (Dz.U. z 1988 r. nr 67 poz. 444).

***Orzecznictwo sądów powszechnych***

Postanowienie Sądu Apelacyjnego w Lublinie z dnia 21 grudnia 2011 r., sygn. akt II AKz 611/11.

**Słowa kluczowe**: kontrola operacyjna, czynności operacyjno-rozpoznawcze, prawa człowieka, klauzule limitacyjne, prawo do prywatności.

**Keywords**: operational surveillance, operational and investigative actions, human rights, limitation clauses, right to privacy.

**Paweł Wawrzyniak**

# Ewolucja problematyki przestępczości bankowej z uwzględnieniem ważniejszych zagrożeń[1]

## 1. Aspekt bankowości klasycznej

Willie Sutton, słynny amerykański rabuś bankowy, w swojej kilkudziesięcioletniej karierze, rozpoczętej w latach 20. XX w., ukradł niemal 2 mln dolarów. Kiedy schwytało go FBI, dziennikarz zadał mu pytanie: *Willie, dlaczego okradasz banki?* Sutton udzielił odpowiedzi, później często cytowanej: *Bo są w nich pieniądze*. Choć mógł ukraść dwóm milionom ludzi po dolarze, wybrał bardziej logiczne i efektywne podejście, okradając „agregatorów waluty" (czyli banki)[2].

W Polsce każdego roku policyjne statystyki odnotowują od 100 do 200 przypadków rozboju w bankowym oddziale, a prawie co drugi sprawca tego rodzaju czynów zostaje ujęty przez organy ścigania. Pewien wzrost przestępczości bankowej przyniósł kryzys lat 2007–2011. O ile w 2009 r. odnotowano na terenie całego kraju 126 napadów rabunkowych na banki, o tyle w następnym roku zdarzyły się aż 192 tego rodzaju przypadki. Wraz z ustępowaniem zjawisk kryzysowych liczba rozbojów powróciła do wcześniejszego poziomu – w 2012 r. odnotowano jedynie 125 takich sytuacji. Warto jednak pamiętać, że w policyjnych statystykach pod pojęciem „napad na placówkę bankową" uwzględnia się również przestępstwa popełnione w agencjach i placówkach prowadzonych przez franczyzobiorców. W odniesieniu do tych ostatnich wymogi bezpieczeństwa są nierzadko obniżone w porównaniu do typowego bankowego oddziału. Właśnie takie punkty, tak samo jak oddziały dużych banków komercyjnych, zlokalizowane z reguły w niedużych miasteczkach gminnych, najczęściej padają ofiarą bandytów[3].

Przedstawione powyżej dane mają szczególne znaczenie w przypadku tzw. bankowości klasycznej (inaczej – tradycyjnej), która stawia na bezpośredni kontakt z klientem i z tego względu wymaga istnienia rozległej sieci placówek. Te placówki są jedynymi

[1] Fragment pracy magisterskiej pt. *Cyberprzestępczość i cyberterroryzm jako kluczowe zagrożenia dla bankowości cyfrowej* (Wyższa Szkoła Administracji i Biznesu w Gdyni, Wydział Prawa i Administracji). Praca zajęła II miejsce w siódmej edycji Ogólnopolskiego konkursu Szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2016/2017). Autor wykorzystał rozdział II pt. *Ewolucja problematyki przestępczości bankowej z uwzględnieniem ważniejszych zagrożeń*, rozdział III pt. *Zagrożenia cyberprzestępcze i cyberterrorystyczne w bankowości* (podrozdział 4 – *Terrorystyczny wymiar cyberprzestępczości*) oraz w zakończeniu posumowania rozdziału II, rozdziału III i fragment rozdziału I pt. *Charakterystyka ogólna podstawowych pojęć i kategorii – definicyjna operacjonalizacja terminów*.

[2] M. Goodman, *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, Gliwice 2016, s. 77–78.

[3] K.J. Mórawski, *Raport Specjalny Bezpieczeństwo: Placówki pod specjalnym nadzorem*, http://alebank.pl/raport-specjalny-bezpieczenstwo-placowki-pod-specjalnym-nadzorem/?id=57632&catid=944, s. 40 [dostęp: 8 V 2018].

kanałami dystrybucji, stąd bankowość klasyczna bywa nazywana także „jednokanałową" lub „oddziałocentryczną"[4]. Należy jednak mieć świadomość, że prawdopodobieństwo włamania do bankowych placówek terenowych lub napadu na nie będzie zawsze wyższe niż w przypadku dobrze zabezpieczonych central (i skarbców).

### 1.1. Napady i włamania do placówek bankowych

Banki są deponentami wielkich sum pieniędzy, stają się więc dość oczywistym celem ataków[5]. Napad (skok) na bank to jedno z najbardziej zuchwałych przestępstw przeciwko mieniu. Napastnicy wyposażeni w broń wystawiają zarówno siebie, jak i osoby postronne, które przypadkowo znalazły się w miejscu napadu, na śmiertelne niebezpieczeństwo. Skoki na bank są postrzegane też jako romantyczne przestępstwa wymagające iście ułańskiej fantazji. Sławni rabusie trafiają na plakaty hollywoodzkich produkcji, jak choćby Bonnie i Clyde[6]. Tego rodzaju przestępcy cieszą się również mirem i podziwem współwięźniów[7].

Oprócz napadów popularnym przestępstwem w obrębie bankowości klasycznej są włamania do placówek bankowych, które są realizowane po godzinach ich pracy. Złodzieje starają się przede wszystkim obejść zabezpieczenia techniczne banku, aby po zakończonym rabunku niepostrzeżenie oddalić się wraz z łupem. Aby zminimalizować ryzyko, złodzieje wybierają placówki, do których jest możliwe wejście np. od zaplecza (mniejsza liczba potencjalnych świadków), wcześniej przeprowadzają także ocenę wdrożonych zabezpieczeń i ich słabych stron.

Każdy bank ma własny system bezpieczeństwa, w dużym stopniu ujednolicony pod względem zasad organizacji, który jest oparty na obowiązujących regulacjach prawnych, doświadczeniach zdobytych w przeszłości, wspólnie wypracowanych standardach branżowych, dostępnych rozwiązaniach technologicznych oraz administracyjnych.

Można przyjąć, że typowy system bezpieczeństwa banku obejmuje następujące zabezpieczenia[8]:

- fizyczne (mechaniczne i budowlane),
- techniczne (elektroniczne systemy zabezpieczeń),
- personalne (pracownicy ochrony, świadomy personel banku),
- organizacyjno-prawne (procedury, instrukcje, regulaminy, podział budynku na strefy).

---

[4] Zob. J. Kroc, *Strategie dystrybucji w bankowości detalicznej według koncepcji Accenture*, w: *Wyzwania bankowości detalicznej*, Z. Jagiełło (red.), Gdańsk 2015, s. 92–93.

[5] R. Patterson, *Kompendium terminów z zakresu bankowości po polsku i angielsku*, Warszawa 2015, s. 285.

[6] Media i kultura masowa upowszechniają mit romantycznego przestępstwa bankowego nie tyko w przypadku typowych rabusiów, przestępców ściśle powiązanych z klasyczną bankowością, lecz także w stosunku do tzw. hakerów czy raczej – „bankowych cyberprzestępców", którzy stanowią zagrożenie dla bankowości elektronicznej, internetowej oraz cyfrowej. W pewnym sensie ma tutaj znaczenie kulturowy stereotyp buntownika, antysystemowego outsidera, „wolnego człowieka" stawiającego czoła systemowi wyzysku, który w powszechnym odbiorze może być kojarzony z grupami przestępców stających naprzeciw instytucji gromadzących „wielki i niedostępny kapitał". Z pewnością jest to wyobrażenie niewłaściwe i szkodliwe społecznie, chociaż dla wielu odbiorców wciąż pozostaje atrakcyjne (a nawet motywujące).

[7] R. Patterson, *Kompendium terminów*…, s. 285.

[8] P. Ornoch, *Bezpieczeństwo fizyczne i środowiskowe*, http://bs.net.pl/artykuly-nie-tylko-dla-informatykow/bezpieczenstwo-fizyczne-i-srodowiskowe [dostęp: 8 V 2018].

System bezpieczeństwa banku sprawia, że banków, z definicji, nie da się łatwo okraść. Większe zasoby gotówki są przechowywane w skarbcach bankowych z zamkiem czasowym, którego nie są w stanie otworzyć nawet członkowie personelu. Kasjerzy mają do dyspozycji niewielka ilość gotówki (jest to zazwyczaj równowartość kilkugodzinnych transakcji), a personel chronią kuloodporne szyby. W oddziałach znajdują się dodatkowo uzbrojeni strażnicy (w USA już dawno temu zaprzestano praktyki wydawania broni kasjerom). W oddziałach znajdują się ukryte systemy alarmowe, które można potajemnie uruchomić, a monitoring z reguły rejestruje przebieg zdarzeń (dlatego większość rabusiów zakłada maski)[9].

### 1.2. Ataki na zaplecze bankowości klasycznej

Bankowość klasyczną można także rozumieć szerzej. Skoro najważniejszym jej kryterium jest posiadanie rozbudowanej sieci placówek obsługi klienta (i wysoka jakość usług), to musi istnieć także odpowiednie zaplecze infrastrukturalne: centrale, oddziały i skarbce, w tym bezpieczna metoda transportu wartości pieniężnych (a także dokumentów lub mienia) realizowana przez konwojentów. To właśnie oni bywają często celem ataku przestępców, przy czym przebieg tych zdarzeń bywa bardzo brutalny, a same napady są zwykle doskonale przygotowane.

Przykładem brutalnego napadu na konwojentów może być zdarzenie z 14 marca 2013 r., kiedy to członkowie jednego z odłamów grupy mokotowskiej zaatakowali ochroniarzy Konsalnetu, którzy transportowali pieniądze od przedsiębiorców z centrum azjatyckiego w Wólce Kosowskiej. Uzbrojeni w pistolety napastnicy podbiegli do pary konwojentów i zaczęli strzelać im w plecy. Jeden z ochroniarzy dostał co najmniej trzy kule. Tyle samo pocisków trafiło jego partnerkę. Konwojenci przeżyli tylko dzięki temu, że mieli na sobie kamizelki kuloodporne. Jeden z policjantów zaangażowanych w sprawę stwierdził wówczas, że bandyci strzelali, aby zabić. Zrabowali worki skarbowe zawierające 4,2 mln zł[10].

Zawsze istnieje ryzyko rabunku wartości pieniężnych i mienia zdeponowanych w skarbcu bankowym. Jednak ze względu na wysoki poziom zabezpieczenia tego typu obiektów, jest to zadanie bardzo trudne w realizacji i – jako zagrożenie – mało prawdopodobne. Warto przywołać włamanie do skarbca oddziału Lloyds Bank, do którego doszło w 1971 r. w Wielkiej Brytanii na słynnej ulicy Baker Street[11]. Przygotowania do włamania trwały trzy miesiące. W tym czasie przestępcy musieli między innymi wykopać 15-metrowy tunel na głębokości 1,5 m, który prowadził od wynajętego sklepu pod skarbiec oddziału bankowego, przechodząc pod restauracją „Chicken Inn". Prace związane z kopaniem mogły odbywać się wyłącznie w weekendy, aby nie zdradzić podejrzanej aktywności.

[9] R. Patterson, *Kompendium terminów*…, s. 286.

[10] R. Pasztelański, *Brutalny gang oskarżony o serię napadów, w tym atak w Wólce Kosowskiej*, http://www.tvp.info/15638754/brutalny-gang-oskarzony-o-serie-napadow-w-tym-atak-w-wolce-kosowskiej [dostęp: 8 V 2018].

[11] *221B Baker Street* to adres fikcyjnej postaci Sherlocka Holmesa, detektywa, bohatera powieści i opowiadań kryminalnych sir Arthura Conana Doyle'a.

Po dotarciu na miejsce przestępcy musieli sforsować około metrowej grubości żelbetową ścianę skarbca, do czego użyli najlepszej jakości wierteł dostępnych na rynku oraz – ostatecznie – materiałów wybuchowych. Po wejściu do skarbca opróżnili ponad 260 skrytek depozytowych, w których oprócz pieniędzy znajdowała się także biżuteria, kosztowości oraz inne przedmioty[12]. Co ciekawe, utrzymywana przez nich w dniu rabunku komunikacja radiowa była podsłuchiwana i nagrywana przez Roberta Rowlandsa, radioamatora, który złożył zawiadomienie na policję. Dzięki temu – po początkowej zwłoce spowodowanej niedowierzaniem – służby policyjne mogły podjąć stosowne działania mające na celu ustalenie miejsca pobytu sprawców i ich ujęcie. Niestety, zanim udało się zlokalizować źródło transmisji radiowych, przestępcy bezpiecznie opuścili skarbiec, zabierając cały łup, który w 1971 r. oszacowano na 3 mln funtów brytyjskich[13]. Niektóre źródła sugerują, że na ścianie skarbca włamywacze pozostawili zuchwałe graffiti (potraktowane jako wyzwanie dla tych, którzy będą prowadzić dochodzenie) o treści: *Let's see how Sherlock Holmes solves this one* (*Zobaczmy, jak Sherlock Holmes sobie teraz poradzi* – tłum. aut.)[14].

### 1.3. Podstawy prawne bezpieczeństwa bankowości klasycznej

Należyte zabezpieczenie placówek bankowych nie jest wyłącznie wewnętrzną sprawą poszczególnych instytucji finansowych. W art. 5 ust. 2 pkt 1c ustawy o ochronie osób i mienia[15] sklasyfikowano banki oraz przedsiębiorstwa wytwarzające, przechowujące bądź transportujące wartości pieniężne w znacznych ilościach jako: (…) *obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa*. Również na podstawie ustawy o zarządzaniu kryzysowym[16] instytucje finansowe – w tym sektor bankowy – zostały uznane za element infrastruktury krytycznej. Wynikają z tego określone obowiązki dotyczące zabezpieczenia i ochrony wskazanych w nich obiektów[17]. Banki są zobowiązane między innymi do zapewnienia ochrony swoim obiektom i do tego celu stosują:

[12] Spekuluje się, że w skrytkach odnaleziono także pornografię dziecięcą (przestępcy mieli pozostawić ją na miejscu włamania, aby policjanci mogli podjąć właściwe działania wobec właścicieli skrytek) oraz materiały kompromitujące niektóre postacie brytyjskich elit, w tym księżniczkę Małgorzatę.

[13] R. Walsh, *The Baker Street Bank Heist*, http://www.crimemagazine.com/baker-street-bank-heist, [dostęp: 8 V 2018].

[14] P. Lashmar, *Hatton Garden ringleader Brian Reader also masterminded Lloyds Baker Street heist 45 years ago*, http://www.independent.co.uk/news/uk/crime/hatton-garden-ringleader-brian-reader-also-masterminded-lloyds-baker-street-heist-45-years-ago-a6814956.html [dostęp: 8 V 2018]. Podobna zuchwałość cechuje także niektórych cyberprzestępców, którzy wprost rzucają wyzwanie organom ścigania lub swoim oponentom, np. innym grupom cyberprzestępczym lub instytucjom. Zwykle podmieniają oni zawartość stron internetowych, wyświetlają komunikaty na ekranie komputerów przy użyciu złośliwego oprogramowania (ang. *malicious software, malware*) lub prowadzą działalność na portalach społecznościowych i w „głębokiej sieci" (ang. *deep web*). Efekty tego typu działań są bardzo zróżnicowane – od bardzo prymitywnych przekazów (obraźliwe lub ideologiczne hasła, często pisane niepoprawnym językiem) po atrakcyjne opracowania graficzne (o wymiarze wręcz propagandowym – np. dorobek grupy Anonymous, w którym odnajdziemy stosunkowo dobrej jakości filmy prezentujące konkretny, ukierunkowany przekaz).

[15] *Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* (t.j.: Dz.U. z 2018 r. poz. 2142).

[16] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j.: Dz.U. z 2018 r. poz. 1401, ze zm.).

[17] K.J. Mórawski, *Raport Specjalny*…, s. 40.

1) specjalistyczne uzbrojone formacje ochronne (tzw. SUFO)[18] lub
2) odpowiednie zabezpieczenia techniczne – pod tym pojęciem rozumie się elektroniczne urządzenia i systemy alarmowe, sygnalizujące zagrożenie chronionych osób i mienia oraz środki zabezpieczenia mechanicznego (np. sejfy).

W praktyce obydwa te elementy są stosowane łącznie[19]. Istotnym zbiorem wytycznych w zakresie uzgadniania wymaganych prawem planów ochrony dla tego typu obiektów jest także *Metodyka uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie*, opracowana przez Biuro Prewencji Komendy Głównej Policji[20]. Niektóre obiekty bankowe, np. mniejsze placówki, nie podlegają obowiązkowej ochronie, jednak Komenda Główna Policji zaleca, aby w takich przypadkach instytucje bankowe opracowały własne instrukcje bezpieczeństwa[21].

W odniesieniu do bezpieczeństwa konwojów najważniejszą regulacją jest rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne[22].

## 2. Aspekt bankowości elektronicznej

Technologie zmieniły w zasadniczy sposób oblicze banków, a szczególnie formy świadczenia usług bankowych klientom, kładąc nacisk zarówno na samoobsługę, jak i powstanie nowoczesnych kanałów dystrybucji, a także na usprawnienie pracy, co pociągnęło za sobą zwiększenia wolumenu operacji bankowych. Wprowadzenie i upowszechnienie bankomatów, telefonów, komputerów oraz kart płatniczych pociągnęło za sobą przeobrażenia rynku usług bankowych. Jednak dopiero wykorzystanie komputerów na większą skalę zmieniło całkowicie charakter bankowości. Rozpoczęła się nowa era kontaktu na linii klient–bank, zarówno w zakresie dostępu do informacji o rachunkach bankowych, jak i nowych sposobów dokonywania operacji. Stąd zarówno w teorii, jak i w praktyce pojawiło się pojęcie „bankowość elektroniczna", które jest związane z wykorzystaniem systemów informatyczno-komunikacyjnych do usprawnienia i przyspieszenia realizacji zleceń klientów banków, a tym samym przyspieszenia obiegu pieniądza bezgotówkowego[23].

Bankowość elektroniczna (inaczej *e-banking*, od ang. *electronic banking*) nie ma jednoznacznej definicji, dlatego na poziomie ogólnym zakłada się, że bankowość

[18] Służby, w tym Wewnętrzne Służby Ochrony (WSO), powołane przez określoną instytucję lub prywatne przedsiębiorstwa tworzone przez osoby, które uzyskały koncesję Ministra Spraw Wewnętrznych i Administracji na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia (i świadczą usługi na rzecz innych podmiotów). Są one uprawnione m.in. do legitymowania osób przebywających na terenie podlegającym ochronie oraz do użycia środków przymusu bezpośredniego i broni palnej. Nadzór nad SUFO sprawuje Komendant Główny Policji.

[19] K.J. Mórawski, *Raport Specjalny*..., s. 40.

[20] *Metodyka uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie*, Warszawa 2016, Komenda Główna Policji, http://www.policja.pl/download/1/219800/metodyka.pdf [dostęp: 8 V 2018].

[21] K.J. Mórawski, *Raport Specjalny*…, s. 41.

[22] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (t.j.: Dz.U. z 2016 r. poz. 793).

[23] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia*, Białystok 2011, s. 193.

elektroniczna to wszelkie nowoczesne formy działalności banków, do których są wykorzystywane urządzenia elektroniczne umożliwiające łatwy kontakt klienta z bankiem. Wywierają one silny wpływ na działalność operacyjną banków i ich organizację[24]. Ten termin po raz pierwszy pojawił się w latach 80. XX w., lecz upowszechnił się dopiero w latach 90. wraz z rozwojem bankowości internetowej[25]. Za początek oferowania klientom bankowości elektronicznej należy jednak uznać wprowadzenie przez banki w latach 60. bankomatów do wypłacania gotówki oraz dostępu telefonicznego do rachunków[26]. Cechą charakterystyczną bankowości elektronicznej, w odróżnieniu do bankowości klasycznej (jednokanałowej), jest „wielokanałowość", czyli równoległa dostępność dla klienta różnych kanałów komunikacji z bankiem. W żadnym wypadku nie oznacza to, że bankowość elektroniczna wyklucza istnienie bankowości oddziałocentrycznej, wręcz przeciwnie – może stanowić jej doskonałe uzupełnienie.

Rozwój bankowości elektronicznej na świecie nastąpił w drugiej połowie XX wieku w USA w czterech etapach[27]:

1) lata 60. to pojawienie się pierwszych bankomatów, które umożliwiły dostęp do rachunków klientów, a więc bankowość terminalowa,
2) lata 70. to dostęp do rachunków za pośrednictwem telefonu, czyli bankowość telefoniczna,
3) lata 80. to wykorzystanie komputerów do obsługi rachunków, a więc powstanie bankowości komputerowo-modemowej, czyli *home banking* (bankowość domowa) i *corporate banking* (bankowość korporacyjna),
4) lata 90. to świadczenie usług przez Internet, a więc bankowość internetowa.

Innym istotnym momentem w historii, który sprzyjał pojawieniu się bankowości elektronicznej, było wdrożenie w 1950 r. przez Bank of America pierwszego bankowego systemu komputerowego: ERMA (ang. *Electronic Recording Method of Accounting* – elektroniczna metoda zapisu księgowania)[28]. Można przyjąć, że w tym momencie technologie komputerowe na dobre zagościły w wielkich bankach.

### 2.1. Zagrożenia dla bankowych ośrodków przetwarzania danych

Wraz z pierwszymi komputerami pojawiła się potrzeba utworzenia bankowych ośrodków przetwarzania danych, OPD (inaczej – centrum danych, ang. *data center*), których lokalizacja geograficzna, standardy konstrukcyjne (projekty techniczne) oraz późniejsze procedury i plany działania (standardy utrzymaniowe) muszą zapewniać bezpieczeństwo systemom teleinformatycznym i ich danym. To bezpieczeństwo jest

[24] Tamże, s. 194.
[25] Bankowość internetowa jest odmianą bankowości elektronicznej, w której kanałem komunikacyjnym między klientem a bankiem jest sieć Internet.
[26] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia…*, s. 194.
[27] Tamże, s. 198.
[28] T.L. Morisi, *Commercial banking transformed by computer technology*, Monthly Labor Review 1996, sierpień, https://stats.bls.gov/opub/mlr/1996/08/art4full.pdf, s.30 [dostęp: 8 V 2018]; *Bank of America revolutionizes banking industry*, http://about.bankofamerica.com/en-us/our-story/bank-of-america-revolutionizes-industry.html#fbid=T4jvCWpikvv [dostęp: 8 V 2018].

rozumiane jako zapewnienie wysokiej dostępności świadczonych usług (tryb pracy 24 godziny/7 dni w tygodniu) oraz ochronę informacji wrażliwych i danych podlegających ustawowej ochronie[29]. Do dziś powstało wiele standardów technicznych (np. amerykański standard ANSI/TIA 942 *Telecommunications Infrastructure Standard for Data Centers* oraz seria norm Unii Europejskiej PN-EN 50600-1: *Technika informatyczna. Wyposażenie i infrastruktura centrów przetwarzania danych*), a także quasi-standardów (np. komercyjne wytyczne Uptime Institute[30]), które precyzują wymagania w zakresie bezpiecznej konstrukcji i eksploatacji OPD.

Zarówno w przypadku ANSI/TIA 942, jak i Uptime Institute, rozróżnia się cztery poziomy zaawansowania infrastruktury technicznej OPD, które przekładają się bezpośrednio na poziomy jej dostępności (czyli możliwości utrzymania ciągłości działania OPD w sytuacji awaryjnej, np. długotrwałego zaniku zasilania z sieci miejskiej). Te poziomy można także odnieść do wielkości konkretnego przedsiębiorstwa (np. banku), co będzie miało wpływ na projekty techniczne. Zapewnienie dostępności wymaganej dla wybranego poziomu wymusza bowiem wdrożenia konkretnych rozwiązań technicznych (patrz tabela).

**Tabela.** Wpływ wielkości biznesu na projekt OPD.

| Poziom | Charakterystyka biznesu | Wpływ na projekt OPD |
|---|---|---|
| 1 | – mała firma,<br>– ograniczona widoczność online,<br>– mała zależność od IT,<br>– niedostępność jest tolerowana | – wiele pojedynczych punktów awarii (ang. *Single Point of Failure*, SPOF) we wszystkich obszarach projektu,<br>– brak podtrzymania zasilania z agregatu prądotwórczego, zasilacz bezprzerwowy (ang. *Uninterruptible Power Supply*, UPS) podtrzymuje sprzęt IT do 8 minut,<br>– nie przetrwa 10-minutowego zaniku zasilania z sieci miejskiej |

[29] W odniesieniu do regulacji obowiązujących na terenie Polski mowa tutaj szczególnie o: tajemnicach przedsiębiorstwa (w myśl *Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*, t.j.: Dz.U. z 2018 r. poz. 419, ze zm.), danych osobowych, w odniesieniu do których ustawodawca w art. 36 *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz.U. z 1997 r. nr 133 poz. 883 (akt uchylony, obecnie obowiązuje *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*, Dz.U. z 2018 r. poz. 1000, ze zm. – dop. red.) nakłada obowiązek stosowania środków techniczno-organizacyjnych zapewniających ochronę odpowiednią do zagrożeń, a także informacjach niejawnych (na mocy *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, t.j.: Dz.U. z 2018 r. poz. 412).

[30] Uptime Institute LLC, adres witryny internetowej: https://uptimeinstitute.com/ [dostęp: 8 V 2018].

| Poziom | Charakterystyka biznesu | Wpływ na projekt OPD |
|---|---|---|
| 2 | – częściowe zyski z działalności online,<br>– wiele serwerów,<br>– telefonia krytyczna dla biznesu,<br>– duża zależność od poczty elektronicznej,<br>– limitowana tolerancja dla niedostępności | – elementy nadmiarowe w systemie chłodzenia i zasilania,<br>– podtrzymanie zasilania z agregatu prądotwórczego,<br>– przetrwa 24 godziny bez zasilania z sieci miejskiej,<br>– lokalizacja wybrana z minimalnym uwzględnieniem ryzyka otoczenia,<br>– paraizolacja,<br>– serwerownia odseparowana od innych pomieszczeń (np. UPS, magazyn, biuro) |
| 3 | – światowa obecność,<br>– większość zysków z działalności online,<br>– telefonia VoIP,<br>– wysoka zależność od IT,<br>– wysokie koszty przestoju,<br>– rozpoznawalna marka | – dwie linie zasilania (aktywna/pasywna) z sieci miejskiej,<br>– nadmiarowy system zasilania i chłodzenia,<br>– nadmiarowe łącza operatorskie,<br>– przetrwa 72 godziny bez zasilania z miasta (agregat prądotwórczy),<br>– dokładna analiza ryzyka przy wyborze lokalizacji,<br>– ogniotrwałość min. 1 godzina,<br>– możliwe prowadzenie bezprzerwowych przeglądów |
| 4 | – wielki biznes,<br>– większość zysków z transakcji elektronicznych,<br>– model biznesowy całkowicie zależny od IT,<br>– ekstremalne koszty przestoju | – dwie niezależne linie zasilania z sieci miejskiej,<br>– nadmiarowe (2N) systemy zasilania i chłodzenia,<br>– autonomia 96 godzin bez zasilania z miasta,<br>– ścisłe kryteria wyboru lokalizacji,<br>– ogniotrwałość min. 2 godziny,<br>– wysoki poziom bezpieczeństwa fizycznego i zabezpieczeń technicznych,<br>– obsada techniczna 24/7 |

Źródło: V. Avelar, *Guidelines for Specifying Data Center Criticality / Tier Levels*, http://www.apc.com/salestools/VAVR-6PHPBU/VAVR-6PHPBU_R2_EN.pdf, s. 6 [dostęp: 22 XI 2018].

Dedykowane bankowe ośrodki przetwarzania danych mogą podlegać w Polsce obowiązkowej ochronie, dlatego w obszarze bezpieczeństwa fizycznego i zabezpieczeń technicznych mają zastosowanie przede wszystkim przepisy ustawy o ochronie osób i mienia[31] oraz wytyczne zawarte w *Metodyce uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie*[32].

W odniesieniu do ośrodków przetwarzania danych – i szerzej – bankowych systemów teleinformatycznych warto przywołać przyjętą 8 stycznia 2013 r.[33] przez Komisję Nadzoru Finansowego (KNF) *Rekomendację D*[34], która dotyczy zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. Znaczenie mają również normy dotyczące bezpieczeństwa informacji ISO/IEC 27000, ISO 31000, odnoszące się do zarządzania ryzykiem, oraz ISO 22301, dotycząca zarządzania ciągłością działania.

Ze względów bezpieczeństwa zaleca się, aby OPD umieszczać w dedykowanych, zabezpieczonych budynkach, najlepiej na obrzeżach miast, w miejscach, gdzie są dostępne media (w tym stabilne źródło energii elektrycznej), możliwość łatwego dojazdu, transportu ciężkiego sprzętu. Ponadto istnieje małe prawdopodobieństwo wystąpienia ryzyka negatywnego wpływu środowiska naturalnego (np. katastrof naturalnych, klęsk żywiołowych, zagrożeń sejsmicznych lub powodzi) lub otoczenia (np. awarii technicznych, katastrof komunikacyjnych, aktów wandalizmu, ataków terrorystycznych). W przypadku gdy centrum danych znajduje się wewnątrz siedziby przedsiębiorstwa, powstają dodatkowe problemy związane z nakładaniem się dwóch różnych systemów bezpieczeństwa fizycznego (np. w naturalny sposób oczekuje się, że ulgowo potraktujemy ruch osobowo-materiałowy w pomieszczeniach biurowych budynku, a bardziej restrykcyjnie na obszarze centrum danych). Jeżeli dodatkowo OPD znajduje się w centrum miasta, pojawiają się kolejne niekorzystne uwarunkowania (np. obiekt może się znaleźć na trasie przemarszu kibiców, grup manifestantów, może wystąpić niestabilne zasilanie bądź ryzyko wpływu katastrofy komunikacyjnej). Wszelkie wspomniane zagrożenia muszą być przedmiotem dokładnej analizy ryzyka, która pozwoli podjąć decyzję o wyborze bezpiecznej lokalizacji OPD i umożliwi dostosowanie parametrów technicznych (niezawodność) oraz przyjęcie właściwych standardów w obszarze bezpieczeństwa fizycznego i zabezpieczeń technicznych (zdj. 1). Tego typu analiza musi być także okresowo ponawiana (np. w cyklu jednorocznym), gdyż charakterystyka zagrożeń na danym obszarze będzie ulegać zmianie w czasie eksploatacji obiektu.

[31] *Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* (Dz.U. z 2018 r. poz. 2142).
[32] *Metodyka uzgadniania planów ochrony….*
[33] *Przyjęcie nowej Rekomendacji D*, https://www.knf.gov.pl/aktualnosci/2013/Przyjecie_nowej_Rekomendacji_D.html [dostęp: 20 II 2017].
[34] *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf [dostęp: 8 V 2018].


**Zdj. 1.** Zabezpieczenia techniczne w OPD firmy Google (Dublin, Irlandia). Widać m.in.: płot, bramę wejściową, stanowisko ochrony, maszty z kamerami CCTV; w tle: dedykowany budynek centrum danych, w którym znajdują się pomieszczenia serwerów, techniczne i biurowe. Źródło: Google „Dublin Data Centre" (Main Entrance) Ireland, http://www.panoramio.com/photo/115851510 [dostęp: 20 II 2017].

Przy okazji omawiania tematyki bezpieczeństwa OPD należy także wspomnieć o konieczności konwojowania mienia (często wysokiej wartości[35], np. kosztownego sprzętu komputerowego) lub danych (np. zgromadzonych na nośnikach magnetycznych lub cyfrowych, w tym kopii bezpieczeństwa umieszczonych na taśmach, a także dokumentacji drukowanej) między podstawowym i zapasowym centrum danych, centralą banku lub archiwum. Konwoje – podobnie jak w przypadku transportu wartości pieniężnych – są potencjalnie narażone na napady ze strony przestępców, którzy mogą być zainteresowani zarówno kosztownym sprzętem IT, jak i danymi przewożonymi między obiektami bankowymi. Takie dane mogą być użyte do szantażu lub dalszej działalności przestępczej (w tym cyberprzestępczej).

Wszelkie nośniki danych (dokumenty i media magnetyczne lub elektroniczne), które nie muszą być przechowywane, należy dodatkowo niszczyć fizycznie (komisyjnie i zgodnie z przyjętymi procedurami). Do utylizacji należy wykorzystać odpowiedni sprzęt, np. niszczarkę do dokumentów lub dysków twardych (zdj. 2). Zniszczenie danych powinno być udokumentowane stosownym protokołem. Niewłaściwe podejście do niszczenia nośników danych może spowodować wyciek informacji, co przestępcy mogą wykorzystać do zdobycia danych osobowych lub innych informacji (np. danych finansowych,

[35] Art. 115 § 6 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: Dz.U. 2018 r. poz. 1600, ze zm.) definiuje mienie wysokiej wartości jako takie, którego: „(…) wartość w czasie popełnienia czynu zabronionego przekracza 1 000 000 złotych".

szczegółów konfiguracji systemów IT, a nawet adresów serwerów i poświadczeń pozwalających na dostęp do bankowych systemów teleinformatycznych). Takie informacje mogą być przydatne w realizacji dalszej działalności przestępczej (i cyberprzestępczej).

**Zdj. 2.** Pracownik firmy Google podczas niszczenia twardych dysków (widoczne dwie mechaniczne niszczarki).
Źródło: Kadr z filmu *Security and Data Protection in a Google Data Center*, https://www.youtube.com/watch?v=cLory3qLoY8 [dostęp: 11 V 2018].

Książkowymi przykładami naruszeń zasad bezpieczeństwa są tzw. żółte karteczki przyklejone do monitora (zawierające login i hasło użytkownika), monitory ekranowe zwrócone w stronę klientów lub okien (często jest to spowodowane niewłaściwą aranżacją powierzchni biurowej, w której nie uwzględnia się wymogów bezpieczeństwa), co pozwala na podgląd wykonywanych operacji (i ewentualny wyciek danych), dokumenty pozostawiane na biurku (zawierające dane potencjalnie przydatne przestępcom) lub wyrzucone na śmietnik (skąd mogą być łatwo pozyskane przez przestępców). Dlatego pomimo nowoczesnego charakteru bankowości elektronicznej, istnieje potrzeba sięgania do standardów bezpieczeństwa wypracowanych w bankowości klasycznej (m.in. bezpieczeństwo fizyczne). Zwykłe, ludzkie niedopatrzenie może bowiem umożliwić przestępcom rekonesans lub pozwolić na uzyskanie fizycznego dostępu do wewnętrznej sieci bankowej, a to może im ułatwić przeprowadzenie udanego ataku na systemy teleinformatyczne.

Listy zagrożeń bezpieczeństwa bankowości elektronicznej nie można ograniczyć wyłącznie do ataków mających miejsce w cyberprzestrzeni. Działalność przestępcza skierowana przeciw obiektom fizycznym (np. infrastrukturze krytycznej, OPD, konwojom) może mieć na celu: uzyskanie dodatkowych informacji, które mogą być przydatne przestępcom do przeprowadzania kolejnych ataków (także w cyberprzestrzeni), uzyskanie bezpośredniego, fizycznego dostępu do systemów teleinformatycznych (lub krytycznych elementów infrastruktury technicznej), a nawet świadome zaburzenie ciągłości działania banku (wygenerowanie strat) czy zniszczenie danych (np. ryzyko sabotażu,

działania o charakterze terrorystycznym). Z tego względu obszar bezpieczeństwa fizycznego i zabezpieczeń technicznych musi być integralną częścią systemu bezpieczeństwa, razem z obszarem cyberbezpieczeństwa. Istotne jest tu także bezpieczeństwo personelu (właściwy dobór pracowników i ich przeszkolenie) oraz pozyskiwanie sprzętu i oprogramowania z autoryzowanych, bezpiecznych źródeł.

### 2.2. Zagrożenia związane z bankomatami

Popularną odmianą bankowości elektronicznej jest bankowość dostępna za pośrednictwem samoobsługowych automatów bankowych (tzw. bankomatów). Te urządzenia służą celom informacyjnym i płatniczym. Pierwszą funkcją bankomatów była wypłata gotówki, a ich urządzenia umieszczano zazwyczaj w oddziałach banków. Jest to jedna z najstarszych form bankowości elektronicznej[36].

Pierwszy bankomat na świecie został uruchomiony przez First Pennsylvania Bank w Stanach Zjednoczonych w 1964 r., a do powszechnego użytku bankomaty zostały wprowadzone w 1969 r. w Wielkiej Brytanii. Od tego czasu bankomaty bardzo szybko się rozpowszechniały, a ich liczba stale wzrastała[37]. Pierwszy bankomat w Polsce został zainstalowany przez Bank Pekao SA w 1990 r.[38] Obecnie szacuje się, że w 2021 r. na świecie będzie zainstalowanych około 4 mln bankomatów[39]. W raporcie *How crime can undermine the convenience of cash* (*Jak przestępczość może podważyć pozycję gotówki* – tłum. aut.) opracowanym przez Wincor Nixdorf International GmbH (producenta m.in. bankomatów) zauważa się, że przecięty klient bankowości elektronicznej (użytkownik) korzysta z bankomatu (pobiera środki) średnio pięć razy w miesiącu[40]. Te statystyki mają istotne znaczenie, ponieważ każdorazowe wykorzystanie bankomatu stwarza przestępcom możliwości działania. Sieci bankomatów mogą być prywatne (należące wyłącznie do jednej instytucji) lub współdzielone, czyli tworzone i utrzymywane przez wiele instytucji finansowych, które korzystają z nich wzajemnie i dzielą się kosztami obsługi[41], co również będzie miało przełożenie na potencjalny zakres i charakter działalności przestępczej.

Rozwój bankomatów ewoluował od prostych urządzeń służących wyłącznie do wypłaty gotówki (ang. *cash dispenser*) do wieloczynnościowych bankomatów typu ATM (ang. *Automated Teller Machine*), które oprócz wypłaty gotówki umożliwiają dostęp do salda rachunku, dokonywanie przelewów, udostępniają informacje i ogłoszenia banku, a niektóre dysponują nawet funkcją depozytową (czyli mogą przyjmować gotówkę w depozyt)[42]. Do korzystania z usług za pośrednictwem bankowości terminalowej niezbędne jest wydanie klientowi przez bank karty płatniczej bądź bankomatowej oraz kodu

[36] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia…*, s. 199.
[37] Tamże, s. 200.
[38] Tamże.
[39] *Global ATM installed base to reach 4M by 2021*, https://www.atmmarketplace.com/news/global-atm-installed-base-to-reach-4m-by-2021/ [dostęp: 11 V 2018].
[40] *How can crime undermine the convenience of cash*, https://www.atmia.com/whitepapers/how-crime-can-undermine-the-convenience-of-cash/86/ [dostęp: 10 V 2018].
[41] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia…*, s. 200.
[42] Tamże, s. 199.

identyfikacyjnego (PIN). Karty mają jednak znacznie szersze zastosowanie, są bowiem wykorzystywane przede wszystkim w rozliczeniach pieniężnych. Stąd też za prostą formę bankowości terminalowej można uznać elektroniczne punkty sprzedaży tzw. POS (ang. *Point of Sale*), umożliwiające dokonywanie transakcji w punktach handlowych. Ich funkcją jest autoryzacja płatności i sprawdzenie dostępności środków[43]. Terminale POS są więc urządzeniami, które odczytują karty płatnicze i w momencie zapłaty przez klienta za towar lub usługę, łączą za pomocą sieci teleinformatycznej system informatyczny banku z kasami sieci handlowej. Terminale POS ułatwiają wszystkim punktom przyjmującym zapłatę kontakt z bankiem jako wystawcą kart płatniczych. Zatem karty płatnicze są to bezgotówkowe elektroniczne instrumenty płatnicze[44]. Zarówno z bankomatami, terminalami POS, jak i kartami płatniczymi, wiąże się także szczególny rodzaj przestępczości.

Możemy rozróżnić dwie główne kategorie ataków na ATM: fizyczne i logiczne[45]. Specyficznym rodzajem zagrożeń przestępczością powiązaną z bankomatami będą także: napad na klientów w czasie pobierania gotówki, na konwojentów w czasie ładowania bankomatu pieniędzmi lub podczas serwisu bankomatu, a także przestępstwa popełniane bezpośrednio przez pracowników ochrony lub serwisu[46].

### *Ataki fizyczne*

W ramach typowych ataków fizycznych na bankomaty należy przede wszystkim wymienić: *skimming*, przechwytywanie kart i gotówki oraz zniszczenie z użyciem ładunków wybuchowych lub w wyniku aktu wandalizmu[47]. *Skimming* pozostaje najbardziej popularnym atakiem na ATM i powoduje prawie 95 proc. wszystkich strat[48]. Na świecie znane są także kradzieże całych urządzeń[49].

*Skimming* to atak polegający na nieautoryzowanym przechwyceniu informacji zapisanych na pasku magnetycznym karty przez modyfikację sprzętu lub oprogramowania urządzenia płatniczego (np. bankomatu). Może być także realizowany przy użyciu zewnętrznego czytnika kart. *Skimming* często jest łączony z kradzieżą numeru PIN, do czego wykorzystuje się nakładki na klawiatury numeryczne lub ukryte kamery. Pozwala to na wyprodukowanie fałszywej karty.

[43] Tamże, s. 200.
[44] Tamże.
[45] *ATM Security. Explaining Attack Vectors, Defense Strategies and Solutions*, http://docplayer.net/76384265-Atm-security-explaining-attack-vectors-defense-strategies-and-solutions-an-ncr-white-paper.html, s. 2 [dostęp: 10 V 2018].
[46] Takim przykładem może być serwisant bankomatów, który znalazł sposób na włamywanie się do zaplombowanych kasetek bankomatowych. Został ujęty przez policję przy współpracy agencji ochrony, która zgłosiła sprawę, zob. *Okradał bankomaty, miast uzupełniać w nich kasę*, http://bydgoszcz.tvp.pl/13142481/okradal-bankomaty-miast-uzupelniac-w-nich-kase [dostęp: 10 V 2018].
[47] *How can crime*..., s. 4.
[48] *ATM Security*..., s. 4.
[49] Jako przykład o charakterze lokalnym może przytoczyć nieudaną kradzież bankomatu z 26 III 2016 r. w Brokowie, o czym pisał „Dziennik Bałtycki", zob. *Borkowo koło Gdańska: Skradziono bankomat. Jeden ze sprawców wciąż na wolności*, http://www.dziennikbaltycki.pl/wiadomosci/kartuzy/a/borkowo-kolo-gdanska-skradziono-bankomat-jeden-ze-sprawcow-wciaz-na-wolnosci-zdjecia-wideo,9794749/ [dostęp: 10 V 2018]. Dwóch mężczyzn przywiązało do bankomatu linę i wyrwało go, używając do tego samochodu. Swój łup załadowali na samochód i uciekli z miejsca przestępstwa. Wkrótce po zdarzeniu, w wyniku pościgu, policja ujęła jednego ze sprawców i zabezpieczyła samochód przestępców wraz ze skradzionym urządzeniem.

Skutecznym pomysłem na zmniejszenie ryzyka związanego ze *skimmingiem* jest implementacja globalnego standardu EMV (nazwa pochodzi od pierwszych liter organizacji, twórców standardu: Europay, MasterCard i Visa), który umożliwia obsługę płatności przy użyciu kart z mikroprocesorem[50]. Wydawane obecnie karty hybrydowe mają zarówno mikroprocesor, jak i pasek magnetyczny z zakodowaną informacją o tym, że karta posiada chip. Utrudnia to przestępcom używanie fałszywych kart, ponieważ użycie karty fałszywej w urządzeniu, które potrafi obsłużyć chip, wiąże się z ryzykiem wykrycia próby oszustwa. Dodatkowo wydawca karty może odmówić dokonania autoryzacji takiej transakcji. W konsekwencji wdrożenia technologii EMV sprawcy przestępstw, aby prowadzić swoją nielegalną działalność, poszukują kart, które nie działają jeszcze w technologii EMV (nie posiadają mikroprocesora) lub miejsc na świecie z urządzeniami obsługującymi tylko karty płatnicze z paskiem magnetycznym[51]. Na zdjęciu 3 przedstawiono urządzenia służące do przeprowadzania *skimmingu*. Warto zauważyć, że po ich zamontowaniu większość użytkowników bankomatu nie będzie miała najmniejszych podejrzeń i stanie się ofiarą przestępców.


**Zdj. 3.** Przykładowe urządzenia służące do *skimmingu* – zewnętrzny czytnik kart (pozwala na odczyt paska magnetycznego karty) oraz nakładka na klawiaturę (pozwala przechwycić PIN).

Źródło: V. Biryukov, *Żonglowanie kartami: Przestępstwa z wykorzystaniem bankomatów*, https://plblog.kaspersky.com/zonglowanie-kartami-dzialalnosc-przestepcza-z-wykorzystaniem-bankomatow/2565/ [dostęp: 11 V 2018].

[50] J. Biegański, *Sposoby popełniania przestępstw związanych z elektronicznymi instrumentami płatniczymi po wdrożeniu EMV*, w: *Przestępczość teleinformatyczna*, J. Kosiński (red.), Szczytno 2012, s. 19.
[51] Tamże, s. 23.

W 2014 r. organizacja European ATM Security Team (EAST)[52] zarejestrowała ponad 17 000 ataków fizycznych na około 400 000 bankomatów w Europie. Całkowite straty osiągnęły 306,5 mln euro, co oznacza wzrost o 13 proc. w stosunku do poprzedniego roku[53].

### *Ataki logiczne*

Największy wzrost i różnorodność ataków na bankomaty obserwuje się jednak w ramach ataków logicznych. Są to wszelkie ataki wykorzystujące nowoczesną technologię i mające na celu użycie podatności (czyli słabości lub luk w zabezpieczeniach), które nie były znane w momencie projektowania i produkcji konkretnych urządzeń. Od 2012 r. widoczny jest alarmujący wzrost częstości ataków logicznych na całym świecie. Tego rodzaju przestępstwa pozwalają na zaatakowanie dużej liczby bankomatów za jednym razem. Rezultatem ataku może być kradzież całej gotówki z urządzeń ATM, co w bardzo krótkim czasie jest w stanie spowodować znaczne straty finansowe. Ataki logiczne można podzielić na dokonywane z użyciem[54]:

1) tzw. czarnych skrzynek *(*ang. *black box)* – dedykowanych urządzeń, które podłączone do urządzenia ATM dają przestępcy możliwość ominięcia układu kontroli dyspensera gotówki i mogą zmusić bankomat do wypłaty (czarna skrzynka może być kontrolowana zdalnie z użyciem smartfona),
2) złośliwego oprogramowania (ang. *malicious software*, w skrócie – *malware*) działającego w sieci bankomatów, które pozwala przechwycić komunikację między urządzeniem ATM a komputerem głównym i umożliwia atakującemu wypłatę gotówki,
3) złośliwego oprogramowania zainstalowanego na twardym dysku urządzenia ATM – takie oprogramowanie może przejąć kontrolę nad bankomatem i dokonać nieautoryzowanej wypłaty gotówki.

Na zdjęciu 4 przedstawiono urządzenie typu „czarna skrzynka" podłączone do bankomatu za pomocą kabla USB. Wykorzystano tutaj powszechnie dostępną i tanią platformę Raspberry Pi model B (opracowaną do celów edukacyjnych przez Raspberry Pi Foundation[55]), na której jest możliwe zainstalowanie m.in. systemu operacyjnego GNU/Linux (np. Raspbian). Koszt całości bez oprogramowania do atakowania bankomatu wynosi ok. 200 zł (system operacyjny jest dostępny za darmo).

[52] European ATM Security Team (EAST), adres witryny internetowej: https://www.association-secure-transactions.eu/ [dostęp: 10 V 2018].
[53] *How can crime…*, s. 3.
[54] *ATM Security…*, s. 8–11.
[55] Raspberry Pi Foundation, witryna internetowa: https://www.raspberrypi.org/ [dostęp: 10 V 2018].

**Zdj. 4.** „Czarna skrzynka" (urządzenie w przezroczystej obudowie) podłączona do bankomatu.

Źródło: Kadr z filmu *Jackpotting an ATM with a black box*, https://www.youtube.com/watch?v=3HYA0MvizpM [dostęp: 11 V 2018].

W 2014 r. EAST, już po odkryciu pierwszych ataków na bankomaty z użyciem złośliwego oprogramowania w Europie Zachodniej, zebrała dane i opublikowała pierwsze statystyki. Poinformowano o 51 incydentach, które z powodu nieautoryzowanych wypłat spowodowały straty w wysokości 1,23 mln euro[56].

### 2.3. Zagrożenia związane z bankowością internetową

Istotną odmianą bankowości elektronicznej jest bankowość internetowa, która pojawiła się w USA w połowie lat 90. XX w. Pionierami bankowości internetowej w Europie były banki skandynawskie. W Polsce, w 1998 r., bankowość internetową zaoferował jako pierwszy Powszechny Bank Gospodarczy w Łodzi, który został następnie przejęty przez Bank Pekao SA. Bankowość internetowa szybko zyskała dużą popularność wśród klientów i stała się podstawowym standardem w instytucjach finansowych na całym świecie, w ramach obsługi klientów masowych[57]. Wpływ miało upowszechnienie się Internetu, w tym usług stałego dostępu do sieci.

Bankowość internetowa stwarza wiele możliwości i przynosi korzyści zarówno dla klientów, jak i dla samych banków. Z punktu widzenia banku istotna jest szansa stałego wzrostu liczby klientów, rozmiar tego rynku jest bowiem równoznaczny z liczbą użytkowników Internetu na całym świecie, podczas gdy tradycyjne oddziały banku ograniczają się do liczby potencjalnych klientów zamieszkujących w pobliżu. Korzystanie przez klientów z usług bankowych za pośrednictwem Internetu charakteryzuje się też niskim stopniem skomplikowania, zapewnia dużą oszczędność czasu i możliwość

[56] *How can crime*…, s. 3.
[57] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia*…, s. 207.

dokonywania zleceń przez całą dobę[58]. Jeżeli wziąć pod uwagę rozmiar rynku oraz charakterystykę usług bankowych w Internecie, który znosi ograniczenia fizyczne związane z klasyczną bankowością, czyli z czasem (dostępność w trybie 24/7) i miejscem (zleceń można dokonywać z każdego miejsca na świecie, w którym mamy połączenie z Internetem), to łatwo zrozumieć motywację cyberprzestępców. Atak może być przeprowadzany w dowolnym czasie i miejscu, łatwiej także ukryć swoją działalność.

Podstawowym czynnikiem ograniczającym rozwój bankowości internetowej pozostaje bariera bezpieczeństwa, ponieważ klienci obawiają się możliwości dokonywania operacji na ich rachunkach przez osoby trzecie. Zagrożenia bezpieczeństwa mogą być wynikiem błędu ludzkiego, nieprawidłowego działania sprzętu, oprogramowania, a także działalności przestępczej. Wśród rozlicznych źródeł zagrożeń wymienia się między innymi[59]:

1) łamanie haseł dostępu,
2) oszukiwanie zabezpieczeń, ich obejście lub też zneutralizowanie,
3) wykorzystywanie luk w zabezpieczeniach,
4) przechwytywanie otwartych połączeń sieciowych,
5) blokowanie usług,
6) wirusy komputerowe,
7) inne.

Ograniczenie zagrożeń wymaga stworzenia złożonej i kompleksowej architektury bezpieczeństwa. Wymaga to uwzględnienia szerokiej gamy czynników, takich jak: bezpieczeństwo fizycznego dostępu do systemów informatycznych (patrz wcześniej omówione kwestie związane z bezpieczeństwem ośrodków przetwarzania danych), określenie procedury wielopoziomowych zabezpieczeń dostępu personelu do systemów (istotną sprawą są możliwe naruszenia i przestępstwa, których źródłem są pracownicy banku – zarówno obszaru biznesowego, jak i IT), kontrola nadzorcza, możliwy wpływ klęsk żywiołowych lub katastrof, a także bezpieczeństwo logiczne, czyli bezpieczeństwo samych komputerów i przechowywanych danych (np. ochrona antywirusowa, szyfrowanie dysków twardych). Do zwiększenia bezpieczeństwa przyczyniają się tzw. systemy *audit log*, pozwalające na pełny zapis, kto i w jakim celu miał dostęp do systemu[60].

W celu ochrony pieniędzy i danych klientów banki muszą stosować różnorodne zaawansowane rozwiązania, gdyż włamania do ich systemów informatycznych powodują straty nie tylko finansowe, lecz także utratę zaufania do tej instytucji. Stąd banki są zmuszone do zwiększania nakładów ponoszonych na zapewnienie bezpieczeństwa systemów informatycznych[61]. Wydaje się więc, że w przypadku spektakularnego ataku, konsekwencją dla banku jako instytucji zaufania publicznego[62] będzie utrata reputacji.

[58] Tamże, s. 207–208.
[59] Tamże, s. 214.
[60] Tamże.
[61] Tamże.
[62] Zaufanie publiczne – zaufanie pochodzące od ogółu, usankcjonowane powszechnym przeświadczeniem; z reguły wzmacniane i gwarantowane przez państwo w drodze rozwiązań prawnych i administracyjnych.

W Polsce największym problemem użytkowników bankowości elektronicznej, w tym internetowej, jest brak zaufania. Banki muszą uświadamiać klientów, jak wielką rolę w zapewnianiu bezpieczeństwa podczas przeprowadzania operacji drogą elektroniczną odgrywają sami klienci (np. udostępnianie hakerom[63] swoich danych i haseł za pomocą fałszywych odnośników czy podstawionych stron WWW[64]). To oznacza, że zaufanie do bankowości elektronicznej to nie tylko stosowane przez banki rozwiązania w zakresie bezpieczeństwa, lecz także przekonanie klientów, że potrafią korzystać z niej w sposób prawidłowy i bezpieczny[65].

Jednak bankowość elektroniczna dotyczy nie tylko kontaktu samego klienta z bankiem w zakresie płatności, lecz także całego systemu płatności, a więc i rozliczeń międzybankowych. W wyniku postępu technologicznego powstały elektroniczne systemy płatności zarówno wewnątrz poszczególnych krajów, jak i na arenie międzynarodowej. Takim przykładem jest np. Stowarzyszenie na rzecz Światowej Międzybankowej Telekomunikacji Finansowej (ang. Society for Worldwide Interbank Financial Telecommunication, SWIFT), które znacznie przyspieszyło przekaz środków pieniężnych i informacji niezbędnych do przeprowadzania rozliczeń[66]. Ta zmiana technologiczna oznacza, że bankowość elektroniczna (zwłaszcza w swojej internetowej odmianie) stała się podatna na ataki cyberprzestępców i cyberterrorystów, których działania mogą mieć zasięg globalny. Co więcej, banki, będąc częścią ogólnoświatowego systemu finansowego, stały się także narażone na działania związane z cyberwojną[67].

W 2016 r. doszło do ataków na system bankowy SWIFT, które przeprowadzali hakerzy (ang. *black hats*) z grupy Lazarus. Prawdopodobnie jest to grupa pochodząca z Korei Północnej, działająca na zlecenie administracji Kim Dzong Una. Przypuszcza się, że łączne straty spowodowane ich działalnością przekraczają 100 mln dolarów. Według ekspertów z BAE Systems hakerzy odpowiedzialni za ataki na systemy bankowe SWIFT chcieli, aby uznano ich za rosyjskich przestępców. Po analizie złośliwego oprogramowania okazało się, że umieszczone tam teksty w języku rosyjskim zostały przełożone za pomocą tłumacza online[68].

### 3. Aspekt bankowości cyfrowej

Najpopularniejszą odmianą bankowości wciąż pozostaje bankowość elektroniczna ze swoją internetową odmianą. Banki mają jednak świadomość konieczności szybkiego

[63] Tutaj w sensie: cyberprzestępcom, tzw. czarnym kapeluszom.
[64] Jest to tzw. *phishing*.
[65] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia…*, s. 215.
[66] Tamże, s. 195–196.
[67] W literaturze przedmiotu jako pierwszy przejaw cyberwojny podaje się często cyberataki z 27 IV 2007 r. skierowane przeciw m.in. instytucjom rządowym, mediom i bankom w Estonii. Estoński premier Andrus Ansip miał być przekonany, że przynajmniej za częścią tych cyberataków stała Rosja, a na terenie jego kraju testowano nowy rodzaj konfliktu – wojnę cybernetyczną, zob. *Na Estonii testowano wojnę cybernetyczną*, https://www.wprost.pl/107407/ [dostęp: 10 V 2018]. Należy jednak podkreślić, że te informacje nigdy nie zostały całkowicie potwierdzone, a żadna ze stron nie wypowiedziała formalnie wojny drugiej stronie. W rzeczywistości oznacza to, że mieliśmy do czynienia nie z cyberwojną, ale z cyberkonfliktem.
[68] T. Fastyn, *Ataki na system SWIFT. Operacja pod fałszywą flagą?*, http://www.cyberdefence24.pl/551844,ataki-na-system-swift-operacja-pod-falszywa-flaga [dostęp: 10 V 2018].

adaptowania się do wymagań swoich klientów. Obecnie zwraca się uwagę na postępującą tzw. transformację cyfrową banków, która ma doprowadzić do powstania bankowości cyfrowej. Warto zastanowić się, skąd w ogóle pomysł na cyfryzację banków? Czy obecna postać bankowości elektronicznej, możliwość kontaktu z bankiem przez Internet nie powinny nam wystarczyć?

Analizy przeprowadzone przez Accenture, globalną firmę świadczącą usługi z zakresu konsultingu, nowoczesnych technologii i outsourcingu, wykazały, że instytucje finansowe powinny wyjść naprzeciw oczekiwaniom starzejącej się części społeczeństwa, a jednocześnie otworzyć się na potrzeby młodego pokolenia tzw. millennialsów (osób urodzonych w latach 1980–1995). Wymaga to dokonania rewizji oferty produktowej, modeli dystrybucji, a także przejścia cyfrowej transformacji. Najważniejsza jest jednak taka zmiana w wizji i misji, aby to klient został postawiony w centrum wszystkich działań i operacji banków[69]. Wydaje się, że każda zmiana zachodząca w obrębie bankowości zawsze była podporządkowana potrzebom klientów, jednak w ostatnim czasie banki spotykają się z zarzutem zbyt wolnej reakcji na potrzeby rynku, przesadnej formalizacji i zajmowania się samymi sobą.

Prezes PKO BP Zbigniew Jagiełło tłumaczy potrzebę transformacji cyfrowej banków w następujący sposób:

> Na rynek wchodzą pokolenia klientów o nowych, cyfrowych nawykach, nieobciążonych przywiązaniem do marek, a jednocześnie traktujących urządzenia mobilne jako immanentny element swojej codzienności, służący zaspakajaniu zarówno tych podstawowych, jak i bardziej wyrafinowanych potrzeb życiowych. Ze smartfonem lub tabletem w ręce, gdziekolwiek się znajdują, mogą zrobić zakupy, obejrzeć ulubiony serial, podzielić się ze światem przemyśleniami po lekturze najmodniejszej książki sezonu (oczywiście w wersji cyfrowej), kupić polisę ubezpieczeniową na chwilę przed wyjazdem na egzotyczny urlop, czy wreszcie zaciągnąć pożyczkę gotówkową na jego opłacenie. Tej łatwości w nabywaniu produktów i usług klient z cyfrowego pokolenia Y, zwany potocznie millennialsem, oczekuje także od banku. Jeśli jej nie otrzymuje, z łatwością i bez sentymentów skłonny jest zaspokoić swoje potrzeby u konkurencji[70].

Ten aspekt podkreśla także Jarosław Kroc, prezes polskiego oddziału Accenture. Stwierdził on:

> Można zaryzykować tezę, że pokolenie millennials już nie musi korzystać z produktów bankowych. To banki potrzebują ich jako klientów. Oni nie muszą przychodzić do oddziału po konto – mają Google Wallet, a za chwilę też rozwiązanie od Facebook. Płatności online realizują przez systemy PayPal, PayU, mobilny SkyCash lub wirtualnymi bitcoinami. Tak jest szybciej, wygodniej i bardziej intuicyjnie[71].

[69] J. Kroc, *Strategie dystrybucji*…, s. 91.
[70] Z. Jagiełło, *Bankowość detaliczna w obecnych warunkach rynkowych. Kierunki rozwoju*, w: *Wyzwania bankowości detalicznej*, Z. Jagiełło (red.), Gdańsk 2015, s. 9.
[71] J. Kroc, *Strategie dystrybucji*…, s. 94.

Mając na uwadze potrzeby nowej grupy klientów (millennialsów), nie można jednak zapomnieć o pozostałych odbiorcach usług bankowych, którzy będą preferować inne, bardziej klasyczne kanały komunikacji z bankiem, choćby bankowość terminalową, internetową czy osobisty kontakt z doradcą w lokalnej placówce banku. Bankowość cyfrowa, przynajmniej w założeniu, nie powinna stwarzać ryzyka cyfrowego wykluczenia części społeczeństwa (np. osób starszych).

Firma Accenture zwraca uwagę, że transformacja cyfrowa banków jest procesem wieloetapowym. Wyróżnia jej trzy aspekty[72]:

1) koncentracja na kliencie (ang. *Customer Centricity*),
2) opracowanie nowych modeli biznesowych (ang. *New Business Models*),
3) dystrybucja omnikanałowa (ang. *Omnichannel Distribution*).

Właśnie dystrybucja omnikanałowa będzie stanowić istotne wyzwanie z punktu widzenia bezpieczeństwa bankowości w najbliższym czasie. Zbigniew Jagiełło tłumaczy jej istotę w taki sposób:

> Duże zróżnicowanie grup klientów powoduje, że coraz istotniejszym wyzwaniem jest zachowanie ich lojalności wobec banków. W zakresie dystrybucji wydaje się, że optymalny model powinien dążyć do omnikanałowości. To zupełnie inna kategoria niż wielokanałowość. Kluczem do sukcesu nie jest bowiem równoległe, niezależne funkcjonowanie różnych kanałów, ale takie ich sprzężenie, by się wzajemnie przenikały i uzupełniały. Dzięki temu klient zyska swobodę wyboru i gwarancję jednakowego standardu obsługi oraz tej samej ceny produktu w każdym z dostępnych kanałów. Tak rozumiana omnikanałowość umożliwia dopasowanie miejsca, formy i czasu dotarcia do klienta z informacją, przewidywanie jego zachowań, a nawet kreowanie jego potrzeb[73].

Można przyjąć, że omnikanałowość stanowi istotę bankowości cyfrowej. Jest ona ściśle powiązana nie tylko z przenikaniem się dotychczas istniejących (i nowo powstających) kanałów komunikacji z bankiem, lecz także z adaptacją nowoczesnych technologii teleinformatycznych. W rezultacie mamy do czynienia z sytuacją, w której system bezpieczeństwa banku musi dokładnie obejmować wszystkie wykorzystywane kanały komunikacyjne (i analizować je pod kątem potencjalnych zagrożeń) – począwszy od bankowości tradycyjnej, przez elektroniczną, terminalową i internetową aż po nowe obszary związane z dużą mobilnością usług cyfrowych i podatnościami nowoczesnych, często jeszcze nie do końca poznanych, technologii. Istotne tu więc będzie zjawisko przenikania się zagrożeń, w tym ryzyko ataków hybrydowych, występujących jednocześnie w wielu kanałach i wykorzystujących różne techniki i metody działania.

[72] Tamże.
[73] Z. Jagiełło, *Bankowość detaliczna*…, s. 10.

### 3.1. *Big Data*, IoT, technologie mobilne i analiza wielkich zbiorów danych

Zdaniem Zbigniewa Jagiełły omnikanałowość i *Big Data*[74] to kluczowe wyzwania technologiczne dla bankowości w najbliższych latach[75]. Czym zatem jest *Big Data*?

*Big Data* służy przewidywaniu przyszłości i odkrywaniu nowych wartości na podstawie bieżącej analizy nieustannie zwiększających się, bardzo dużych zbiorów danych. Te dane są gromadzone i przetwarzane w czasie rzeczywistym, a ich przyrost jest znaczny w stosunkowo krótkim czasie. Analizy mają prowadzić do otrzymania aktualnych wyników, których podstawą są dane bieżące, a nie historyczne. Dzięki temu można m.in. dokładniej poznać rynek i stworzyć profil klienta[76]. Taki profil nie tylko pozwala dostosować ofertę do potrzeb danego odbiorcy usług bankowych, lecz także otwiera możliwości lepszej oceny jego wiarygodności.

Marc Goodman, emerytowany policjant i ekspert w dziedzinie cyberprzestępczości, w książce pt. *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, zwraca uwagę na to, że:

> Wszyscy dookoła nas bez przerwy generują dane. Wszystkie procesy cyfrowe, czujniki, telefony komórkowe, urządzenia GPS, silniki samochodowe, badania w laboratoriach medycznych, transakcje z użyciem karty kredytowej, zamki elektroniczne w hotelach, elektroniczne świadectwa szkolne i czynności podejmowane w serwisach społecznościowych produkują dane. Smartfony przekształcają ludzi w żywe czujniki generujące potężne ilości informacji o sobie. W efekcie urodzone dzisiaj dzieci będą żyły w cieniu gigantycznego cyfrowego śladu, biorąc pod uwagę, że aż 92% niemowlaków zaistniało już w jakiś sposób w Internecie[77].

Istotna jest tutaj koncepcja tzw. IoT (ang. *Internet of Things* – Internet rzeczy), która zakłada możliwość podłączenia do globalnej sieci dowolnego, dającego się zidentyfikować urządzenia. Dotyczy to m.in. sprzętu RTV, AGD, wszelkiego rodzaju sensorów, tzw. *wearables* („urządzeń ubieranych" – tłum. aut.), budynków czy pojazdów. Eksperci z firmy Cisco szacują, że do 2020 r. na świecie będzie podłączonych do sieci około 50 mld tego typu urządzeń (za początek ery IoT uważa się lata 2008–2009, kiedy to liczba podłączonych do sieci urządzeń przekroczyła liczebność ludności)[78]. Ten obszar także będzie stanowić dla banków jedno ze źródeł pozyskiwania danych o klientach, ich nawykach konsumenckich, trybie życia, decyzjach, miejscu przebywania, ich otoczeniu itd.

---

[74] Ten termin nie ma jednoznacznej definicji – historycznie odnosi się do wielkich zbiorów danych, które są przetwarzane z użyciem nowoczesnych technologii informatycznych. Nigdzie jednak nie określono, jaka ilość danych pozwala uznać dany zbiór za *Big Data* (co można przetłumaczyć jako: „duże dane").

[75] Z. Jagiełło, *Bankowość detaliczna…*, s. 7.

[76] M. Graczyk-Kucharska, *Big data koniecznością współczesnego marketingu*, „Problemy Zarządzania, Finansów i Marketingu" 2015, nr 41, s. 267.

[77] M. Goodman, *Zbrodnie przyszłości...*, s. 77.

[78] D. Evans, *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, Cisco IBSG, IV 2011, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, s. 3 [dostęp: 10 V 2018].

W ten sposób wracamy do gromadzenia i analizy wielkich zbiorów danych i ich wykorzystania dzięki rozwiązaniom mobilnym[79]. Bazy użytkowników bankowości mobilnej mają szacunkowo wzrosnąć z 0,8 mld w 2014 r. do 1,8 mld w 2019 r.[80]. W praktyce wymaga to bardzo istotnej ewolucji modeli analitycznych, zdolnych do przetwarzania niewyobrażalnie dużej ilości danych pochodzących z bardzo rożnych, nie tylko bankowych, źródeł.

Większego znaczenia nabierają więc cyberbezpieczeństwo oraz stabilność i niezawodność systemów informatycznych. Świadomość klientów w tym zakresie i ich oczekiwania wobec banków rosną z każdym rokiem, niezależnie od podziałów demograficznych oraz zasobności portfela[81]. Najważniejszym zagrożeniem będzie potencjalny wyciek danych lub nadużycia wynikające z łatwości przekraczania bariery etycznej związanej z gromadzeniem danych o klientach.

### 3.2. *Cloud computing*

Charakterystyczna dla bankowości cyfrowej jest także integracja bankowych systemów teleinformatycznych z rozwiązaniami opartymi na tzw. chmurze obliczeniowej (ang. *cloud computing*). Zgodnie z definicją proponowaną przez NIST[82] *cloud computing* to: (…) *model zakładający wszechobecny i wygodny dostęp do współdzielonej puli konfigurowalnych zasobów komputerowych (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które mogą być szybko dostarczane i zwalniane przy minimalnym zaangażowaniu kadry zarządzającej oraz interakcji z dostawcą usług*[83].

Usługi w modelu chmury obliczeniowej mogą być świadczone wewnętrznie przez własny dział IT i przy wykorzystaniu infrastruktury należącej do banku lub przez dostawców zewnętrznych (wyspecjalizowane firmy dysponujące własnymi OPD). W raporcie *Top 10 Trends in Banking 2016* przygotowanym przez firmę Capgemini zauważa się, że największe banki na świecie podwyższają poziom inwestycji w rozwiązania oparte na modelu *cloud computing*. Jednak większość z nich (70 proc. w 2014 r.) decydowało się na budowę i wykorzystanie własnych chmur obliczeniowych (tzw. chmury prywatne). Te decyzje były podyktowane bezpieczeństwem danych. Mimo to 10 proc. banków korzystało z zasobów publicznych chmur obliczeniowych (gdzie infrastruktura dostawcy była współdzielona pomiędzy wielu klientów), a 20 proc. banków – z chmur hybrydowych (czyli takich, w których dostępne są zarówno zasoby własne, jak i zewnętrzne, w zależności od potrzeb i możliwości prawno-technicznych)[84].

[79] Z. Jagiełło, *Bankowość detaliczna…,* s. 10.
[80] A. Kumar, A. Saxena, V. K. Suvarna, V. Rawat, *Top 10 Trends in Banking in 2016*, https://www.capgemini.com/wp-content/uploads/2017/07/banking_top_10_trends_2016.pdf, s. 12 [dostęp: 10 V 2018].
[81] Z. Jagiełło, *Bankowość detaliczna…*, s. 10.
[82] National Institute of Standards and Technology, NIST (Narodowy Instytut Standardów i Technologii) – agenda rządowa przy Departamencie Handlu (ang. Department of Commerce) USA. Adres witryny internetowej: https://www.nist.gov/ [dostęp: 10 V 2018].
[83] P. Mell, T. Grance, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, s. 2 [dostęp: 10 V 2018].
[84] A. Kumar, A. Saxena, V. K. Suvarna, V. Rawat, *Top 10 Trends…*, s. 10.

W związku z rosnącym zapotrzebowaniem na przechowywanie coraz większej ilości danych, koniecznością szybkiego angażowania dużych mocy obliczeniowych potrzebnych do analiz i coraz większą integracją rozwiązań teleinformatycznych (omnikanałowość) banki dostrzegają potencjał chmur obliczeniowych. Obecnie widzą w nich główny czynnik wzrostu, a nie tylko sposób na ograniczenie kosztów operacyjnych[85].

### 3.3. Konieczność wymiany podstawowych systemów bankowych

Typową oznaką transformacji cyfrowej banków jest również wymiana (a nie gruntowna modernizacja) obecnie funkcjonujących, podstawowych systemów bankowych (ang. *core banking system*). Cyfryzacja musi bowiem zachodzić także w samym sercu banku, a nie tylko w obszarze kanałów komunikacyjnych dostępnych dla klientów.

Jednym z głównych powodów jest konieczność redukcji złożoności architektonicznej tych systemów i umożliwienie im szybszej adaptacji do zmieniających się trendów oraz potrzeb cyfrowego świata (np. integracja z chmurami obliczeniowymi czy technologiami *Big Data*). Podstawowym kryterium jest możliwość szybkiego włączania nowych, cyfrowych, dziś jeszcze nieistniejących, kanałów dostępu do usług bankowych i wsparcie wcześniej przedstawionej omnikanałowości[86].

Złożoność architektoniczna obecnych systemów bankowych wyklucza ich użycie nie tylko ze względu na istniejące ograniczenia techniczne, lecz także z punktu widzenia bezpieczeństwa danych i transakcji bankowych. Jednocześnie dołączanie do nich kolejnych kanałów obsługi klienta będzie w przyszłości otwierać nowe możliwości dla cyberprzestępców.

### 3.4. Kryptowaluty jako pieniądz bankowości cyfrowej

Transformacja cyfrowa banków wiąże się także z problematyką wykorzystania tzw. walut wirtualnych (szczególnie kryptowalut), które są cyfrową reprezentacją wartości i nie są emitowane przez banki centralne ani żadne instytucje państwowe. Co ważne, waluty cyfrowe nie muszą być powiązane z walutą konwencjonalną (tzw. pieniądzem fiducjarnym[87]), ale są akceptowane przez osoby fizyczne lub prawne jako środek płatniczy i mogą być przesyłane, przechowywane lub sprzedawane elektronicznie. Głównymi zainteresowanymi są tutaj m.in. użytkownicy sieci, giełdy, platformy handlowe i dostawcy usług *e-wallet* (inaczej: portmonetek internetowych)[88].

Europejski Organ Nadzoru Bankowego (ang. European Banking Authority, EBA) w 2014 r. wydał opinię na temat wirtualnych walut, których w tamtym czasie istniało

[85] Tamże, s. 11.
[86] Tamże, s. 14.
[87] Pieniądz fiducjarny (łac. *fides* – wiara) – waluta, która nie ma oparcia w dobrach materialnych (np. w kruszcach). Wartość takiej waluty ma źródło z reguły w dekretowanym prawnie monopolu co do wykorzystania jej na danym obszarze jako legalnego środka płatniczego oraz jest oparta na popycie generowanym przez instytucje państwowe, głównie przez pobór podatków. Wartość pieniądza fiducjarnego zakłada istnienie zaufania do emitenta, zob. *Pieniądz fiducjarny*, https://www.nbportal.pl/slownik/pozycje-slownika/pieniadz-fiducjarny [dostęp 11 V 2018].
[88] *EBA Opinion on 'virtual currencies'*, European Banking Authority, VII 2014 r., https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, s. 5 [dostęp: 10 V 2018].

już ponad 200 odmian[89]. Zwrócono uwagę na to, że waluty cyfrowe mają pewne zalety: niższy koszt obsługi transakcji, zwiększona szybkość transakcji czy powszechna dostępność. Jednak dla EBA bardziej istotne było ryzyko związane z ich używaniem. W ramach przyjętych kategorii zidentyfikowano ich ponad 70, w tym: ryzyko dla użytkowników, ryzyko dla uczestników rynku niebędących użytkownikami, ryzyko związane z integralnością finansową (np. pranie pieniędzy i inne formy przestępczości finansowej), ryzyko dla systemów płatniczych korzystających z walut konwencjonalnych i ryzyko dla regulatorów oraz instytucji nadzorczych[90].

Najbardziej atrakcyjną odmianą walut wirtualnych są tzw. kryptowaluty (także: waluty kryptograficzne), w tym najbardziej popularny bitcoin. Technologie związane z kryptowalutami wciąż są w fazie rozwoju. Główną tego przyczyną jest brak wspólnego podejścia i zunifikowanej platformy obsługi. W wielu przypadkach kryptowaluty nie osiągnęły jeszcze poziomu dojrzałości (wiarygodności) wymaganego od konwencjonalnych walut. Dotyczy to także przypadku popularnego bitcoina, którego przyszłość jest uznawana za niepewną, waluta ta bowiem powstała jako efekt eksperymentu[91].

Widoczna jest jednak presja rynku na przyjęcie wspólnego standardu w zakresie obsługi kryptowalut. Banki takie, jak UBS, Deutsche Bank, Santander, BNY Melon, rozpoczęły prace nad własną kryptowalutą. Także Goldman Sachs i JPMorgan zdecydowały się rozwijać własne rozwiązania. Równolegle Bank of England pracuje nad prototypem kryptowaluty, która miałaby być emitowana przez państwo[92]. Z kolei Holenderski Bank Centralny (hol. De Nederlandsche Bank, DNB) przeprowadził testy związane z użyciem bitcoinów do 2140 r. (szacowana data wyczerpania się możliwości tworzenia nowych bitcoinów na podstawie wykorzystywanego algorytmu)[93] w celu określenia jej przydatności i rozpoznania ewentualnych zagrożeń.

Obecnie kryptowaluty znajdują się w centrum zainteresowania zarówno cyberprzestępców, jak i banków oraz ich klientów. Dla cyberprzestępców istotna jest anonimowość, szybkość, dostępność i szerokie możliwości finansowania działań przestępczych (np. wyłudzenia, okupy). Z kolei dla banków najważniejsze jest uwiarygodnienie kryptowalut, lepsze poznanie ich możliwości, zrozumienie mechanizmów zarządzania ryzykiem oraz opracowanie wspólnych standardów i regulacji. Dopiero wówczas rozliczenia w kryptowalutach będą mogły być oferowane klientom.

W kontekście kryptowalut szczególną uwagę należy zwrócić również na uregulowanie spraw związanych z praniem brudnych pieniędzy i finansowaniem terroryzmu. Ponieważ te zjawiska mają charakter globalny, potrzebna jest efektywna współpraca

[89] Tamże, s. 10.
[90] Tamże, s. 5.
[91] *Driving the Digital Transformation. The EBF blueprint for digital banking and policy change*, European Banking Federation, http://www.ebfdigitalbanking.eu/images/EBF_DigitalReport.pdf, s. 38 [dostęp: 10 V 2018].
[92] L. Brus, *4 major banks to create cryptocurrency for settlement*, http://www.coinfox.info/news/6263-4-major-banks-to-create-cryptocurrency-for-settlement [dostęp: 10 V 2018].
[93] M. del Castillo, *Dutch Central Bank Presents Results of Cryptocurrency Experiments*, http://www.coindesk.com/dutch-central-bank-cryptocurrency-experiments/ [dostęp: 10 V 2018].

banków i instytucji państwowych (w tym służb zajmujących się zwalczaniem przestępczości zorganizowanej, terroryzmu i wszelkich powiązanych odmian cyberprzestępczości) na szczeblu międzynarodowym. Wymaga to nie tylko odpowiednich regulacji prawnych, lecz także budowania zintegrowanych systemów bezpieczeństwa zarówno na poziomie państwowym, jak i międzynarodowym, np. w ramach Unii Europejskiej.

## 4. Terrorystyczny wymiar cyberprzestępczości

Czy terroryzm (i jego nowoczesna odmiana – cyberterroryzm) w ogóle powinien znajdować się w centrum zainteresowania banków, jeżeli chodzi o bezpieczeństwo? Bez wątpienia tak, szczególnie, że istnieje ścisły związek między działalnością terrorystyczną a cyberprzestępczością.

Terroryzm stawia sobie za cel wpływanie na władzę, używając przemocy lub grożąc jej użyciem. Jest to podstawowe zagrożenie wynikające z działalności terrorystycznej. W przeciwieństwie do „zwykłej" przestępczej przemocy, bezpośrednia ofiara terrorystów nie jest dla nich głównym obiektem ataku. Ofiary, wybierane mniej czy bardziej przypadkowo, zawsze mają znaczenie symboliczne. Nieświadomie i bezwolnie stają się przekaźnikami informacji komunikowanej przez terrorystów[94]. W tym sensie akt terrorystyczny można interpretować jako swoisty akt komunikacyjny, w uproszczeniu – mający nadawcę, odbiorcę (masowego), określoną treść funkcjonującą w danym kontekście oraz chcący wywołać zamierzony efekt i sprzężenie zwrotne (ten akt ma wymiar socjotechniczny). Przemoc terrorystów jest więc formą komunikowania określonych treści szerokiej rzeszy odbiorców. Wszystko inne w ich działaniu jest temu podporządkowane[95].

W tych rozważaniach istotne jest podkreślenie, że terroryzm zawsze pozostaje zorientowany politycznie (istotny jest wpływ na władzę), a nie finansowo (czyli na uzyskanie nielegalnych dochodów). Pozwala to odróżnić działalność terrorystyczną od zwykłej przestępczości zorganizowanej. Mimo że głównym celem terrorystów nie jest zysk finansowy, muszą oni dysponować niemałym zapleczem finansowym, aby skutecznie prowadzić swoją działalność. W przypadku braku niezależności finansowej, otwiera się pole do współpracy grup terrorystycznych z niektórymi państwami lub grupami przestępczymi[96].

Oczywistym kierunkiem poszukiwania środków służących finansowaniu działalności terrorystycznej jest cyberprzestrzeń. Co ważne, nie wymaga to od grup terrorystycznych dysponowania zaawansowaną wiedzą techniczną (choć, oczywiście, mając na uwadze własną niezależność i rachunek ekonomiczny, należy przyjąć, że taki proces także ma miejsce), mogą one natomist skorzystać ze skomercjalizowanego i profesjonalnego rynku cyberprzestępczego, czyli tzw. cyberprzestępstwa jako usługi (ang. *Cybercrime as a Service*, CaaS). Oznacza to współpracę grup terrorystycznych z grupami cyberprzestępczymi (przynajmniej do momentu wybudowania własnych struktur będących w stanie prowadzić

[94] K. Kozłowski, *Terroryzm jako zagrożenie państwa*, w: *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, S. Sulowski, M. Brzeziński (red.), Warszawa 2009, s. 301.
[95] Tamże.
[96] Tamże, s. 303–304.

niezależną działalność w cyberprzestrzeni). Warto podkreślić, że tego typu współpraca zdaje się godzić w interesy obydwu grup: cyberprzestępców (ukierunkowanych na zysk) oraz cyberterrorystów (ukierunkowanych na efekt polityczny bądź szukających środków do finansowania swojej działalności). W rezultacie, biorąc pod uwagę ukrywanie prawdziwej tożsamości napastników w cyberprzestrzeni, czemu sprzyja zjawisko CaaS, powstaje bardzo skomplikowana sieć zależności. O ile bowiem wciąż można bronić się przed samymi atakami w cyberprzestrzeni (prewencja jako główne zadanie banków w omawianym aspekcie), o tyle zwalczanie cyberprzestępczości i cyberterroryzmu (które jest głównym zadaniem służb państwowych) staje się bardzo utrudnione.

Dokładna analiza cech konkretnego ataku ma ogromne znaczenie, ponieważ tylko wówczas, kiedy odkryje się rzeczywistą tożsamość napastników, jest się w stanie poznać prawdziwą naturę przeprowadzanych przez nich działań, rozważyć ich bezpośrednie motywy, oszacować zasoby, które mogą zostać (lub zostały) wykorzystane podczas ataku i w ten sposób określić jego skalę; a wreszcie – przypisać konkretną motywację: finansową lub polityczną. Należy też wspomnieć o działaniach, które mogą być realizowane przez służby specjalne (w przypadku niektórych państw mogą one działać w powiązaniu z grupami cyberprzestępczymi lub cyberterrorystycznymi) w ramach tzw. cyberszpiegostwa lub cyberwojny[97].

Jednoznaczne wskazanie określonego typu aktywności w cyberprzestrzeni jest możliwe wyłącznie po dokładnej analizie cech ataku (i jego kontekstu). Pozwala także uruchomić skuteczne działania kontrwywiadowcze lub właściwie ukierunkowany kontratak. Ma to szczególne znaczenie, jeżeli weźmie się pod uwagę to, że wszelkie tego typu państwowe odpowiedzi wymagają usprawiedliwienia na mocy prawa międzynarodowego. Przykładowo, pamiętając, że Internet jest obecnie traktowany jako piąty teatr działań wojennych (w ramach państw NATO)[98], istotny jest art. 5 Traktatu Północnoatlantyckiego. Jego użycie przez państwa NATO w celu przeprowadzenia wspólnej odpowiedzi jest możliwe wyłącznie po uzyskaniu absolutnej pewności co do źródła i motywacji strony atakującej. W takim przypadku należy bezsprzecznie przypisać odpowiedzialność za atak konkretnemu państwu, a dopiero wówczas uruchomić odpowiednie kontrdziałania. Bez dogłębnej wiedzy trudno bowiem odróżnić atak cyberprzestępczy od aktu cyberterroryzmu, działań haktywistów[99] lub służb obcych państw[100].

[97] P. Kijewski, P. Jaroszewski, J.A. Urbanowicz, J. Armin, *The Never-Ending Game of Cyberattak Attribution. Exploring the Threats, Defenses and Research Gaps*, https://www.researchgate.net/publication/303601738_The_Never-Ending_Game_of_Cyberattack_Attribution, s. 176 [dostęp: 14 V 2018]

[98] *Krajobraz bezpieczeństwa polskiego internetu 2015. Raport roczny z działalności CERT Polska*, Warszawa 2016, s. 18.

[99] Haktywizm polega na wykorzystaniu umiejętności hakerskich do realizacji działań o wymowie społecznej lub politycznej (np. wolność słowa, ochrona praw człowieka, prywatność w sieci, ochrona środowiska, zwalczanie sekt religijnych, walka z pedofilią itd.). W tym sensie haktywiści przypominają tradycyjnych aktywistów, którzy przeprowadzają różnego rodzaju akcje (blokady, manifestacje, happeningi itp.) służące im do promocji określonej ideologii, systemu wartości, punktu widzenia bądź do blokowania niekorzystnych, ich zdaniem, decyzji lub działań rządów, przedsiębiorstw itp. Zob. D. Cieślak, *Haktywiści - hakerzy w służbie społeczeństwa*, http://next.gazeta.pl/internet/1,104530,7612128,Haktyw isci_hakerzy_w_sluzbie_spoleczenstwa.html [dostęp: 14 V 2018].

[100] Tamże.

Z kolei w przypadku typowej, jednoznacznie zidentyfikowanej cyberprzestępczości, dogłębna analiza cech ataku pozwala przeprowadzać efektywne śledztwa policyjne oraz postępowania procesowe. W rezultacie możliwe jest nie tylko postawienie napastnikom właściwych zarzutów, lecz także skorelowanie dokonanego czynu z innymi, podobnymi działaniami realizowanymi przez tę samą grupę cyberprzestępczą lub jej współpracowników[101].

Mając na uwadze ogólnoświatowy wymiar współczesnej bankowości oraz globalny charakter cyberprzestrzeni i wszelkich związanych z nią zagrożeń, trzeba mieć świadomość, że banki znajdują się na celowniku grup przestępczych, w tym terrorystów. Ich ataki mogą mieć wymiar zarówno kryminalny (motywacja finansowa), jak i polityczny (ideologiczny). Może o tym świadczyć kadr z filmu propagandowego terrorystów Daesh, na którym jednoznacznie wskazano potencjalne cele ataków (zdj. 5).


**Zdj. 5.** Kadr z filmu propagandowego terrorystów z Daesh rozpowszechnianego w Internecie, w którym wskazują oni jednoznacznie na potencjalne cele ataków – globalne, amerykańskie koncerny, w tym bank Citi (lewy, górny róg) i Merill Lynch, część Bank of America (prawy, dolny róg).

Źródło: *Estado Islámico: Éstas son las empresasy países amenazados por terroristas (VIDEO)*, https://diariocorreo.pe/mundo/estado-islamico-estas-son-las-empresas-y-paises-amenazados-por-terroristas-video-635558/ [dostęp: 14 V 2018].

Udany atak na duży bank mógłby spowodować paraliż sektora finansowego. Byłoby to wydarzenie bardzo spektakularne i na pewno atrakcyjne z punktu widzenia terrorystów. Sukces skutecznie podważyłby także zaufanie klientów (indywidualnych i korporacyjnych) do współczesnej bankowości, co z kolei miałoby ogromny, negatywny wpływ na rozwój gospodarczy społeczeństw znajdujących się na celowniku terrorystów. Tego typu operacja mogłaby być opatrzona odpowiednią kampanią informacyjną (dezinformacyjną?) w Internecie, realizowaną za pomocą filmów, materiałów graficznych

[101] Tamże.

i innych środków przekazu, wzmacniających przesłanie, a nawet zyskujących poparcie szerszych grup społecznych dla tego typu działań. Widoczne jest bowiem wspieranie działań cyberterrorystycznych (lub kampanii haktywistów noszących takie znamiona) częstokroć bardzo profesjonalnymi materiałami propagandowymi, które mają na celu przekazanie rzekomej ideologicznej podbudowy ataku, wywołanie strachu lub uzyskanie wsparcia dla prowadzonych operacji.

Innym istotnym punktem styku cyberprzestępców i terroryzmu jest tzw. *cyberlaundering*, czyli pranie brudnych pieniędzy – środków finansowych pochodzących z nielegalnej (w tym cyberprzestępczej) działalności, które mogą być następnie użyte – za pomocą nowoczesnych technologii – do finansowania działalności terrorystycznej[102]. Współczesne elektroniczne systemy płatnicze, w tym dostępność kryptowalut, a także rozwój bankowości cyfrowej otwierają ogromne możliwości przed cyberprzestępcami. W rezultacie obowiązek przeciwdziałania praniu brudnych pieniędzy i finansowaniu terroryzmu, który w Polsce m.in. na instytucje bankowe nakładają ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[103] oraz dyrektywy i rozporządzenia UE[104], okazuje się zadaniem wyjątkowo złożonym. Może o tym świadczyć nie tylko stopień zaawansowania technologicznego cyberprzestępców, wachlarz dostępnych im możliwości, lecz także liczba aktów prawnych, które starają się ten obszar regulować.

Jeżeli chodzi o dotychczasową skuteczność, zarówno działań zapobiegawczych (realizowanych m.in. przez banki), jak i kontroli ze strony instytucji państwowych, wystarczy jedynie przywołać wyniki raportu NIK, w którym stwierdzono:

---

[102] Zob. D.A. Leslie, *Legal Principles for Combatting Cyberlaundering*, https://www.springer.com/cda/content/document/cda_downloaddocument/9783319064154-c1.pdf?SGWID=0-0-45-1467905-p176710334, s. 55 [dostęp: 14 V 2018].

[103] *Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz.U. z 2000 r. nr 116 poz. 1216), (akt uchylony, obecnie obowiązującą ustawą jest *Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, Dz.U. z 2018 r. poz. 723, ze zm.).

[104] Dla przykładu: (1) *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE*; (2) *Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu*; (3) *Dyrektywa Komisji 2006/70/WE z dnia 1 sierpnia 2006 r. ustanawiająca środki wykonawcze do dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady w odniesieniu do definicji osoby zajmującej eksponowane stanowisko polityczne, jak również w odniesieniu do technicznych kryteriów stosowania uproszczonych zasad należytej staranności wobec klienta oraz wyłączenia z uwagi na działalność finansową prowadzoną w sposób sporadyczny lub w bardzo ograniczonym zakresie*; (4) *Rozporządzenie (WE) nr 1781/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie informacji o zleceniodawcach, które towarzyszą przekazom pieniężnym*; (5) *Rozporządzenie Rady z dnia 20 stycznia 2014 r. zmieniające rozporządzenie (UE) nr 267/2012 w sprawie środków ograniczających wobec Iranu*; (6) *Rozporządzenie Rady (WE) nr 501/2009 z dnia 15 czerwca 2009 r. wykonujące art. 2 ust. 3 rozporządzenia (WE) nr 2580/2001 w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu i uchylające decyzję 2009/62/WE*; (7) *Rozporządzenie Rady (WE) nr 881/2002 z dnia 27 maja 2002 r. wprowadzające niektóre szczególne środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z Osamą bin Ladenem, siecią Al-Kaida i Talibami i uchylające rozporządzenie Rady (WE) nr 467/2001 zakazujące wywozu niektórych towarów i usług do Afganistanu, wzmacniające zakaz lotów i rozszerzające zamrożenie funduszy i innych środków finansowych w odniesieniu do Talibów w Afganistanie*.

(…) w okresie objętym kontrolą (od początku 2013 r. do połowy 2015 r.) skuteczność systemu kontroli nad instytucjami, które zobowiązane są do rejestrowania transakcji ponadprogowych i podejrzanych, była niska. Przy szacowanej na 18,2 mld zł w 2014 r. skali zjawiska prania pieniędzy, w postępowaniach karnych zabezpieczono majątek w wysokości 1,2 mln zł oraz orzeczono przepadek mienia o wartości 11,5 mln zł, czyli 0,07 proc. szacowanej kwoty. W 2015 r. skala zjawiska prania pieniędzy szacowana była na ponad 17 mld zł, natomiast w postępowaniach karnych zabezpieczono majątek w wysokości 3 mln zł oraz orzeczono przepadek mienia o wartości blisko 100 mln zł, co stanowiło 0,6 proc. wymienionej kwoty[105].

Przywołane wyniki związane z polskim sektorem bankowym można uznać za rozczarowujące. Należy jednak mieć świadomość, że zjawisko prania brudnych pieniędzy i finansowania terroryzmu ma wymiar globalny, a więc skuteczne przeciwdziałanie jest możliwe tylko w ramach współpracy międzynarodowej.

## Zakończenie

W niniejszym opracowaniu autor pokusił się o przedstawienie rysu historycznego przestępczości bankowej z uwzględnieniem trzech dominujących obecnie odmian bankowości: klasycznej, elektronicznej (dostępnej za pośrednictwem wielu kanałów – zwłaszcza przez sieć terminali ATM i Internet) oraz rodzącej się bankowości cyfrowej (omnikanałowej). Warto zaznaczyć, że transformacja cyfrowa jeszcze długo nie będzie oznaczać całkowitego zaniku placówek bankowych – wciąż jest to jeden z istotnych kanałów kontaktu z klientem oprócz bankomatów, Internetu czy technologii mobilnych.

Dla bankowości cyfrowej istotne jest czerpanie z doświadczeń przeszłości i świadomość zagrożeń funkcjonujących w różnych, współoddziałujących na siebie kanałach. W obrębie bankowości cyfrowej mamy zatem do czynienia z całą gamą zagrożeń, co wymaga wdrożenia kompleksowego systemu bezpieczeństwa banku. Taki system powinien obejmować wszystkie obszary ryzyka – od placówek przez oddziały, centrale, skarbce, ośrodki przetwarzania danych i zaplecza IT, sieci bankomatów, bankowość internetową aż do nowo powstających kanałów dystrybucji, np. aplikacji mobilnych. Istotną rolę odgrywają także nowe technologie, które zwiększają ryzyko wycieku danych (*Big Data*, *cloud computing*), oraz stabilne, nowoczesne, podstawowe systemy bankowe (ang. *core banking systems*), które muszą się cechować przejrzystą architekturą[106] zapewniającą bezpieczeństwo i łatwość adaptacji nowych rozwiązań w przyszłości. Kontrowersje budzą kryptowaluty, do których instytucje bankowe mają bardzo zróżnicowany stosunek (dostrzegają zarówno ich wady, jak i zalety), a także

[105] *NIK o systemie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu*, https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/nik-o-systemie-przeciwdzialania-praniu-pieniedzy-oraz-finansowaniu-terroryzmu.html [dostęp: 14 V 2018].

[106] Architektura – ogólna, ramowa budowa systemu komputerowego lub oprogramowania określająca strukturę systemu, przydział funkcji jego elementom, protokoły interakcji między elementami (interfejsy) oraz metody konstrukcji systemu, zob. *Słownik pojęć*, K. Goczyła (red.), w: *Metody wytwarzania oprogramowania*, S. Szejko (red.), Warszawa 2002, s. 299.

technologia *blockchain* (inaczej: łańcuch bloków), która być może zrewolucjonizuje m.in. sposób obsługi transakcji[107].

Cyberprzestrzeń jako piąty teatr działań wojennych jest polem aktywności służb obcych państw (np. prowadzenia działalności wywiadowczej), a także potencjalnym obszarem prowadzenia operacji wojskowych. Oczywistym celem ataków będzie infrastruktura krytyczna państwa, której istotną częścią są systemy finansowe, w tym bankowe. Im bardziej postępuje cyfryzacja banków, tym większe jest ryzyko, że staną się one celem ataku. Jak twierdzą autorzy raportu *Beyond Security. Cyber Threats and the Financial Sector: Is anybody safe?*, opublikowanego przez BT Global Services[108], ataki ze strony cyberterrorystów lub zagrożenia związane z cyberwojną prawdopodobnie mniej będą dotyczyć wojskowych lub rządowych sieci, niż np. rynku finansowego, giełd i izb rozrachunkowych, które są łatwiejszymi celami[109].

Ważnym obszarem działalności grup przestępczych oraz terrorystycznych jest pranie brudnych pieniędzy. Bankowość cyfrowa – wraz z jej omnikanałowością, a więc zasadą docierania do klienta za pomocą możliwie największej liczby przenikających się kanałów (od kontaktu z pracownikiem banku w placówce po użycie nowoczesnych technologii) – otwiera wiele nowych możliwości. Banki już dziś nie najlepiej radzą sobie z kontrolowaniem tego zjawiska, a w przyszłości jego skala i różnorodność będą się zwiększać, dlatego konieczne jest wypracowanie całkiem nowych metod przeciwdziałania.

Wszystko to stanowi nie lada wyzwanie nie tylko dla banków, lecz także dla służb odpowiedzialnych za zwalczanie przestępczości i terroryzmu. Wydaje się, że w przyszłości konieczne będzie ścisłe współdziałanie banków i służb, a także przełamanie wielu stereotypów związanych z taką współpracą, w tym integracja sektora państwowego, prywatnego i pozarządowego na rzecz cyberbezpieczeństwa. Mając na uwadze globalny charakter opisywanych zjawisk, konieczna jest kooperacja na szczeblu międzynarodowym.

**Bibliografia:**

*ATM Security. Explaining Attack Vectors, Defense Strategies and Solutions*, NCR Corporation, 2016, http://docplayer.net/76384265-Atm-security-explaining-attack-vectors-defense-strategies-and-solutions-an-ncr-white-paper.html [dostęp: 10 V 2018].

Avelar V., *Guidelines for Specifying Data Center Criticality / Tier Levels. White Paper#122*, http://it-resource.schneider-electric.com/i/482623-wp-122-guidelines-for-specifying-data-center-criticality-tier-levels/5? [dostęp: 11 V 2018].

[107] Technologia *blockchain* jest tematem na tyle interesującym, że bez wątpienia wymaga osobnego opracowania z perspektywy bezpieczeństwa, stwarza bowiem nie tylko nowe możliwości dla sektora finansowego, lecz także dla administracji państwowej.

[108] BT Global Services, adres witryny internetowej: http://www.globalservices.bt.com/ [dostęp: 12 V 2018].

[109] *Beyond Security. Cyber Threats and the Financial Sector: Is anybody safe?*, https://www.globalservices.bt.com/static/assets/pdf/financial_markets/Finance_sector_Cyber_final.pdf [dostęp: 12 V 2018].

*Bank of America revolutionizes banking industry*, http://about.bankofamerica.com/en-us/our-story/bank-of-america-revolutionizes-industry.html#fbid=T4jvCWpikvv [dostęp: 8 V 2018].

*Beyond Security. Cyber Threats and the Financial Sector: Is anybody safe?*, https://www.globalservices.bt.com/static/assets/pdf/financial_markets/Finance_sector_Cyber_final.pdf [dostęp: 12 V 2018].

Biegański J., *Sposoby popełniania przestępstw związanych z elektronicznymi instrumentami płatniczymi po wdrożeniu EMV*, w: *Przestępczość teleinformatyczna*, J. Kosiński (red.), Szczytno 2012, Wyższa Szkoła Policji.

Biryukov V., *Żonglowanie kartami: Przestępstwa z wykorzystaniem bankomatów*, https://plblog.kaspersky.com/zonglowanie-kartami-dzialalnosc-przestepcza-z-wykorzystaniem-bankomatow/2565/ [dostęp: 11 V 2018].

*Borkowo koło Gdańska: Skradziono bankomat. Jeden ze sprawców wciąż na wolności*, http://www.dziennikbaltycki.pl/wiadomosci/kartuzy/a/borkowo-kolo-gdanska-skradziono-bankomat-jeden-ze-sprawcow-wciaz-na-wolnosci-zdjecia-wideo,9794749/ [dostęp: 10 V 2018].

Brus L., *4 major banks to create cryptocurrency for settlement*, http://www.coinfox.info/news/6263-4-major-banks-to-create-cryptocurrency-for-settlement [dostęp: 10 V 2018].

Castillo M. del, *Dutch Central Bank Presents Results of Cryptocurrency Experiments*, http://www.coindesk.com/dutch-central-bank-cryptocurrency-experiments/ [dostęp: 10 V 2018].

*Driving the Digital Transformation. The EBF blueprint for digital banking and policy change*, European Banking Federation, http://www.ebfdigitalbanking.eu/images/EBF_DigitalReport.pdf [dostęp: 10 V 2018].

*EBA Opinion on 'virtual currencies'*, European Banking Authority, VII 2014 r., https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [dostęp: 10 V 2018].

*Estado Islámico: Éstas son las empresas y países amenazados por terroristas (VIDEO)*, https://diariocorreo.pe/mundo/estado-islamico-estas-son-las-empresas-y-paises-amenazados-por-terroristas-video-635558/ [dostęp: 16 V 2018].

Evans D., *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, Cisco IBSG, IV 2011 r., http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [dostęp: 10 V 2018].

Fastyn T., *Ataki na system SWIFT. Operacja pod fałszywą flagą?*, http://www.cyberdefence24.pl/551844,ataki-na-system-swift-operacja-pod-falszywa-flaga [dostęp: 10 V 2018].

*Global ATM installed base to reach 4M by 2021*, https://www.atmmarketplace.com/news/global-atm-installed-base-to-reach-4m-by-2021/ [dostęp: 11 V 2018].

Goodman M., *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, Gliwice 2016, Helion.

*Google "Dublin Data Centre" (Main Entrance) Ireland*, http://www.panoramio.com/photo/115851510 [dostęp: 20 II 2017].

Graczyk-Kucharska M., *Big data koniecznością współczesnego marketingu*, „Problemy Zarządzania, Finansów i Marketingu" 2015, nr 41.

*How can crime undermine the convenience of cash*, Wincor Nixdorf International GmbH, 2015, https://www.atmia.com/whitepapers/how-crime-can-undermine-the-convenience-of-cash/86/ [dostęp: 10 V 2018].

Jagiełło Z., *Bankowość detaliczna w obecnych warunkach rynkowych. Kierunki rozwoju*, w: *Wyzwania bankowości detalicznej*, Z. Jagiełło (red.), Gdańsk 2015, Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa, s. 7–10.

Kadr z filmu: *Jackpotting an ATM with a black box*, https://www.youtube.com/watch?v=3HYA0MvizpM [dostęp: 11 V 2018].

Kadr z filmu: *Security and Data Protection in a Google Data Center*, https://www.youtube.com/watch?v=cLory3qLoY8 [dostęp: 11 V 2018].

Kozłowski K., *Terroryzm jako zagrożenie państwa*, w: *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, S. Sulowski, M. Brzeziński (red.), Warszawa 2009, Elipsa.

*Krajobraz bezpieczeństwa polskiego internetu 2015. Raport roczny z działalności CERT Polska*, Warszawa 2016, NASK/CERT Polska.

Kroc J., *Strategie dystrybucji w bankowości detalicznej według koncepcji Accenture*, w: *Wyzwania bankowości detalicznej*, Z. Jagiełło (red.), Gdańsk 2015, Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa, s. 91–94.

Kumar A., Saxena A., Suvarna V. K., Rawat V., *Top 10 Trends in Banking in 2016*, Capgemini, 2016, https://www.capgemini.com/wp-content/uploads/2017/07/banking_top_10_trends_2016.pdf [dostęp: 10 V 2018].

Lashmar P., *Hatton Garden ringleader Brian Reader also masterminded Lloyds Baker Street heist 45 years ago,* http://www.independent.co.uk/news/uk/crime/hatton-garden-ringleader-brian-reader-also-masterminded-lloyds-baker-street-heist-45-years-ago-a6814956.html [dostęp: 8 V 2018].

Leslie D.A., *Legal Principles for Combatting Cyberlaundering*, https://www.springer.com/cda/content/document/cda_downloaddocument/9783319064154-c1.pdf?SGWID=0-0-45-1467905-p176710334 [dostęp: 14 V 2018].

Mell P., Grance T., *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, NIST, IX 2011 r., http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [dostęp: 10 V 2018].

*Metodyka uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie*, Warszawa 2016, Komenda Główna Policji, http://www.policja.pl/download/1/219800/metodyka.pdf [dostęp: 8 V 2018].

Mórawski K.J., *Raport Specjalny Bezpieczeństwo: Placówki pod specjalnym nadzorem*, http://alebank.pl/raport-specjalny-bezpieczenstwo-placowki-pod-specjalnym-nadzorem/?id=57632&catid=944 [dostęp: 8 V 2018].

Morisi T.L*., Commercial banking transformed by computer technology*, „Monthly Labor Review" 1996, sierpień, https://stats.bls.gov/opub/mlr/1996/08/art4full.pdf [dostęp: 8 V 2018].

*Na Estonii testowano wojnę cybernetyczną*, https://www.wprost.pl/107407/ [dostęp: 10 V 2018]

Niczyporuk P., Talecka A., *Bankowość. Podstawowe zagadnienia*, Białystok 2011, Temida 2.

*NIK o systemie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu*, https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/nik-o-systemie-przeciwdzialania-praniu-pieniedzy-oraz-finansowaniu-terroryzmu.html [dostęp: 14 V 2018].

*Okradał bankomaty, miast uzupełniać w nich kasę*, http://bydgoszcz.tvp.pl/13142481/okradal-bankomaty-miast-uzupelniac-w-nich-kase [dostęp: 10 V 2018].

Ornoch P., *Bezpieczeństwo fizyczne i środowiskowe*, http://bs.net.pl/artykuly-nie-tylko-dla-informatykow/bezpieczenstwo-fizyczne-i-srodowiskowe [dostęp: 8 V 2018].

Pasztelański R., *Brutalny gang oskarżony o serię napadów, w tym atak w Wólce Kosowskiej*, http://www.tvp.info/15638754/brutalny-gang-oskarzony-o-serie-napadow-w-tym-atak-w-wolce-kosowskiej [dostęp: 8 V 2018].

Patterson R., *Kompendium terminów z zakresu bankowości po polsku i angielsku*, Warszawa 2015, Ministerstwo Finansów.

*Przyjęcie nowej Rekomendacji D*, https://www.knf.gov.pl/aktualnosci/2013/Przyjecie_nowej_Rekomendacji_D.html [dostęp: 20 II 2017].

Walsh R., *The Baker Street Bank Heist*, http://www.crimemagazine.com/baker-street-bank-heist [dostęp: 8 V 2018].

*Słownik pojęć*, w: *Metody wytwarzania oprogramowania*, S. Szejko (red.), Warszawa 2002.

**Akty prawne:**

*Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L141 z 5 czerwca 2015 r., s. 73).*

*Dyrektywa Komisji 2006/70/WE z dnia 1 sierpnia 2006 r. ustanawiająca środki wykonawcze do dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady w odniesieniu do definicji osoby zajmującej eksponowane stanowisko polityczne, jak również w odniesieniu do technicznych kryteriów stosowania uproszczonych zasad należytej staranności wobec klienta oraz wyłączenia z uwagi na działalność finansową prowadzoną w sposób sporadyczny lub w bardzo ograniczonym zakresie (Dz. Urz. UE L 214 z 4 sierpnia 2006 r., s. 29).*

*Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu (Dz. Urz. UE L 309 z 35 listopada 2005r., s. 15).*

*Rozporządzenie Rady z dnia 20 stycznia 2014 r. zmieniające rozporządzenie (UE) nr 267/2012 w sprawie środków ograniczających wobec Iranu* (Dz.Urz. UE L 15 z 20 stycznia 2014, s. 18).

*Rozporządzenie Rady (WE) nr 501/2009 z dnia 15 czerwca 2009 r. wykonujące art. 2 ust. 3 rozporządzenia (WE) nr 2580/2001 w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu i uchylające decyzję 2009/62/WE (Dz. Urz. UE L 151z 16 czerwca 2009 r., s. 14).*

*Rozporządzenie (WE) nr 1781/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie informacji o zleceniodawcach, które towarzyszą przekazom pieniężnym* (Dz. Urz. UE L 345 z 8 grudnia 2006 r., s. 1).

*Rozporządzenie Rady (WE) nr 881/2002 z dnia 27 maja 2002 r. wprowadzające niektóre szczególne środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z Osamą bin Ladenem, siecią Al-Kaida i Talibami i uchylające rozporządzenie Rady (WE) nr 467/2001 zakazujące wywozu niektórych towarów i usług do Afganistanu, wzmacniające zakaz lotów i rozszerzające zamrożenie funduszy i innych środków finansowych w odniesieniu do Talibów w Afganistanie* (Dz. Urz. UE L 139 z 29 maja 2002 r., s. 9).

*Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf [dostęp: 8 V 2018].

*Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz.U. z 2018 r. poz. 1000, ze zm.).

*Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz.U. z 2018 r. poz. 723, ze zm.).

*Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (t.j.: Dz.U. z 2018 r. poz. 412, ze zm.).

*Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* (t.j.: Dz.U. z 2018 r. poz. 2142).

*Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (Dz.U. z 2018 r.,poz. 1600, ze zm.).

*Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* (t.j.: Dz.U. z 2018 r. poz. 419, ze zm.).

*Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (Dz.U. z 2010 r. nr 166 poz. 1128).

**Słowa kluczowe:** bankowość, zagrożenia, ryzyka, transformacja cyfrowa, przestępczość.

**Keywords**: banking, threats, risk, digital transformation, crime.

**Krzysztof Wąsala**

# Problematyka karnoprocesowa w ustawie o działaniach antyterrorystycznych[1]

## Wprowadzenie

Autor wskazuje zmiany dotyczące istotnych instytucji karnoprocesowych, które zostały wprowadzone w ustawie o działaniach karnoprocesowych. Przeszukanie i przedstawienie zarzutów to instytucje, którym nadano nowy kształt przez zastosowanie regulacji zawartych w ustawie. Z uwagi na to, że te uregulowania w znaczący sposób modyfikują wskazane instytucje procesowe, należy poddać analizie charakter i kształt tych zmian, zwłaszcza pod kątem ich spójności ze standardem zarówno konwencyjnym, jak i konstytucyjnym. *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[2] jest elementem dostosowywania krajowego prawodawstwa do skuteczniejszego zwalczania terroryzmu. Określono w niej zasady prowadzenia działań antyterrorystycznych oraz współpracy między właściwymi organami realizującymi te działania. Ustawa stwarza nowe możliwości w organizacji pracy operacyjnej oraz procesowej podczas realizacji działań antyterrorystycznych oraz kontrterrorystycznych. Część rozwiązań jest zupełną nowością, niestosowaną do tej pory w Polsce przez organy ścigania oraz służby specjalne, natomiast zakres innych został rozszerzony i przystosowany do realnych potrzeb zmierzających do poprawy bezpieczeństwa. Konsekwencją wejścia w życie ustawy o działaniach antyterrorystycznych były zmiany w wielu innych ustawach, które zawierają uprawnienia organów ścigania i służb specjalnych, najczęściej rozszerzając istniejące już regulacje prawne lub wprowadzając nowe.

## 1. Przeszukanie

Do dowodowych czynności poszukiwawczych regulowanych przepisami *Kodeksu postępowania karnego* należy zaliczyć:

1) zatrzymanie rzeczy, przesyłek oraz korespondencji i wykazu połączeń telekomunikacyjnych lub innych przekazów informacji (art. 217 i 218 kpk),

[1] Fragment pracy magisterskiej pt. *Karnoprocesowe aspekty ustawy o działaniach antyterrorystycznych* (Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii). Praca została wyróżniona w siódmej edycji ogólnopolskiego konkursu Szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2016/2017). Autor wykorzystał rozdział 3 pt. *Problematyka karnoprocesowa w ustawie o działaniach antyterrorystycznych*, podrozdziały 3.2. pt. *Przeszukanie* oraz 3.3. pt. *Przedstawienie zarzutów.*

[2] Tekst jednolity: Dz.U. z 2018 r. poz. 452, ze zm.

2) przeszukanie w celu znalezienia i zajęcia rzeczy, korespondencji lub danych (art. 219 i nast. kpk),
3) podsłuch procesowy (art. 237 i nast. kpk)[3].

Powyższe przepisy stosuje się w odniesieniu do rzeczy oraz przekazu informacji, które mogą stanowić dowód w sprawie, czy wręcz do przedmiotu czynu zabronionego, w tym niebezpiecznego dla życia lub zdrowia, a także do zabezpieczenia majątkowego lub ujęcia poszukiwanej osoby[4]. Przeszukanie obok zatrzymania rzeczy jest czynnością najczęściej wykonywaną w celu poszukiwania dowodów w prowadzonej sprawie, budzącą wielokrotnie emocje osób, które jej doświadczyły, z uwagi na wkraczanie w wolności konstytucyjne i prawa osobiste obywateli w zakresie nienaruszalności mieszkania. Ustawa o działaniach antyterrorystycznych wprowadza zmiany w sposobie stosowania instytucji przeszukania, m.in. umożliwia przeprowadzenie przeszukania także w nocy.

### 1.1. Uregulowanie instytucji przeszukania w *Kodeksie postępowania karnego*

Przeszukanie to poszukiwawczo-wykrywcza czynność dowodowa, będąca jednocześnie środkiem przymusu pozwalającym na legalne wkroczenie w sferę konstytucyjnie gwarantowanych praw i wolności osobistych w postaci nietykalności osobistej (art. 41 ust. 1 Konstytucji RP) i nienaruszalności mieszkania (art. 50 Konstytucji RP). Ze względu na wykrywczy charakter przeszukania tę czynność unormowano jednak w przepisach o dowodach, nie zaś w ramach środków przymusu procesowego[5]. Instytucja przeszukania jest regulowana w art. 219 i następnych w *Kodeksie postępowania karnego*. Przeszukanie dzieli się na przeszukanie osoby i poszukiwanie rzeczy. Zgodnie z art. 219 § 1 kpk można dokonać przeszukania pomieszczeń i innych miejsc w celu wykrycia, zatrzymania albo przymusowego doprowadzenia osoby podejrzanej, a także w celu znalezienia rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym. Przeszukanie może objąć pomieszczenia (mieszkania i inne lokale), inne miejsca (środki transportu, miejsca otwarte), a także osobę, jej odzież i podręczne przedmioty. Bezwzględną przesłanką do przeprowadzenia tej czynności jest uzasadniona podstawa do przypuszczenia, że osoba poszukiwana lub wymienione rzeczy znajdują się w danym miejscu. Podstawą oceny, że występuje uzasadniona podstawa do przypuszczenia, że poszukiwana osoba lub rzecz znajdują się w określonym miejscu, nie mogą być okoliczności uzyskane w sposób nieprocesowy, które ze swej istoty mają niepotwierdzony i wątpliwy charakter. Tak więc wyłącznie dane, które zostały uzyskane w sposób procesowy i były właściwie zweryfikowane, mogą stanowić podstawę do oceny, że poszukiwana rzecz znajduje się w miejscu planowanego przeszukania[6]. Przy zaistnieniu tej przesłanki można dokonać przeszukania w każdej sprawie, poszukując każdego dowodu i nie ograniczając się do

[3] D. Gruszecka, *Zatrzymanie rzeczy i przeszukanie*, w: *Proces karny*, J. Skorupka (red.), Warszawa 2017, s. 461.
[4] T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 2014, s. 536.
[5] Tamże, s. 539.
[6] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2015, s. 534.

możności dokonywania przeszukania wyłącznie w celu znalezienia dowodów o istotnym znaczeniu[7]. Organ procesowy powinien zatem dysponować informacjami, na podstawie których może zasadnie przypuszczać, że w danym miejscu lub u danej osoby (bądź przy niej) znajdują się określone, poszukiwane przedmioty, albo że w danym miejscu lub pomieszczeniu przebywa osoba podejrzana. W wielu sprawach przeszukanie nie będzie konieczne dla znalezienia rzeczy mogącej stanowić dowód. Przykładowo można podać, że w sprawach czynnej napaści na funkcjonariusza państwowego przeszukanie w ogóle jest zbędne, a w sprawach dotyczących podrobienia faktury VAT w celu odnalezienia jednej faktury nie jest konieczne przeszukanie pomieszczeń całego przedsiębiorstwa[8].

Osobę, u której ma nastąpić przeszukanie, należy przed przystąpieniem do tej czynności zawiadomić o jej celu i wezwać do wydania poszukiwanych przedmiotów (art. 224 § 1 kpk). Osobie, u której będzie prowadzona czynność przeszukania, jeszcze przed dokonaniem tej czynności należy okazać postanowienie sądu lub prokuratora (organem uprawnionym do wydania postanowienia o przeszukaniu jest wyłącznie sąd, a w postępowaniu przygotowawczym prokurator) i doręczyć odpis tego postanowienia, a także uzyskać potwierdzenie jego odbioru. W uzasadnieniu postanowienia należy przywołać dowody i okoliczności, na podstawie których uznaje się, że istnieje uzasadniona podstawa do przypuszczenia, że osoba podejrzana lub rzeczy znajdują się w przeszukiwanym miejscu bądź u przeszukiwanej osoby. Wymogów uzasadnienia nie spełnia stwierdzenie, że „zachodzi uzasadniona podstawa do przypuszczenia". Należy wprost powołać się na dowody i okoliczności w danej konkretnej sprawie, które uzasadniają takie przypuszczenie. Tylko tak sformułowane uzasadnienie pozwoli na weryfikację zasadności dokonywanej czynności, w wypadku zaskarżenia postanowienia o przeszukaniu[9].

Dobrowolne wydanie poszukiwanych przedmiotów powinno zakończyć czynność. W razie dobrowolnego wydania przedmiotów wymienionych w postanowieniu o przeszukaniu, cel czynności został osiągnięty i należy odstąpić od przeszukania[10]. Dobrowolne wydanie rzeczy przez osobę, u której ma być przeprowadzone przeszukanie, nie uniemożliwia organom dokonania tej czynności. Kontynuacja przeszukania pomimo dobrowolnego wydania przedmiotów powinna się ograniczać tylko do sytuacji, w której organ nie potrafi wskazać, jakich przedmiotów poszukuje, a zachodzi podejrzenie, że z powodu braku dokładnego określenia przedmiotów w wezwaniu do ich dobrowolnego wydania nie wszystkie, które mogą stanowić dowód, zostały wydane[11]. Przykładem jest sytuacja, gdy na żądanie wydania marihuany osoba, u której nastąpiło przeszukanie, dobrowolnie to uczyniła, ale zachodzi uzasadniona wątpliwość, czy została wydana całość poszukiwanego narkotyku[12]. Podczas przeszukania ma prawo być obecna osoba przybrana przez prowadzącego czynność. Może być również obecna osoba wskazana

[7] D. Gruszecka *Zatrzymanie rzeczy i przeszukanie*…, s. 463.
[8] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 533.
[9] Tamże, s. 535.
[10] Tamże, s. 538.
[11] *Kodeks postępowania karnego. Komentarz*, t. 1, D. Świecki (red.), Warszawa 2015, s. 734.
[12] Tamże.

przez tego, u kogo dokonuje się przeszukania, jeżeli nie uniemożliwia to przeszukania lub nie utrudnia go w istotny sposób. Przeszukanie może nastąpić również wtedy, gdy właściciel czy posiadacz lokalu jest nieobecny. W takim przypadku zgodnie z kpk do przeszukania należy przywołać przynajmniej jednego dorosłego domownika lub sąsiada[13]. Jeżeli miejscem, w którym będzie dokonywane przeszukanie, jest pomieszczenie lub miejsce zamknięte należące do instytucji państwowej lub samorządowej, o zamierzonym przeszukaniu trzeba zawiadomić kierownika tej instytucji lub jego zastępcę albo organ nadrzędny i dopuścić ich do udziału w tej czynności[14].

Przeszukanie jest czynnością obligatoryjnie protokołowaną[15]. Zawartość protokołu przeszukania jest uregulowana w art. 229 kpk. Według tego przepisu protokół zatrzymania rzeczy lub przeszukania powinien oprócz ogólnych wymagań wymienionych w art. 148 kpk (czyli oznaczenia czynności, jej czasu i miejsca oraz osób w niej uczestniczących, podania przebiegu czynności oraz oświadczeń i wniosków jej uczestników, podania postanowień i zarządzeń wydanych w toku czynności czy też stwierdzenia innych okoliczności przebiegu czynności) zawierać oznaczenie sprawy, z którą zatrzymanie rzeczy lub przeszukanie ma związek, dokładną godzinę rozpoczęcia i zakończenia czynności, dokładną listę zatrzymanych rzeczy i w miarę potrzeby ich opis, a także wskazanie polecenia sądu lub prokuratora. Jeżeli polecenie nie zostało uprzednio wydane, zamieszcza się w protokole wzmiankę o poinformowaniu osoby, u której czynność przeprowadzono, że na jej wniosek otrzyma postanowienie w przedmiocie zatwierdzenia czynności.

Przeszukania może dokonać prokurator albo, na polecenie sądu lub prokuratora, policja, a także inny organ – w wypadkach wskazanych w ustawie (na przykład organy finansowe w sprawach o czyny skarbowe z *Kodeksu karnego skarbowego*). W art. 227 kpk nakazuje się, aby przeszukanie było przeprowadzone zgodnie z celem tej czynności, z zachowaniem umiaru oraz bez wyrządzania niepotrzebnych szkód i dolegliwości. Naruszenie tych reguł może rodzić odpowiedzialność Skarbu Państwa (np. policji) za działania funkcjonariuszy (art. 417 *Kodeksu cywilnego*). Przeszukanie rozpoczyna się od okazania osobie, u której ma być przeprowadzone, postanowienia sądu lub prokuratora. Jeżeli zachodzą czynności niecierpiące zwłoki, a sąd lub prokurator nie wydali postanowienia, to organ dokonujący przeszukania przedstawia nakaz kierownika swojej jednostki lub legitymację służbową, a następnie zwraca się niezwłocznie do sądu lub prokuratora o zatwierdzenie przeszukania[16]. Postanowienie sądu lub prokuratora należy doręczyć osobie, u której dokonano przeszukania, w terminie siedmiu dni od daty czynności na zgłoszone do protokołu żądanie tej osoby, o czym należy ją pouczyć. Podejmując decyzję o zatwierdzeniu przeszukania, sąd lub prokurator powinni ustalić, czy dokonanie przeszukania na podstawie nakazu kierownika właściwej jednostki lub legitymacji służbowej było uzasadnione oraz czy posta-

[13] Art. 224 kpk.
[14] Art. 222 kpk.
[15] Art. 143 § 1 pkt. 6 kpk.
[16] Art. 220 § 3 kpk.

nowienie o zarządzeniu przeszukania nie mogło być uprzednio wydane, a także czy czynność została przeprowadzona w sposób przewidziany w art. 227 kpk i udokumentowana zgodnie z art. 229 kpk[17]. Jeżeli przeszukanie nastąpiło bez uprzedniego polecenia sądu lub prokuratora, a w ciągu siedmiu dni od dnia czynności nie nastąpiło jej zatwierdzenie, należy niezwłocznie zwrócić zatrzymane rzeczy osobie uprawnionej, chyba że nastąpiło dobrowolne wydanie, a osoba ta nie złożyła wniosku o zatwierdzenie czynności[18].

Pora przeszukania jest uzależniona od miejsc, które są przeszukiwane, gdyż zgodnie z art. 221 § 1 kpk przeszukania pomieszczeń zamieszkałych można dokonać w godz. od 6.00 do 22.00, a w porze nocnej, czyli od 22.00 do 6.00, tylko w wypadkach niecierpiących zwłoki, z tym że przeszukanie rozpoczęte za dnia można prowadzić nadal mimo rozpoczęcia pory nocnej. Za pomieszczenia zamieszkałe uważa się także przyczepy kempingowe i zamieszkałe namioty[19]. W orzecznictwie ETPC (Europejskiego Trybunału Praw Człowieka – dop. red.) w Strasburgu pojęcie m i e s z k a n i e odnosi się nie tylko do miejsc, w którym prowadzone jest życie prywatne i rodzinne, lecz także do wszelkich relacji międzyludzkich, a więc również o charakterze oficjalnym. Innymi słowy to, czy dane miejsce jest mieszkaniem, zależy od istnienia wystarczających |i trwałych związków z tym miejscem[20]. Lokale powszechnie dostępne dla nieokreślonej liczby osób (na przykład dworce kolejowe, lokale gastronomiczne, rozrywkowe, artystyczne) albo służące do przechowywania przedmiotów można przeszukiwać bez ograniczeń czasowych[21]. Przeszukania osoby i odzieży na niej należy dokonywać w miarę możności za pośrednictwem osoby tej samej płci (art. 223 kpk). Nie dotyczy to podręcznych przedmiotów tej osoby (torebka, walizka, teczka itd.). W szczególnych przypadkach przeszukanie może być dokonane za pośrednictwem osoby innej płci. Sytuacja wyjątkowa może wystąpić, gdy dokonuje się przeszukania w wypadkach niecierpiących zwłoki, określonych w art. 220 § 3 kpk. Do takiej sytuacji może dojść w momencie zatrzymania przez policjanta uciekającego przestępcy, którym okazuje się kobieta, i zachodzi uzasadnione przypuszczenie, że ma ona przy sobie niebezpieczne narzędzie, wcześniej użyte[22]. Znalezione przedmioty, po dokonaniu ich oględzin i sporządzeniu opisu, zabiera się lub oddaje na przechowanie osobie godnej zaufania z zaznaczeniem obowiązku przedstawienia ich na każde żądanie organu prowadzącego postępowanie. Dotyczy to także przedmiotów mogących stanowić dowód innego przestępstwa niż to, w odniesieniu do którego dokonywano czynności, rzeczy podlegających przepadkowi lub których posiadanie jest zabronione. Osobie zainteresowanej należy natychmiast wręczyć pokwitowanie stwierdzające, jakie przedmioty i przez kogo zostały zatrzymane[23].

[17] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), s. 536.
[18] Art. 230 § 1 kpk.
[19] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), …, s. 537.
[20] *Kodeks postępowania karnego. Komentarz*, t. 1, D. Świecki (red.)…, s. 732.
[21] *Postępowanie karne*, K.T. Boratyńska (red.), Warszawa 2015, s. 300.
[22] *Kodeks postępowania karnego. Komentarz*, t. 1, D. Świecki (red.), s. 733.
[23] Art. 228 kpk.

Istotnym narzędziem ochrony praw naruszonych przeszukaniem lub zatrzymaniem rzeczy oraz kontroli legalności i prawidłowości tych czynności jest możliwość zaskarżenia w drodze zażalenia wszelkich postanowień dotyczących dowodów rzeczowych oraz przeszukania i zatrzymania rzeczy. Środek odwoławczy przysługuje nie tylko stronom, lecz także każdej osobie, której prawa zostały naruszone przez wspomniane działania. Określenie właściwości sądu jako organu odwoławczego dodatkowo podkreśla znaczenie tego uprawnienia[24]. Jeśli te czynności zostały przeprowadzone w postępowaniu przygotowawczym, to zażalenie rozpoznaje sąd rejonowy, w którego okręgu toczy się postępowanie. Jeśli zaś postanowienie o przeszukaniu (także zatrzymaniu rzeczy czy dowodów rzeczowych) zostało wydane w toku postępowania jurysdykcyjnego, to zażalenie na to postanowienie rozpoznaje sąd nadrzędny. Jedynie w stosunku do decyzji referendarza sądowego przysługuje sprzeciw (art. 93a § 3 i art. 4 kpk). Powyższa regulacja jest skutkiem orzeczenia Trybunału Konstytucyjnego[25], który uznał, że brak możliwości wniesienia zażalenia do sądu na czynności prokuratora w toku postępowania przygotowawczego jest niezgodny z art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP.

### 1.2. Uregulowanie instytucji przeszukania w ustawie o działaniach antyterrorystycznych

Artykuł 25 ustawy o działaniach antyterrorystycznych aktualizuje uprawnienie Agencji Bezpieczeństwa Wewnętrznego do przeprowadzenia przeszukania. W przypadku podejrzenia przestępstwa o charakterze terrorystycznym lub usiłowania jego popełnienia albo przygotowania, w celu wykrycia, zatrzymania albo przymusowego doprowadzenia osoby podejrzewanej, a także w celu znalezienia rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, prokurator może postanowić o przeprowadzeniu przeszukania pomieszczeń i innych miejsc znajdujących się na wskazanym w postanowieniu obszarze, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że osoba podejrzewana lub wymienione rzeczy na tym obszarze się znajdują[26]. Dodatkowo, w celu znalezienia rzeczy wymienionych w tym artykule, można także dokonać przeszukania osób, ich odzieży i podręcznych przedmiotów, znajdujących się na obszarze wskazanym w postanowieniu[27]. Przeszukania można dokonać o każdej porze doby (art. 25 ust. 3). Postanowienie prokuratora należy okazać osobie, u której przeszukanie ma być przeprowadzone (art. 25 ust. 4). W zakresie nieuregulowanym w niniejszym artykule do przeszukania stosuje się przepisy *Kodeksu postępowania karnego*.

### 1.3. Analiza porównawcza uregulowania instytucji przeszukania

Zakres regulacji dotyczących instytucji przeszukania w ustawie o działaniach antyterrorystycznych został ograniczony podmiotowo do przypadków (…) *podejrzenia*

[24] D. Gruszecka *Zatrzymanie rzeczy i przeszukanie*…, s. 465.
[25] Wyrok TK z 3 VI 2018 r. (K 38/07, OTK-A 2008, nr 6 poz. 102).
[26] Art. 25 ust. 1 ustawy o działaniach antyterrorystycznych.
[27] Art. 25 ust. 2 ustawy o działaniach antyterrorystycznych.

*lub usiłowania popełnienia albo przygotowania przestępstwa o charakterze terrorystycznym*, dopuszczając możliwość całodobowego przeprowadzenia przeszukania. Należy jednak przypomnieć, że nie jest to nowatorskie rozwiązanie, gdyż *Kodeks postępowania karnego* w art. 221 zezwala – w uzasadnionych sytuacjach – na prowadzenie przeszukania w ciągu całej doby. Taką sytuacją jest zagrożenie o charakterze terrorystycznym, które uznawane jest za przypadek niecierpiący zwłoki[28]. Doktryna przyjmuje przy tym, że pod pojęciem przypadki niecierpiące zwłoki należy rozumieć konkretne okoliczności, które wskazują na możliwość ukrycia, przemieszczenia czy zniszczenia przedmiotów, a także ucieczki lub ukrycia się poszukiwanej osoby[29]. Tym samym już kodeksowe rozwiązanie pozwala na nocne przeszukania. Artykuł 25 ustawy o działaniach antyterrorystycznych *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, że ta przesłanka będzie stanowić dla służb specjalnych podstawę do przeprowadzania swoistych „przeszukań trałowych", a więc przeszukiwań dużej liczby pomieszczeń na danych obszarze, z nadzieją znalezienia konkretnej osoby. Ustawodawca 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 kpk). Zastępuje je natomiast wymogiem, aby istniały uzasadnione podstawy do przypuszczenia, że osoba podejrzana lub wymienione rzeczy znajdują się na danym obszarze[30].

Regulacje zawarte w *Kodeksie postępowania karnego* zezwalają na dokonanie przeszukania w celu znalezienia każdego dowodu, nie ograniczając tej przesłanki do znalezienia dowodów istotnych, znaczących, ważnych. Wątpliwe jest jednak dokonywanie przeszukania w celu znalezienia dowodu mało istotnego, pośredniego i pochodnego. Trywialnie rzecz ujmując, nie można poszukiwać za pomocą przeszukania wszystkiego i wszędzie. Przeszukanie powinno być przeprowadzane, gdy jest niezbędne dla pozyskania określonych dowodów do celów procesowych, ponieważ w inny sposób (mniej dolegliwy) nie da się ich pozyskać[31]. Niedopuszczalne jest wydanie postanowienia o przeszukaniu bez dokładnego wskazania (określenia) poszukiwanej rzeczy, poprzestając na poleceniu znalezienia np. rzeczy mogących stanowić dowód w sprawie. Taki sposób określenia przedmiotu przeszukania (nierzadki w praktyce) powoduje, że de facto to nie organ podejmujący decyzję o przeszukaniu, ale organ wykonujący tę czynność decyduje o tym, jaka rzecz może stanowić dowód w sprawie, a przez to podlegać zajęciu[32]. Artykuł 25 ust. 1 ustawy

[28] P. Niemczyk, *Jakoś to będzie – czyli ustawa antyterrorystyczna*, w: *Antyterroryzm. Polska i Świat,* Warszawa 2016, nr 4, s. 49.

[29] S. Steinborn, *Kodeks postępowania karnego. Komentarz do wybranych przepisów,* LEX/el 2016.

[30] *Uwagi Helsińskiej Fundacji Praw Człowieka do projektu ustawy o działaniach antyterrorystycznych* (druk sejmowy nr 516), http://www.hfhr.pl/wp-content/uploads/2016/05/HFPC_ustawa_antyterrorystyczna.pdf, s. 18 [dostęp: 12 V 2017].

[31] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 533.

[32] Tamże, s. 535.

o działaniach antyterrorystycznych daje prokuratorowi możliwość wydania postanowienia o przeprowadzaniu przeszukania pomieszczeń i innych miejsc znajdujących się na obszarze wskazanym w postanowieniu. W przypadku realizacji tego postanowienia mamy zdecydowanie szerszy zakres miejscowy i podmiotowy, gdyż w przypadku spraw kryminalnych przeszukanie dotyczy podejrzanego i pomieszczeń do niego należących (mowa jest tu o obszarze, co daje szersze możliwości). Przy takiej przesłance służby są uprawnione do przeszukiwania pomieszczeń mieszkalnych w całych dzielnicach. Zakładając więc, że np. domniemany terrorysta wsiadł w Warszawie na stacji metra Centrum do pociągu w kierunku Kabat, służby otrzymają kompetencję do tego, aby przeszukać wszystkie pomieszczenia na południe od stacji Centrum. Wydaje się, że wymogiem minimum do tak szerokiej ingerencji w prywatność obywateli powinno być przynajmniej powiązanie jej z najwyższymi stopniami zagrożenia terrorystycznego, które jest uregulowane w ustawie o działaniach antyterrorystycznych[33]. Wskazane rozwiązanie zastosowania postanowienia o przeszukaniu na danym obszarze byłoby bardzo interesujące zwłaszcza na gruncie cyberprzestępczości, cyberterroryzmu, gdzie przez analogię można by wydać postanowienie o przeszukaniu komputera sprawcy „X" i wszystkich z nim powiązanych, czyli w przypadku sieci np. kilkuset komputerów, na podstawie jednego postanowienia[34].

W wyroku z 28 kwietnia 2005 r. w sprawie Buck vs Niemcy (nr 41604/98, wyrok z 28 kwietnia 2005 r.) Europejski Trybunał Praw Człowieka zwrócił uwagę na konieczność uwzględnienia przy przeszukaniu ciężaru gatunkowego przestępstwa będącego przedmiotem sprawy, w której zarządzono przeszukanie, możliwości uzyskania poszukiwanej rzeczy w inny sposób, zastosowania niezbędnych zabezpieczeń, aby skutki przeszukania utrzymać w rozsądnych granicach, a także rozmiaru możliwych reperkusji dla reputacji osoby, wobec której dokonano przeszukania. W konkluzji Trybunał podkreślił, że przeszukanie pomieszczeń jest dopuszczalne tylko wtedy, gdy zdobycie niezbędnych dowodów winy osób oskarżonych nie jest możliwe w inny sposób[35].

W razie zatwierdzenia przez sąd lub prokuratora przeszukania, które zostało dokonane w sposób sprzeczny z ustawą (wbrew celowi i przesłance przeszukania), postanowienie dotyczy zatwierdzenia „nielegalnego przeszukania". Nie można jednak uznać, że takie następcze zatwierdzenie przeszukania powoduje, że przeszukanie dokonane w sposób sprzeczny z ustawą staje się legalne. To ustawa określa, pod jakimi warunkami przeszukanie może być przeprowadzone, a nie sąd lub prokurator. Jeżeli ustawowe przesłanki przeszukania nie zostały spełnione, to przeszukanie jest niezgodne z ustawą, a sąd lub prokurator takiej oceny nie mogą zmienić[36].

[33] *Uwagi Helsińskiej Fundacji Praw Człowieka do projektu ustawy o działaniach antyterrorystycznych*…, s. 18.

[34] W. Mądrzejowski, K. Wiciak, *Walka z przestępczością zorganizowaną na tle rozwiązań przyjętych w ustawie o działaniach antyterrorystycznych*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki (red.), Szczytno 2017, s. 413.

[35] D. Gruszecka *Zatrzymanie rzeczy i przeszukanie*…, s. 464.

[36] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 536.

Należy także odróżnić przeszukanie regulowane w art. 219 kpk od tzw. kontroli osobistej oraz przeglądania bagażu i ładunku w portach, na dworcach i w środkach transportu lądowego, powietrznego i wodnego, czyli pozaprocesowych instytucji przewidzianych przez ustawy szczególne. Materialną przesłanką dokonania kontroli osobistej przez wskazane organy jest istnienie uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary. Na gruncie *Kodeksu postępowania karnego* istnienie uzasadnionego podejrzenia popełnienia przestępstwa jest podstawą wszczęcia postępowania przygotowawczego (art. 303 kpk). Wobec tego, jeśli takie podejrzenie faktycznie występuje, należy wszcząć postępowanie karne albo postępowanie w niezbędnym zakresie i wówczas dokonywać czynności procesowych wskazanych w *Kodeksie*, w tym również przeszukania. W rzeczywistości kontrola osobista jest to przeszukanie, tylko dokonywane poza procesem karnym i nieunormowane w *Kodeksie postępowania karnego*[37].

Na szerszy zakres zastosowania art. 25 ustawy o działaniach antyterrorystycznych, a co za tym idzie na zakres zastosowania instytucji przeszukania, istotny wpływ ma także poszerzenie definicji pojęcia przestępstwo o charakterze terrorystycznym. Kodeksowa definicja stanowi, że przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu: poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczpospolitej Polskiej, lub innego państwa lub organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczpospolitej Polskiej, innego państwa lub organizacji międzynarodowej, a także groźba popełnienia takiego czynu. Ustawodawca wskazał w tej ustawie, aby ta definicja obejmowała wszystkie czyny zagrożone karą pozbawienia wolności do lat trzech, o ile zostały popełnione w jednym z opisanych wyżej celów. Niewątpliwie zmiana ta pozwala na włączenie w zakres pojęcia przestępstwo o charakterze terrorystycznym czynów zabronionych polegających na przygotowaniu do popełnienia określanego przestępstwa. Wśród tych czynów znajdują się m.in.: przygotowanie zamachu na jednostkę sił zbrojnych RP (art. 140 § 3 *Kodeksu karnego*), przygotowanie do sprowadzenia niebezpieczeństwa dla wielu osób poprzez sprowadzenie zagrożenia epidemiologicznego (art. 168 w zw. z art. 165 § 1 ust. 1 kk), przygotowanie do umieszczenia na statku powietrznym urządzenia zagrażającego bezpieczeństwu wielu osób (art. 168 w zw. z art. 167 § 1 kk)[38].

Rzecznik Praw Obywatelskich pozytywnie ocenił regulację zawartą w ust. 5 art. 25 ustawy o działaniach antyterrorystycznych, w świetle której w zakresie nieuregulowanym w art. 25 tej ustawy w stosunku do przeszukania znajdują zastosowanie przepisy *Kodeksu postępowania karnego*. Oznacza to, że w takich sytuacjach powinno się powołać na art. 236 kpk. Zgodnie z nim osobom, których prawa zostały naruszone,

[37] *Kodeks postępowania karnego. Komentarz*, t. 1, D. Świecki (red.)…, s. 729.
[38] *Uwagi Helsińskiej Fundacji Praw Człowieka do projektu ustawy o działaniach antyterrorystycznych*…, s. 19, 20.

przysługuje zażalenie[39]. Europejski Trybunał Praw Człowieka[40] uznał, że w przypadku postępowań odnoszących się do przestępstw o charakterze terrorystycznym znajduje uzasadnienie umożliwienie dokonania przeszukania lub zatrzymania na podstawie przesłanki określonej szerzej niż w innych sytuacjach. Trybunał Konstytucyjny wskazał, że nie jest naruszeniem *Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności* przeprowadzenie przeszukania w warunkach wskazanych powyżej, w sytuacji gdy przysługuje środek zaskarżenia ww. czynności.

W ocenie autora rozszerzenie katalogu przesłanek umożliwiających dokonanie przeszukania w przypadkach odnoszących się do przestępstw o charakterze terrorystycznym jest z jednej strony rozwiązaniem pozytywnie wpływającym na szybkość prowadzonego postępowania i może skutkować odnalezieniem dowodów, które podczas przeszukania przeprowadzonego w sposób „klasyczny", mogłyby nie ujrzeć światła dziennego. Jednocześnie pozostaje możliwość nadużycia uprawnień przez służby, które mogą podciągnąć pod poważne przestępstwo o charakterze terrorystycznym także mniej groźne delikty, zgodnie z zasadą, że cel uświęca środki. Definicję przestępstwa o charakterze terrorystycznym należy jeszcze bowiem poddać ocenie.

## 2. Przedstawienie zarzutów

Bardzo ważną czynnością w toku postępowania przygotowawczego jest przedstawienie zarzutów. Została ona uregulowana w art. 313 i 325g kpk. Przedstawienie zarzutów warunkuje uzyskanie statusu podejrzanego, korzystanie z uprawnień z nim związanych oraz umożliwia podejrzanemu poznanie stawianych mu zarzutów oraz przygotowanie swojej obrony[41]. Postępowanie przygotowawcze od momentu jego wszczęcia toczy się w sprawie (*in rem*). Dzieje się tak aż do chwili, gdy organ postępowania przygotowawczego ustali sprawcę przestępstwa i postępowanie skieruje przeciwko tej osobie (*ad personam*). Od momentu przedstawienia zarzutów osoba podejrzana (czasami nazywana też podejrzewanym) o popełnienie przestępstwa formalnie staje się podejrzanym, któremu przysługuje wiele uprawnień procesowych, zwłaszcza prawo do obrony[42]. Instytucja przedstawienia zarzutów jest istotna z punktu widzenia terminów. Zgodnie z art. 102 kk wszczęcie postępowania przeciwko osobie skutkuje wydłużeniem okresu przedawnienia o pięć lat.

### 2.1. Uregulowanie instytucji przedstawienia zarzutów w *Kodeksie postępowania karnego*

Przedstawienie zarzutów, zgodnie z art. 313 § 1 kpk, powinno nastąpić, jeżeli dane istniejące w chwili wszczęcia śledztwa lub zebrane w jego toku dostatecznie uzasadniają podejrzenie, że czyn popełniła określona osoba. Wymagany jest więc pewien

[39] Opinia Rzecznika Praw Obywatelskich do projektu ustawy o działaniach antyterrorystycznych (druk sejmowy nr 516) z dnia 19 maja 2016 r., s. 16.
[40] Orzeczenie w sprawie Sher i inni przeciwko Zjednoczonemu Królestwu, nr 5201/11.
[41] T. Boratyńska, Ł. Chojniak, W. Jasiński, *Postępowanie karne,* Warszawa 2015, s. 405.
[42] K. Kremens, *Przedstawienie zarzutów*, w: *Proces karny,* J. Skorupka (red.), Warszawa 2017, s. 554.

poziom uprawdopodobnienia opartego na informacjach uzyskanych w toku postępowania (np. przeprowadzonych oględzin, przeszukań, zeznań świadków), że dana osoba popełniła czyn, który ma zostać jej zarzucony. Pojęcie dostatecznie uzasadnione podejrzenie popełnienia czynu nie zostało bliżej określone przez ustawodawcę, jednak pewną wskazówką może być określenie w ustawie przesłanek do wszczęcia śledztwa i stosowania środków zapobiegawczych. Stanowią one bowiem odpowiednio uzasadnione podejrzenie popełnienia przestępstwa (art. 303 kpk) oraz duże prawdopodobieństwo popełnienia przestępstwa (art. 249 § 1 kpk)[43]. Podobny pogląd przedstawił Sąd Najwyższy w swojej uchwale: *Porównanie treści art. 303 z treścią art. 313 kpk prowadzi do jednoznacznego wniosku, że dostatecznie uzasadnione podejrzenie w odniesieniu do konkretnej osoby oznacza wyższy stopień podejrzenia tak co do faktu popełnienia przestępstwa, jak co do osoby sprawcy. Nie chodzi zatem o ustalenie, że określona osoba popełniła przestępstwo, lecz o to, że zebrane dowody wskazują na wysokie prawdopodobieństwo zaistnienia tego faktu*[44].

W celu przedstawienia zarzutów konieczne jest wykonanie trzech czynności wskazanych w omawianym przepisie: sporządzenie postanowienia o przedstawieniu zarzutów, niezwłoczne ogłoszenie postanowienia podejrzanemu i przesłuchanie podejrzanego[45]. Wyjątkiem jest sytuacja, w której osoba podejrzana ukrywa się lub jest nieobecna w kraju. Wówczas, z oczywistych względów, dopuszczalne jest wydanie wyłącznie postanowienia o przedstawieniu zarzutów. Osoba, której to postanowienie dotyczy, staje się tym samym podejrzanym.

Wątpliwości w doktrynie budzi moment nabycia statusu podejrzanego w przypadku, gdy dana osoba nie ukrywa się i jest obecna w kraju. Spór dotyczy bowiem tego, czy momentem wydania postanowienia o przedstawieniu zarzutów w rozumieniu art. 71 § 1 kpk jest sporządzenie postanowienia o przedstawieniu zarzutów (i załączenia go do akt sprawy), czy też dokonanie czynności ogłoszenia postanowienia podejrzanemu i przesłuchania go. Według W. Jasińskiego należy przychylić się do tego drugiego stanowiska. Przemawiają za nim względy gwarancyjne. Niekonsekwencja terminologiczna ustawodawcy dostarcza niestety kontrargumentów natury językowej oraz systemowej, które są podnoszone przez zwolenników stanowiska, że wydanie postanowienia o przedstawieniu zarzutów należy rozumieć jako jego sporządzenie[46]. Wydanie postanowienia jest pojęciem szerszym, gdyż polega również na uzewnętrznieniu jego treści[47]. Pomiędzy terminami wydanie postanowienia z art. 71 § 1 kpk a sporządzenie postanowienia z art. 313 § 1 kpk zachodzi istotna różnica, gdyż dla wydania jest niezbędne dopełnienie kolejnych czynności procesowych wskazanych w tym drugim przepisie, określanych jako promulgacja postanowienia, która jest z kolei konieczna dla skuteczności tej czynności procesowej. Tym samym dla przyjęcia,

[43] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)..., s. 754.
[44] Uchwała Sądu Najwyższego z 23 lutego 2006 r., SNO 3/06, OSN - Sądu Dyscyplinarnego 2006, nr 1 poz. 25.
[45] K. Kremens, *Przedstawienie zarzutów*…, s. 555.
[46] T. Boratyńska, Ł. Chojniak, W. Jasiński, *Postępowanie karne*…, s. 406.
[47] K. Kremens, *Przedstawienie zarzutów*…, s. 555.

że nastąpiło przekształcenie się postępowania z fazy *in rem* w fazę *in personam*, nie jest, poza wypadkami wskazanymi w art 313 § 1 kpk, wystarczające sporządzenie postanowienia o przedstawieniu zarzutów, lecz niezbędne jest również jego ogłoszenie podejrzanemu. Aktualnie katalog okoliczności zwalniających z obowiązku natychmiastowej promulgacji postanowienia o przedstawieniu zarzutów jest katalogiem zamkniętym. Jak stwierdził Sąd Najwyższy, niezwłoczne ogłoszenie nie oznacza nic innego, jak ogłoszenie w możliwie najszybszym czasie, bez zbędnych przerw, a więc już w momencie sporządzenia postanowienia o przedstawieniu zarzutów powinny zostać podjęte także czynności związane z wezwaniem podejrzanego do stawiennictwa w realnym terminie i, jeżeli nie wystąpią przeszkody wymienione w art. 313 § 1 kpk, obowiązkiem organu ścigania jest wykonanie czynności (sporządzenie, ogłoszenie i przesłuchanie podejrzanego) wymienionych w tym przepisie w możliwie krótkich odstępach czasu, bez nieuzasadnionej zwłoki, co nie oznacza „natychmiast". Obowiązek niezwłocznego ogłoszenia postanowienia o przedstawieniu zarzutów ciąży tym samym na organie procesowym i opóźnienie w tym względzie jest możliwe wyłącznie z przyczyn praktycznych (ukrywanie się podejrzanego lub jego nieobecność w kraju)[48]. Ze względów gwarancyjnych, jakie dla obrony podejrzanego ma uzyskanie przez niego pozycji procesowej adekwatnej do ustaleń postępowania, nie jest dopuszczalne opóźnianie wydania postanowienia o przedstawieniu zarzutów. Opóźnienia nie uzasadnia nawet przyjęta taktyka śledcza[49].

Promulgacja postanowienia jest obowiązkowa, ale jedynie wtedy, gdy jest to w ogóle możliwe wobec danej osoby, i wówczas ma to nastąpić niezwłocznie. W innych wypadkach sporządzenie i podpisanie postanowienia oznacza, ze zostało ono wydane, a ogłoszenie go podejrzanemu nastąpi dopiero wtedy, gdy będzie to możliwe, i wówczas niezwłocznie po powstaniu owej możliwości[50].

Postanowienie o przedstawieniu zarzutów w śledztwie wydaje wyłącznie prokurator, nawet jeśli zostało ono powierzone innemu organowi (art. 311 § 3 kpk). Także w postępowaniu w niezbędnym zakresie, jeżeli sprawa ma być prowadzona w formie śledztwa, postanowienie o przedstawieniu zarzutów może wydać jedynie prokurator (art. 308 § 4 kpk). Postanowienie o przedstawieniu zarzutów musi spełniać wymogi formalne wskazane w art. 313 § 2 kpk:

1) wymogi wynikające z art. 94 § 1 kpk (tj. ogólne wymagania stawiane przed każdym wydawanym postanowieniem),
2) wskazanie podejrzanego (dane identyfikacyjne sprawcy – imię i nazwisko, a w razie potrzeby także inne dane, np. imię ojca, data i miejsce urodzenia),
3) precyzyjne określenie zarzucanego czynu,
4) precyzyjne określenie kwalifikacji prawnej czynu (wskazanie przepisu prawa materialnego określającego typ czynu zabronionego, którego znamiona wyczerpuje popełniony czyn).

[48] *Kodeks karny, Kodeks postępowania karnego. Orzecznictwo*, Warszawa 2015, s. 738 i nast.
[49] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 754.
[50] Wyrok Sądu Najwyższego z 2 czerwca 2010 r., V KK 376/09.

Postanowienie o przedstawieniu zarzutów nie musi zawierać uzasadnienia – przeciwnie z art. 313 § 3 kpk.

Do czasu zawiadomienia o terminie zapoznania się z materiałami śledztwa podejrzany może żądać podania mu ustnie podstaw zarzutów, a także sporządzenia uzasadnienia na piśmie, o czym należy go pouczyć (art. 313 § 3 kpk). Potwierdzeniem pouczenia podejrzanego o prawie żądania podania ustnie podstaw zarzutów, a także o prawie żądania sporządzenia uzasadnienia tego postanowienia jest podpis podejrzanego[51]. W uzasadnieniu należy przede wszystkim wskazać, jakie fakty i dowody zostały przyjęte za podstawę zarzutów (art. 313 § 4 kpk). To uzasadnienie należy doręczyć podejrzanemu i jego obrońcy w terminie 14 dni (art. 313 § 3 kpk).

Wydanie postanowienia o przedstawieniu zarzutów jest konieczną przesłanką zastosowania środków zapobiegawczych, np. tymczasowego aresztowania czy poręczenia majątkowego. Zgodnie z art. 249 § 2 kpk w postępowaniu przygotowawczym środki zapobiegawcze można stosować jedynie wobec osoby, której wydano postanowienie o przedstawieniu zarzutów, a nie wobec takiej, którą poinformowano o treści zarzutu w związku z przesłuchaniem w charakterze osoby podejrzanej (art. 308 § 2 kpk). W tym ostatnim przypadku, jeżeli jest planowane zastosowanie środka zapobiegawczego, konieczne jest wydanie odrębnego postanowienia o przedstawieniu zarzutów[52].

Zarzut przedstawiony podejrzanemu może obejmować czyn, który w rzeczywistości przebiegał inaczej, lub też nie obejmować wszystkich czynów zabronionych popełnionych przez podejrzanego. Stąd może wystąpić potrzeba zmiany zarzutów lub ich uzupełnienia. Zmiana zarzutów oznacza konieczność zarzucenia podejrzanemu czynu w postaci zmienionej w istotny sposób lub też konieczność zakwalifikowania czynu z surowszego przepisu. Uzupełnienie zarzutów to konieczność zarzucenia podejrzanemu czynu nieobjętego wydanym uprzednio postanowieniem o przedstawieniu zarzutów (art. 314 kpk). Zmiana oraz uzupełnienie zarzutów następują w formie postanowienia i podlegają tym samym wymogom formalnym co postanowienie o przedstawieniu zarzutów (art. 313 § 2 kpk). Podejrzanemu przysługuje również prawo do żądania uzasadnienia nowego postanowienia na analogicznych zasadach jak przy przedstawieniu zarzutów. Jeżeli zmiana nie miałaby istotnego charakteru lub też miałaby polegać na zakwalifikowaniu czynu z przepisu łagodniejszego, to nie ma potrzeby wydawania odrębnego postanowienia. O treści postanowienia o uzupełnieniu lub zmianie zarzutów należy zawiadomić pokrzywdzonego (art. 100 § 5 w zw. z art. 106 kpk)[53]. Konieczność zmiany zarzutów nie obliguje prokuratora do przedstawienia zarzutów jeszcze przed zakończeniem realizowanych w toku śledztwa czynności operacyjno-rozpoznawczych lub procesowej czynności dowodowej, podczas której uzyskano materiał dowodowy wskazujący na istnienie takiego uzasadnionego podejrzenia popełnienia czynu[54].

[51] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 757.
[52] Tamże, s. 556.
[53] Tamże, s. 557.
[54] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 755.

Zgodnie z art. 325g § 1 kpk nie jest wymagane sporządzenie postanowienia o przedstawieniu zarzutów. Organ prowadzący dochodzenie może zatem samodzielnie zdecydować, czy postąpi zgodnie z procedurą unormowaną w art. 313 kpk, czy też wybierze uproszczoną formułę przedstawienia zarzutów z art. 325g kpk. W przypadku odstąpienia od wydania postanowienia o przedstawieniu zarzutów, przesłuchanie osoby podejrzanej należy zacząć od powiadomienia jej o treści zarzutu wpisanego do protokołu przesłuchania.

Z chwilą wydania postanowienia o przedstawieniu zarzutów wobec danej osoby, a także w momencie, gdy takiej osobie zdecydowano się postawić zarzut w trybie czynności w niezbędnym zakresie (art. 308 kpk) lub w dochodzeniu (art. 325g § 1 i 2 kpk) bez wydawania takiego postanowienia w związku z przystąpieniem do przesłuchania w charakterze podejrzanego, taka osoba uzyskuje formalnie status podejrzanego (art. 71 § 1 kpk). Oznacza to przejście postępowania przygotowawczego z fazy *in rem* w fazę *ad personam*. Podejrzany to osoba, co do której wydano postanowienie o przedstawieniu zarzutów, albo wobec której – bez wydania takiego postanowienia – postawiono zarzut w związku z przystąpieniem do przesłuchania w charakterze podejrzanego. Należy podkreślić, że uproszczony sposób przedstawienia zarzutów ma charakter fakultatywny. Nie ma zatem przeszkód, aby w dochodzeniu wydać jednak postanowienie o przedstawieniu zarzutów. Wydanie takiego postanowienia jest natomiast obligatoryjne w przypadku, kiedy podejrzany jest tymczasowo aresztowany (art. 325g § 1 kpk), a także w przypadku, gdy mają zostać zastosowane w stosunku do niego nieizolacyjne środki zapobiegawcze (art. 249 § 2 kpk)[55].

Podejrzany, zgodnie z art. 299 § 1 kpk, jako strona postępowania przygotowawczego posiada wiele uprawnień. W myśl art. 300 § 1 kpk podejrzanego przed pierwszym przesłuchaniem należy pouczyć o:

1) prawie do składania wyjaśnień, do odmowy składania wyjaśnień lub odmowy odpowiedzi na pytania,
2) prawie do informacji o treści zarzutów i ich zmianach,
3) prawie do składania wniosków o dokonanie czynności śledztwa lub dochodzenia,
4) prawie do korzystania z pomocy obrońcy (art. 84 kpk), w tym do wystąpienia o obrońcę z urzędu w wypadku określonym w art. 78 kpk (obrońca ubogiego podejrzanego),
5) prawie do końcowego zaznajomienia z materiałami postępowania przygotowawczego (art. 321 kpk),
6) prawie do skorzystania z mediacji w postępowaniu karnym (art. 23a § 1 kpk),
7) prawie do korzystania z bezpłatnej pomocy tłumacza (art. 72 § 1 kpk),
8) prawie do wglądu w akta postępowania (art. 156 § 5 i 5a kpk),
9) prawie do żądania bycia przesłuchanym z udziałem ustanowionego obrońcy, z tym że nieobecność obrońcy nie tamuje przesłuchania (art. 301 kpk),
10) prawie do uzgodnienia z prokuratorem treści wniosku o wydanie wyroku i wymierzenie przez sąd ustalonych kar lub innych środków bez przeprowadzania dowodów (art. 335 kpk),

[55] T. Boratyńska, Ł. Chojniak, W. Jasiński, *Postępowanie karne*…, s. 407.

11) prawie do samodzielnego złożenia wniosku o wydanie wyroku i wymierzenie przez sąd ustalonych kar lub innych środków bez przeprowadzania dowodów, w terminie – do doręczenia zawiadomienia o terminie rozprawy (art. 338a kpk),
12) prawie do samodzielnego złożenia wniosku o wydanie wyroku i wymierzenie określonej kary lub innych środków bez przeprowadzania postępowania dowodowego, w terminie – do chwili zakończenia pierwszego przesłuchania wszystkich oskarżonych (art. 387 kpk),
13) obowiązku poddania się oględzinom ciała i innym czynnościom wynikającym z art. 74 kpk oraz konsekwencjach wynikających z niepoddania się tym czynnościom, w tym zatrzymaniu i przymusowemu doprowadzeniu (art. 74 § 3a kpk),
14) obowiązku stawiania się na każde wezwanie w toku postępowania karnego oraz zawiadamiania organu prowadzącego postępowanie o każdej zmianie miejsca zamieszkania lub pobytu (art. 75 § 1 kpk) oraz o konsekwencjach wynikających z niepoddania się tym czynnościom, w tym zatrzymaniu i przymusowemu doprowadzeniu (art. 75 § 2 kpk),
15) obowiązku wskazania adresu, na który będzie kierowana korespondencja, oraz konsekwencjach jego niewskazania (art. 133 § 2 kpk),
16) obowiązku wskazania adresata dla doręczeń w kraju przez podejrzanego przebywającego za granicą oraz konsekwencjach jego niewskazania (art. 138 kpk),
17) konsekwencjach zmiany miejsca zamieszkania lub nieprzebywania pod adresem wskazanym (art. 139 kpk) – tzw. doręczenie fikcyjne.

Zanim dana osoba stanie się podejrzanym, może być traktowana przez pewien czas w postępowaniu jako osoba podejrzana (gdzieniegdzie w literaturze nazywana podejrzewanym). Osoba podejrzana (podejrzewany) to osoba, co do której organy mają informacje typujące ją na sprawcę przestępstwa i wobec której kierują postępowanie, ale jeszcze formalnie nie przedstawiono jej zarzutów. Osoba podejrzana nie jest stroną postępowania przygotowawczego i nie dysponuje takimi uprawnieniami jak podejrzany. Nie ma prawa do obrony i prawa do odmowy złożenia wyjaśnień. Wobec takiej osoby można zastosować niektóre czynności procesowe, np. zatrzymanie (art. 244 § 1 i art. 247 § 1 kpk) lub kontrolę i utrwalanie rozmów (art. 237 § 4 kpk), pomimo braku przedstawienia jej zarzutów. Nie można jednak twierdzić, że osobą podejrzaną jest osoba, wobec której – z naruszeniem art. 313 kpk – zwleka się z wydaniem postanowienia o przedstawieniu zarzutów, i jest nią aż do czasu wydania tego postanowienia. Samo wskazanie w art. 74 § 3 kpk zakresu czynności, których wolno dokonać wobec osoby podejrzanej, świadczy o dostrzeganiu przez ustawodawcę jej szczególnej sytuacji procesowej – właśnie ze względu na jakościowo odmienny (od określonego w art. 313 § 1 kpk) stan dowodów obciążających. Można też nie mieć wątpliwości, że osoba podejrzana może być – bez naruszenia prawa – przesłuchana w charakterze świadka, jednak tylko do chwili, kiedy stan dowodów ją obciążających osiągnie poziom wskazany w art. 313 § 1 kpk. W konsekwencji, osoba przesłuchana w charakterze świadka wbrew wynikającemu

z art. 313 § 1 kpk nakazowi przesłuchania jej jako podejrzanego nie ponosi odpowiedzialności karnej na podstawie art. 233 § 1 kk (składanie fałszywych zeznań)[56].

### 2.2. Uregulowanie instytucji przedstawienia zarzutów w ustawie o działaniach antyterrorystycznych

W przypadku podejrzenia popełnienia 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 wymienionych w art. 9 ustawy o działaniach antyterrorystycznych[57]. Należą do nich czynności polegające na:

1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych,
2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne,
3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej,
4) uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych.
5) uzyskiwaniu dostępu i kontroli zawartości przesyłek.

Powyższe czynności mogą być przeprowadzane niejawnie, nie dłużej niż trzy miesiące[58].

### 2.3. Analiza porównawcza uregulowania instytucji przedstawienia zarzutów

Według Helsińskiej Fundacji Praw Człowieka podstawowe wątpliwości wiążą 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 kpk, w którym wprost jest mowa o dowodach. W ocenie Helsińskiej Fundacji Praw Człowieka tego pojęcia nie da się skutecznie odnieść do informacji z czynności operacyjno-rozpoznawczej, o której mowa w art. 26 ustawy o działaniach antyterrorystycznych. Co więcej, regulacja zawarta w tym przepisie może prowadzić do ograniczenia prawa do obrony podejrzanego. W związku z tym, że informacje gromadzone w ramach czynności operacyjno-rozpoznawczych mają charakter niejawny, przeglądanie akt postępowania, sporządzanie z nich odpisów i kopii będzie odbywało się w trybie określonym w art. 156 § 4 kpk, co samo w sobie jest dość uciążliwe. Ponadto wydaje się, że przez użycie materiałów niejawnych dosyć częste zastosowanie będzie miała regulacja art. 156 § 5 kpk pozwalająca odmówić udostępnienia akt postępowania stronom, ze względu na ochronę interesu państwa[59].

[56] *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.)…, s. 755.
[57] Art. 26 ustawy o działaniach antyterrorystycznych.
[58] Art. 9 ustawy o działaniach antyterrorystycznych.
[59] *Uwagi Helsińskiej Fundacji Praw Człowieka do projektu ustawy o działaniach antyterrorystycznych*…, s. 21.

Sporządzenie postanowienia o przedstawieniu zarzutów nie jest uzależnione od uzyskania informacji innych niż z czynności operacyjno-rozpoznawczych. Warunkiem jest „dostateczne uzasadnienie podejrzenia", które jest pozostawione ocenie prokuratora[60]. Paweł Lubniewski ocenia zapis art. 26 ustawy o działaniach antyterrorystycznych jako uprawniający do stosowania sankcji karnych: *To niezwykle usprawniający system instrument pozwalający odpowiednio wcześnie rozpocząć pracę z osobą, wobec której istnieją przesłanki pozaprocesowe świadczące o powiązaniach z terroryzmem w charakterze osoby podejrzanej*[61]. Podobnie oceniają tę regulację Wiesław Mądrzejowski i Krzysztof Wiciak: (...) *częstokroć istnieją problemy z szybkim pozyskaniem materiału dowodowego, a organy ścigania dysponują li tylko wiedzą operacyjną, w takich sytuacjach wydłużenie czasu na podjęcie działań i możliwość postawienia zarzutów w oparciu o materiał operacyjny byłaby nieoceniona dla efektywności działania organów ścigania*[62].

**Podsumowanie**

Celem tej pracy była analiza i próba oceny ustawodawstwa polskiego w obszarze zagrożeń terrorystycznych i przeanalizowanie konkretnych instytucji karnoprocesowych na tle gwarancji konwencyjnych i konstytucyjnych. Gruntownej analizie została poddana ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych, która jest pierwszym w historii polskiego ustawodawstwa kompleksowym rozwiązaniem legislacyjnym, unifikującym i regulującym wszystkie uprawnienia i obowiązki służb i organów procesowych w sytuacji zagrożenia o charakterze terrorystycznym. W ustawie zastosowano nowe regulacje, które stanowią wyjątek w stosunku do zapisów *Kodeksu postępowania karnego*. Badanie przyczyn, dla których ten stan prawny jest inny niż w *Kodeksie postępowania karnego*, zostało przeprowadzone na podstawie analizy porównawczej i opinii instytucji pozarządowych i Rzecznika Praw Obywatelskich. Różnice w stanie prawnym zostały poddane ocenie. Przytaczano również opinie instytucji takich, jak Helsińska Fundacja Praw Człowieka czy Amnesty International. Wiele zmian wprowadzonych przez ustawę o działaniach antyterrorystycznych budzi wątpliwości natury konwencyjnej i konstytucyjnej, mimo słusznych przesłanek ich stosowania w uzasadnionych przypadkach.

Autor skupił się na omówieniu prawnokarnych regulacji zawartych w ustawie o działaniach antyterrorystycznych. Dogłębnej analizie poddał również instytucję przeszukania i instytucję przedstawienia zarzutów, które uległy istotnym modyfikacjom. Przy ich badaniu posłużono się m.in. Europejską Konwencją Praw Człowieka oraz opiniami Rzecznika Praw Obywatelskich i instytucji pozarządowych, takich jak Fundacja Panoptykon, Amnesty International oraz Helsińska Fundacja Praw Człowieka. W analizie wykorzystano także bogate orzecznictwo Trybunału Konstytucyjnego i Sądu Najwyższego.

[60] P. Lubniewski, *Ustawa antyterrorystyczna wobec służb specjalnych. Rozszerzenie czy aktualizacja uprawnień?*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki (red.) Szczytno 2017, s. 318.
[61] Tamże, s. 329.
[62] W. Mądrzejowski, K. Wiciak, *Walka z przestępczością zorganizowaną*…, s. 413.

Wprowadzone zmiany często są konieczne, aby walka z terroryzmem była efektywna. Nowe uprawnienia mogą naruszać prywatność obywateli i istnieje ryzyko godzenia w prawa obywatelskie, ale mogą też prowadzić do sprawniejszego i skuteczniejszego działania służb, a co za tym idzie – do zapobieżenia kolejnym atakom terrorystycznym i ocalenia istnień ludzkich. Realne niebezpieczeństwo, jakie niesie za sobą terroryzm XXI wieku, powinno zmusić ludzi do zmiany sztywnego i ortodoksyjnego podejścia do ochrony praw człowieka i prywatności. Mimo pozostawionych luk prawnych czy nieprecyzyjnych określeń, służby odpowiedzialne za bezpieczeństwo wewnętrzne i organy procesowe powinny mieć komfort pracy nad zapobieganiem skutkom terroryzmu. Zbyt wiele krwi zostało przelanej, aby dzisiaj protestować przeciwko zmianom niedotyczącym praworządnych obywateli lub dotykających ich w sposób iluzoryczny. Życie ludzi jest dobrem najwyższym, zdecydowanie wyższym niż poczucie prywatności, która w erze mediów społecznościowych jest bardzo złudna.

**Bibliografia:**

Aleksandrowicz T.R., *Bezpieczeństwo w Unii Europejskiej*, Warszawa 2011, Difin.

Aleksandrowicz T.R., *Terroryzm międzynarodowy*, Warszawa 2015, (b.w.).

Bielecki T., *Zamachy w Brukseli. Belgia podnosi alarm terrorystyczny do najwyższego stopnia*, „Gazeta Wyborcza" z 22 marca 2016 r.

Bolechów B., *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2002, Adam Marszałek.

Cichomski M., Zubrzycki W., *Notatka służbowa dotycząca zawieszenia prac Zespołu Zadaniowego do Opracowania Szczegółowych Założeń do Ustawy o Rozpoznawaniu, Przeciwdziałaniu i Zwalczaniu Terroryzmu*, Warszawa 2010, Departament Analiz i Nadzoru MSWiA.

Dominik E., *Said i Cherif Kouachi – kim są zabójcy z Charlie Hebdo*, http:// www.polskatimes.pl/artykul/3709524,said-i-cherif-kouachi-kim-sa-zabojcy-z-charlie-hebdo,id,t.html [dostęp: 18 XI 2016].

*Encyklopedia terroryzmu*, Warszawa 2004, Muza, Bellona.

Grotowicz V., *Terroryzm w Europie Zachodniej*, Warszawa 2000, Wydawnictwo Naukowe PWN.

Grzegorczyk T., Tylman J., *Polskie postępowanie karne*, Warszawa 2014, LexisNexis.

Hoc S., *O penalizacji przestępstw o charakterze terrorystycznym*, „Wojskowy Przegląd Prawniczy" 2004 (b.nr).

Hoffman B., *Oblicza terroryzmu*, Warszawa 1999, Świat Książki.

Kalińska A., *Ustawa antyterrorystyczna. Nowa wersja jeszcze bardziej restrykcyjna*, http:// www.money.pl/gospodarka/wiadomosci/artykul/ustawa-antyterrorystyczna-nowa-wersja, 216,0,2075864.html [dostęp: 18 XI 2016].

Kałan D., Rękawek K., *Gorączka antyterrorystyczna na Słowacji i Węgrzech – lekcje dla Polski*, „Biuletyn" 2016, nr 12, PISM.

*Kodeks karny, Kodeks postępowania karnego. Orzecznictwo*, Warszawa 2015, CH Beck.

*Kodeks postępowania karnego. Komentarz*, t. 1, D. Świecki (red.), Warszawa 2015, C.H. Beck.

*Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2015, C.H. Beck.

*Konstytucja RP*, t. 1: *Komentarz do art. 1–86*, M. Safjan, L. Bosek (red.), 2016, Legalis/el.

Laquer W., *Reflections on Terrorism*, „Foreign Affairs" (b.r. i nr).

Marszałek P.K., *Polskie ustawodawstwo antyterrorystyczne a prawa człowieka*, „Studia Lubuskie" 2016, t. 12.

Moszyński P., *Zamachy w Paryżu. Stolica Francji spłynęła krwią*, „Gazeta Wyborcza" z 14 listopada 2015 r.

*Narodowy Program Antyterrorystyczny na lata 2015–2019* (M.P. z 2014 r. poz. 1218).

Niemczyk P., *Jakoś to będzie - czyli ustawa antyterrorystyczna*, „Antyterroryzm. Polska i Świat" 2016, (b.w.).

*Pattern of Global Terrorism*, Washington 2003, US Department of State.

Pawłowski W., *Terroryzm hybrydowy*, „Gazeta Wyborcza" z (b.d.) 2016.

*Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki (red.), Szczytno 2017, WSPol.

*Postępowanie karne*, K.T. Boratyńska (red.), Warszawa 2015, C.H. Beck.

*Proces karny*, J. Skorupka (red.), Warszawa 2017, Wolters Kluwer.

Przybylski J., *W Polsce ofiar byłoby dużo więcej*, „Do Rzeczy" z 30 marca 2016 r.

*Raport alternatywny Amnesty International do Komitetu Praw Człowieka ONZ*, https:// amnesty.org.pl/wp-content/uploads/2016/11/Raport-alternatywny-dla-Komitetu-Praw- Człowieka-ONZ.pdf [dostęp: 18 XI 2016].

Schmahl S., *Wpływ wydarzeń z 11 września na niemieckie ustawodawstwo dotyczące cudzoziemców i politykę imigracyjną*, Warszawa 2004, Instytut Spraw Publicznych.

Skwara M., *Szkolny front w wojnie z terroryzmem*, http://www.england.pl/aktualnosci/wielka- brytania/news.html?n=3399 [dostęp: 18 XI 2016].

*Slovakia approves restrictive church law targeting Muslims*, http://www.foxnews.com/world/2017/01/31/slovakia-approves-restrictive-church-law-targeting-muslims.html [dostęp: 18 XI 2016].

*Słownik języka polskiego PWN*, http://sjp.pwn.pl/sjp/terroryzm;2578078.html.

Solana J., *Bezpieczna Europa w lepszym świecie. Europejska strategia bezpieczeństwa*, Bruksela 2003, http://consilium.europa.eu/uedocs/cmsUpload/031208ESSIIPL.pdf [dostęp: 18 XI 2016].

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

*The Attacks on Paris: Lessons Learned*, https://static1.squarespace.com/static/5782ad8f9de4bb114784a8fe/t/5783fec9d482e95d4e0b79bf [dostęp: 18 XI 2016].

*The New Oxford Dictionary of English*, Oxford University Press, Oxford 1998.

*Ustawa antyterrorystyczna wchodzi w życie – co się zmienia*, Fundacja Panoptykon, 1 VII 2016 r., https://panoptykon.org/wiadomosc/ustawa-antyterrorystyczna-wchodzi-w-zycie-co-sie- zmienia [dostęp: 18 XI 2016].

*Uwagi Helsińskiej Fundacji Praw Człowieka do projektu ustawy o działaniach antyterrorystycznych* (druk sejmowy nr 516), 987/2016/MPL.

Utrat-Milecki J., *Polityczność przestępstwa*, Warszawa 1997, Wydawnictwo UW.

Wassermann J., *Templariusze i asasyni. Dwa tajemnicze zakony – chrześcijańskich templariuszy i muzułmańskich asasynów*, Warszawa 2007, Bellona.

Wojciechowski S., *Terroryzm. Analiza Pojęcia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1, s. 54–60.

*Współczesne wymiary polskiej polityki bezpieczeństwa*, M. Górka (red.), Warszawa 2015, Difin.

**Akty prawne i inne dokumenty:**

*Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r*. (Dz.U. z 1997 r. nr 78 poz. 483, ze zm.).

*Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia*

*postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/ WSiSW* (Dz. Urz. UE L 119 z 4 V 2016 r., s. 89).

*Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

*Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. z 2017 r. poz. 1920, ze zm.).

*Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: Dz.U. z 2018 r. poz. 1987).

*Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (Dz.U. z 2018 r. poz. 1600, ze zm.).

*Ustawa z dnia 6 kwietnia 1990 o Policji* (t.j.: Dz.U. z 2017 r. poz. 2067, ze zm.).

*Bundesrat Gesetzentwurf der Bundesregierung*, Drucksache 355/15.

*Counter-Terrorism and Security Act 2015*.

*Gesetz zur Finanzierung der Terrorbekämpfung* (*Ustawa o finansowaniu walki z terroryzmem*) z 10 XII 2001 r. (BGBl. 2001 I s. 3436).

*Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz)* (*Ustawa o zwalczaniu międzynarodowego terroryzmu*) z 9 I 2002 r. BGBl. 2002.

*LOI n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026809719&categorieLien=id.

*Terrorism Act 2006*, CH11, 30.03.2006.

*Terrorism Act 2000*, CH11, 21.7.2000.

*Ústava Slovenskej republiky*, Ústavný zákon č. 460/1992 (*Konstytucja Republiki Słowackiej*).

*United States Code*, Title 22, Chapter 38, Section 2656f(d).

*Vereinsgesetz* (*Ustawa o stowarzyszeniach prywatnych*) z 5 VIII 1964 r. (BGBl. 1964 I s. 593), pierwsza poprawka z 4 grudnia 2001 r. (BGBl. 2001 I str. 3319)

*Zákon Národnej rady Slovenskej republiky o Policajnom zbore*, Zákon č. 171/1993 Z. z. (*Ustawa o Policji*).

*Uchwała nr 252 Rady Ministrów z 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019”,* załącznik (M.P. z 2014 r. poz. 1218).

*Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów*, rozdział 5 (t.j.: M.P. z 2016 r. poz. 1006).

*Dekret nr 2002-890 Rady Bezpieczeństwa Wewnętrznego Francji z 15 maja 2002 r.*

Decyzja nr 6 przewodniczącego Międzyresortowego Zespołu do spraw Zagrożeń Terrorystycznych z 12 stycznia 2009 r. w sprawie powołania Zespołu Zadaniowego do Opracowania Szczegółowych Założeń do Projektu Ustawy o Rozpoznawaniu, Przeciwdziałaniu i Zwalczaniu Terroryzmu.

*Opinia do projektu ustawy o działaniach antyterrorystycznych*, 19 V 2016 r., Rzecznik Praw Obywatelskich (druk sejmowy nr 516), https://www.rpo.gov.pl/sites/default/files/ustawa%20antyrrorystyczna%20opinia%2019.05.2016.pdf [dostęp: 18 XI 2016].

Pismo Rzecznika Praw Obywatelskich do Minister Cyfryzacji Anny Streżyńskiej w sprawie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 154), https://docplayer.pl/27464473-Pani-anna-strezynska-minister-cyfryzacji-ul-krolewska-warszawa.html [dostęp: 18 XI 2016].

Raport z 18 listopada 2005 r. (Doc. 14306.3.04) przygotowany na podstawie *Decyzji Rady nr 2002/996/WSiSW z dnia 28 listopada 2002 roku w sprawie ustanowienia mechanizmów oceny systemów prawnych i ich stosowania na poziomie krajowym w walce z terroryzmem* (Dz.U. WE L 349 z 24 XII 2002, s. 1).

*Rządowy projektu ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw*, uzasadnienie Ministra Spraw Wewnętrznych i Administracji (druk 516).

*The European Union Counter Terrorism Strategy 14469/4/05*, 2005 r.

*Sprawozdanie z prac Zespołu Zadaniowego do spraw Usystematyzowania Krajowych Regulacji i Rozwiązań Prawnych Dotyczących Przeciwdziałania Terroryzmowi*, Warszawa 2008 r. BBN (?)

*Stanowisko Fundacji Panoptykon w sprawie projektu ustawy o działaniach antyterrorystycznych*, Warszawa 2016, Fundacja Panoptykon, https://panoptykon.org/biblio/stanowisko-fundacji-panoptykon-w-sprawie-projektu-ustawy-o-działaniach-antyterrorystycznych [dostęp: 18 XI 2016].

Wniosek Rzecznika Praw Obywatelskich z 11 lipca 2016 r. do Trybunału Konstytucyjnego o stwierdzenie niezgodności z Konstytucją niektórych zapisów ustawy o działaniach antyterrorystycznych, 10 VI 2016 r., pismo VII.520.6.2016VV/AG, https://www.rpo.gov.pl/sites/default/files/Wniosek%20do%20TK%20w%20sprawie%20ustawy%20antyterrorystycznej%2011%20lipca%202016.pdf [dostęp: 18 XI 2016].

*Uwagi Helsińskiej Fundacji Praw Człowieka do projektu ustawy o działaniach antyterrorystycznych* (druk sejmowy nr 516), 987/2016/MPL

**Orzecznictwo:**

Wyrok TK z 3 VI 2018 r. (K 38/07, OTK-A 2008, nr 6, poz. 102).

Uchwała Sądu Najwyższego z 23 lutego 2006 r., SNO 3/06, OSN-Sądu Dyscyplinarnego 2006, nr 1, poz. 25.

Wyrok Sądu Najwyższego z 2 VI 2010 r., V KK 376/09.

Wyrok ETPCz z 28 X 1994 r. w sprawie Murray p. Zjednoczone Królestwo.

Uchwała Sądu Najwyższego - Sądu Dyscyplinarnego z dnia 18 października 2004 r., SNO 40/04, OSNSD 2004, nr 2, poz. 33.

Uzasadnienie do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014, sygn. akt K 23/11.

Wyrok ETPC z 4 grudnia 2015 r. w sprawie Zakharov v. Rosja, skarga nr 47413/06.

Wyrok Trybunału Konstytucyjnego z 15 listopada 2000 r. sygn. akt P 12/99, OTK ZU 2000, nr 7, poz. 260.

**Źródła internetowe:**

Federal Bureau of Investigation, https://www.fbi.gov/investigate/terrorism.

Antyterroryzm.gov.pl.

http://www.coe.int.

**Słowa kluczowe:** terroryzm, ustawa antyterrorystyczna, ustawa o działaniach antyterrorystycznych, instytucje karnoprocesowe, przeszukanie, przedstawienie zarzutów.

**Keywords**: terrorism, antiterrorist act, the act on anti-terrorist activities, institutions of penal proceedings, search, informing the subject of the charges levelled against him.