PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 24 (13) 2021

Rada naukowa

prof. dr hab. Brunon Hołyst
dr hab. Krzysztof Indecki
prof. dr hab. Andrzej Mania
prof. dr hab. Stanisław Sulowski
prof. dr hab. Sebastian Wojciechowski
prof. dr hab. Konstanty A. Wojtaszczyk

Recenzenci PBW 24

dr hab. Robert Borkowski
dr Piotr Chorbot
dr Robert Lach
dr Rafał Leśkiewicz
dr hab. Ryszard Machnikowski
prof. dr hab. Piotr Majer
dr Krzysztof Malesa
prof. dr hab. Andrzej Misiuk
dr Witold Ostant
por. r. pr. Łukasz Sokołowski
dr hab. Grzegorz Tylec
płk prof. dr hab. inż. Przemysław Wachulak
prof. dr hab. Waldemar Zubrzycki

INTERNAL SECURITY REVIEW

WARSAW 24 (13) 2021

Zespół redakcyjny Anna Przyborowska (redaktor naczelna)
Elżbieta Dąbrowska (sekretarz Redakcji)
Aneta Olkowska, Grażyna Osuchowska, Izabela Paczesna
Anna Przyborowska (redakcja, korekta)
Agnieszka Dębska (skład)

© Copyright by Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota"
Emów 2021

ISSN 2080-1335

Wszystkie artykuły zamieszczone w czasopiśmie są recenzowane
All the articles published in the magazine are subject to reviews

Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Wersja online czasopisma jest dostępna na stronie www.abw.gov.pl

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) jest zamieszczony w Index Copernicus Journal Master List z liczbą 59,68 punktu. Czasopismo jest również dostępne w bazach: Central European Journal of Social Science and Humanities i Polska Bibliografia Naukowa (PBN)

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

Redakcja
tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 693
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Numer zamknięto i oddano do druku w kwietniu 2021 r.

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

SPIS TREŚCI

I. ARTYKUŁY I ROZPRAWY

Krzysztof Izak
Zmiana w postrzeganiu imigracji, integracji, wielokulturowości i zagrożenia islamskim radykalizmem przez władze niektórych państw UE 11

Małgorzata Kudzin-Borkowska
Cyberbezpieczeństwo w Grupie Wyszehradzkiej – koncepcje i strategie 46

Rafał Wądołowski
Ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane regulacje karne i administracyjne 63

Paweł Pokrzywiński
Izraelskie ustawodawstwo antyterrorystyczne wobec zagrożeń XXI wieku 91

Paweł Gacek
Zakaz członkostwa w partii politycznej funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu oraz uczestnictwa w działalności tej partii lub na jej rzecz 110

Daniel Mider, Ewa Aleksandra Ziemak
Technologie wspierające prywatność – ideologia, prawo, wdrożenia 132

Maciej Aleksander Kędzierski
Możliwość zastosowania inżynierii odwrotnej do zwalczania organizacji przestępczych typu sieciowego 173

II. STUDIA I ANALIZY

Anna Łasińska
Analiza SEM czarnego tonera na wydrukach. Część II 221

Rafał Jurczak
Analiza mikrośladów trinadtlenku triacetonu (TATP) w fazie gazowej z zastosowaniem TD-GC/MS 250

Tomasz Szczepański, Urszula Więckiewicz, Barbara Konior, Patryk Pucułek
Wpływ dezynfekcji pomieszczeń ozonem na skuteczność ujawniania śladów daktyloskopijnych na powierzchni papieru metodą DFO w dobie pandemii SARS-CoV-2 277

III. RECENZJE

Krzysztof Izak
Gérard Chaliand, Arnaud Blin, Historia terroryzmu. Od starożytności do Da'isz 297

Robert Borkowski
Peter Warren Singer, Emerson T. Brooking, Nowy rodzaj wojny: media społecznościowe jako broń 311

Małgorzata Kudzin-Borkowska
Marek Górka, Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017 317

Mariusz Krzysztofiński
Tytus Jaskułowski, Filip Gańczak, Konrad Knoch, Piotr Abryszeński, Ewa Pejaś, Raporty polskie Stasi 1981–1989. Tom 1: W przededniu stanu wojennego czerwiec–grudzień 1981 321

IV. PRZEGLĄD PRAC KONKURSOWYCH

Norbert Nowicki
Normatywne ujęcie czynności operacyjno-rozpoznawczych w aspekcie dowodu nielegalnego 333

Andrzej Karaś
Modelowanie operacji informacyjnych z wykorzystaniem teorii sterowania refleksyjnego 351

V. WYBRANE ARTYKUŁY W JĘZYKU ANGIELSKIM

Krzysztof Izak
Changes in the perception of immigration, integration, multiculturalism and threats of Islamic radicalism in certain EU member states 375

Remigiusz Rosicki
State security as exemplified by the fight against terrorism: a choice between the well-being of the individual and the well-being of the community 404

O autorach 421

Informacje dla autorów czasopisma „Przegląd Bezpieczeństwa Wewnętrznego" i serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego 425

TABLE OF CONTENTS

I. ARTICLES AND DISSERTATIONS

Krzysztof Izak
Changes in the perception of immigration, integration, multiculturalism and threats of Islamic radicalism in certain EU member states 11

Małgorzata Kudzin-Borkowska
Cybersecurity in the Visegrad Group – concepts and strategies 46

Rafał Wądołowski
The protection of State Secrets in the Russian Federation. Selected penal and administrative regulations 63

Paweł Pokrzywiński
Israeli counter-terrorist legislation against the threats of the 21st century 91

Paweł Gacek
The prohibition of political party membership and of participation in political party activities or on its behalf imposed on officers of the Internal Security Agency and Foreign Intelligence Agency 110

Daniel Mider, Ewa Aleksandra Ziemak
Privacy Enhancing Technologies – ideology, law and implementations 132

Maciej Aleksander Kędzierski
The possibility of using reverse engineering to combat network – type criminal organisation 173

II. STUDIES AND ANALYSES

Anna Łasińska
SEM analysis of black toner on printouts. Part II 221

Rafał Jurczak
Micro-traces analysis of triacetone triperoxide (TATP) in the form of vapours using TD-GC/MS 250

Tomasz Szczepański, Urszula Więckiewicz, Barbara Konior, Patryk Pucułek
The effect of ozone disinfection of rooms on the efficacy of revealing dactyloscopic traces on the surface of the paper using the DFO method during the SARS-CoV-2 pandemic 277

III. REVIEWS

Krzysztof Izak
Gérard Chaliand, Arnaud Blin, Historia terroryzmu. Od starożytności do Da'isz 297

Robert Borkowski
Peter Warren Singer, Emerson T. Brooking, Nowy rodzaj wojny: media społecznościowe jako broń 311

Małgorzata Kudzin-Borkowska
Marek Górka, Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017 317

Mariusz Krzysztofiński
Tytus Jaskułowski, Filip Gańczak, Konrad Knoch, Piotr Abryszeński, Ewa Pejaś, Raporty polskie Stasi 1981–1989. Tom 1: W przededniu stanu wojennego czerwiec–grudzień 1981 321

IV. OVERVIEW OF THE WORKS

Norbert Nowicki
Normative approach to operational and reconnaissance activities in terms of illegal evidence 333

Andrzej Karaś
Information operation modeling using reflexive control theory 351

V. SELECTED ARTICLES IN ENGLISH

Krzysztof Izak
Changes in the perception of immigration, integration, multiculturalism and threats of Islamic radicalism in certain EU member states 375

Remigiusz Rosicki
State security as exemplified by the fight against terrorism: a choice between the well-being of the individual and the well-being of the community 404

About the authors 423

Information for the authors of „The Internal Security Review" journal and the Library of Internal Security Review series 425

I

ARTYKUŁY I ROZPRAWY

ARTICLES AND DISSERTATIONS

KRZYSZTOF IZAK
ORCID: 0000-0001-9815-6035

DOI: 10.4467/20801335PBW.21.010.13567

Zmiana w postrzeganiu imigracji, integracji, wielokulturowości i zagrożenia islamskim radykalizmem przez władze niektórych państw UE

Pojęcia integracja, asymilacja i wielokulturowość (multikulturalizm) stały się bardzo popularne w obecnym stuleciu[1]. Jest to skutek napływu imigrantów do Europy. Wykres tego napływu przypomina sinusoidę – krzywą obrazującą wzrost lub zmniejszenie ruchów migracyjnych na nasz kontynent. To zjawisko przybrało największe rozmiary w 2015 r., potęgując już wcześniej nabrzmiałe problemy i zagrożenia z nim związane. Ich przybliżenie jest celem niniejszego artykułu. Autor odpowie również na pytanie, czy działania podejmowane przez władze państw UE w celu rozwiązania zaistniałych problemów i im przeciwdziałania mogłyby odnieść pożądany skutek i przyczynić się do uspokojenia nastrojów społecznych, a jeśli tak, to w jakim zakresie. Czy wprost przeciwnie, te działania mogą prowadzić do jeszcze większego zantagonizowania różnych grup społecznych, a co za tym idzie – do ich radykalizacji.

Założenia badawcze artykułu koncentrują się wokół problemów istotnych dla teraźniejszości i przyszłości Europy, związanych z migracją na nasz kontynent obywateli państw muzułmańskich, którzy nie zawsze potrafią lub chcą się zintegrować z mieszkańcami krajów przyjmujących. Autor zwraca również uwagę na zmieniający się stosunek władz wybranych państw UE do realizowanych przez lata projektów integracji i wielokulturowości. Pojawiły się liczne głosy krytyki koncepcji polityki integracyjnej, związane z przekonaniem o jej nieskuteczności w procesie przystosowania cudzoziemców do europejskiego społeczeństwa. Niektóre państwa zaczęły oficjalnie wycofywać się z projektów działań na rzecz imigrantów, a także odrzucać publiczną dyskusję

[1] Te pojęcia zostały zdefiniowane i zanalizowane w wielu publikacjach. Autor odsyła do książki Janusza Balickiego pt. *Imigranci z krajów muzułmańskich w Unii Europejskiej. Wyzwania dla polityki integracyjnej*, Warszawa 2010.

związaną z wielokulturowością, co świadczy o porażce polityki integracyjnej imigrantów wyznających islam. Tym działaniom towarzyszyła religijna radykalizacja mniejszości muzułmańskich prowadząca do aktów brutalnej przemocy. Po wieloletnim odwracaniu społecznej uwagi od istoty zagrożenia spowodowała ona ostrą reakcję kilku rządów w UE, poza samą Brukselą. Analizując powyższe problemy, autor przy rozpatrywaniu tego zjawiska posłużył się następującymi metodami: historyczną – pozwalającą zrozumieć zmiany zachodzące w środowiskach imigranckich, behawioralną – przez którą rozumie się zachowania jednostek i grup społecznych oraz porównawczą – ukazującą zmiany w reakcji władz państwowych na zagrożenia ze strony zradykalizowanej części mniejszości muzułmańskich.

Przejawy i skutki polityki multikulturalizmu

Nad Sekwaną doskonale widać negatywne skutki przemian społecznych wywołanych zarówno polityką kolejnych rządów wobec imigracji, jak i systemem opiekuńczym państwa. Ich źródłem są m.in. idee propagowane przez francuską lewicę, która od lat przedstawia imigrantów pochodzących z dawnych kolonii wyłącznie jako ofiary krzywd wyrządzonych przez Francję, co z kolei rozbudza w nich postawy rewindykacyjne i roszczeniowe oraz przyczynia się do kształtowania niechęci wobec kraju przyjmującego. Francja jest krajem o największej liczbie populacji muzułmanów w Unii Europejskiej. Jest też krajem najbardziej w UE zagrożonym terroryzmem. Według oficjalnych danych we Francji mieszka 6 mln muzułmanów (przy 70 mln populacji), a według niektórych opinii może ich tam przebywać od 8 do 10 mln[2].

Historia terroryzmu we Francji jest bardzo długa[3]. Po II wojnie światowej była ona związana z wojną o niepodległość Algierii. Po jej zakończeniu Algierię musiało opuścić ponad milion ludzi. Według francuskiego historyka Alaina Besançona pierwszy prezydent V Republiki gen. Charles de Gaulle (1959–1969) wolał zrezygnować z Algierii niż przyjąć do francuskiego społeczeństwa zbyt wielu wyznawców islamu. De Gaulle był przeciwny utrzymaniu francuskiej Algierii, ponieważ obawiał się naruszenia równowagi demograficznej Francji, spowodowanej nadmierną liczbą muzułmanów. Nie uległ zwolennikom francuskiej Algierii, z których wielu było gaullistami, jak premier Michel Debré. Dopiero pod rządami Georges'a Pompidou (1969–1974) i Valery'ego Giscarda d'Estaing (1974–1981) imigracja muzułmańska nabrała tempa. Trzeba jednak

[2] M. Widy, *Życie codzienne w muzułmańskim Paryżu*, Warszawa 2005, s. 22. Wiele współczesnych publikacji wciąż podaje liczbę 6 mln wyznawców islamu we Francji. W ten sposób od 15 lat, kiedy to po raz pierwszy podano tę liczbę, populacja francuskich wyznawców islamu utrzymuje się na stałym poziomie, co jest mało wiarygodne. Szacunkowe dane, charakteryzujące się znacznymi rozbieżnościami, wynikają z tego, że we Francji podczas przeprowadzania spisów ludności obowiązuje zakaz zadawania pytań osobie ankietowanej o wyznawaną religię.

[3] Za początek terroryzmu w społeczeństwie industrialnym uznaje się datę 13 VII 1793 r., kiedy to żyrondystka Charlotte Corday zasztyletowała jakobińskiego trybuna Jeana-Paula Marata.

zaznaczyć, że wszystkie siły polityczne Francji przyczyniły się do sprowadzenia muzułmanów. Wspólnoty religijne – katolicy, protestanci, żydzi – chciały pokazać, że są na innych otwarte, przedsiębiorcy szukali taniej siły roboczej, lewica robiła to w imię idei humanitarnych, prawica zaś chciała utrzymać związki z dawnymi koloniami[4].

W latach 90. XX w. Francja zaczęła się zmagać z ekstremizmem islamskim. Szerzyli go głównie Francuzi pochodzenia algierskiego, którzy występowali przeciw władzom z powodu poparcia przez rząd francuski reżimu wojskowego w Algierii w toczącej się tam wojnie domowej z islamistami. Do Francji przybyła wówczas z Algierii duża grupa uciekinierów, która – podobnie jak wcześniejsi imigranci – osiedliła się w blokowiskach na przedmieściach wielkich miast. W tych dzielnicach jeszcze w latach 60. i 70. dla miejscowych i zagranicznych robotników wybudowano mieszkania w wielopiętrowych blokach, zwane popularnie mieszkaniami z niskim czynszem (fr. *habitation à loyer modéré*, HLM). Z biegiem lat Francuzi wyprowadzili się z nich do lepszych mieszkań lub własnych domów. Podobnie czynili wykształceni, zintegrowani i wzbogaceni obcokrajowcy[5]. Imamowie i misjonarze, którzy przybywali w tym czasie z państw muzułmańskich do Francji i innych krajów zachodniej Europy, angażowali się w głoszenie nauk o islamie. Z trudem jednak przekonywali imigracyjnych robotników do przestrzegania nakazów islamu, ponieważ nie znali ich życiowych problemów. Ponadto imigranci bardziej zabiegali o zapewnienie bytu rodzinie niż o zaspokojenie duchowych potrzeb. Pierwsze pokolenie imigrantów troszczyło się również o wykształcenie licznych dzieci wzrastających w europejskiej kulturze i w ten sposób wypełniali założenia polityki integracji społecznej.

Francja jest przykładem państwa, z którym kojarzono model asymilacji imigrantów, ale można go również odnaleźć w innych krajach, m.in. w Niemczech. W państwach zachodniej Europy uważano, że do końca XX w. wszyscy przybysze będą zasymilowani z ich nowym środowiskiem. Miało to potrwać dwie, a nawet trzy generacje. Jednak niektórzy zaczęli kwestionować tego typu założenia. Według nich nawet w kolejnym pokoleniu różnica kulturowa pomiędzy imigrantami i ich dziećmi a otoczeniem nie zniknie całkowicie. Można też było zaobserwować, że są oni świadomi, że pełna integracja ze społeczeństwem i partycypacja w instytucjach państwowych nie wymaga od imigrantów rezygnacji z własnej tożsamości. We francuskiej tradycji jakobińskiej główny nacisk jest położony na indywidualne stosunki pomiędzy obywatelem a państwem, bez udziału pośredników. Ten model zakłada, że imigranci osiągną wysoki poziom adaptacji kulturowej nowego środowiska. Ci, którym się to uda, zyskają

---

[4] J. Bielecki, *Nie przyjaźnię się z żadnym muzułmaninem*, https://www.rp.pl/artykul/1171826-Nie-przyjaznie-sie-z-zadnym-muzulmaninem.html [dostęp: 16 I 2015].

[5] J. Kubera, *Francuzi, Algierczycy? Relacje między identyfikacjami Francuzów algierskiego pochodzenia*, Toruń 2017, s. 381–383. Podobne osiedla wybudowano w Niemczech Zachodnich dla tureckich robotników, tzw. gastarbeiterów. Niemieckie władze zakładały, że po zakończeniu pracy powrócą oni do kraju, a tymczasem z różnych powodów pozostali i sprowadzili rodziny.

wiele możliwości, pozostali ryzykują marginalizację. Okazało się, że większość została zmarginalizowana[6].

Sytuacja zmieniła się po 1989 r., uznawanym do początku XXI w. za apogeum ekspansji ruchu fundamentalistycznego. W wiek dorosły wkroczyło wówczas pokolenie dzieci imigrantów. Było ono już zaznajomione z kulturą europejską i narażone na liczne przeszkody społeczne, w tym na rynku pracy, co często było spowodowane niepowodzeniami szkolnymi. Właśnie w tym środowisku po raz pierwszy na terenie zachodniej Europy powstała grupa ubogiej muzułmańskiej młodzieży miejskiej, która okazała się bardziej podatna na nawoływania działaczy fundamentalistycznych niż ich rodzice. Ideologia fundamentalistyczna przeniknęła do nowego pokolenia dość łatwo, ponieważ zawiodła polityka integracji. We Francji powstały ruchy: S.O.S. Rasizm, który miał połączyć młodzież ze wszystkich środowisk w wielkim antyrasistowskim porywie, oraz „*rebeu*"[7]. Ten ostatni starał się zmienić mentalność młodych Francuzów pochodzenia arabskiego, która odpowiadałaby ich podwójnej przynależności kulturowej. Okazało się jednak, że młodzi ludzie byli podatni bardziej na wpływy muzułmańskich kaznodziejów i misjonarzy niż na kulturę zachodnią. Organizacje wywodzące się z ruchu Al-Ichwan al-Muslimin (Braci Muzułmanów), Dżama'at-e Islami Pakistan (Muzułmańskiej Partii Pakistanu) oraz tureckiej Refah Partisi (Partii Dobrobytu), dobrze zakorzenione w Europie, przystosowały swoje przesłanie na potrzeby tej części młodzieży, która szybko ulegała reislamizacji. Przy tej okazji rozkwitło nawracanie na islam w m.in. języku francuskim, angielskim, niemieckim, a także polskim. Tłumaczono na te języki dzieła muzułmańskich teoretyków politycznego islamu i dżihadu: Sajjida Kutba i Abu al-Ala al-Maududiego[8]. Jednocześnie agitacja wychodziła poza przestrzeń gmin muzułmańskich. Mieszkańcy Paryża znajdowali w skrzynkach pocztowych ulotki z napisem: *My, muzułmanie, przejmiemy Francję, tak jak wy kiedyś skolonizowaliście Algierię. Francuskie rodziny mają po jednym dziecku, my w tym czasie rodzimy ich pięcioro. Za dwadzieścia lat to my będziemy kontrolować Francję*[9].

Proces nawracania i radykalizacji młodzieży uległ przyspieszeniu po 11 września 2001 r., stanowiącym swoistą cezurę dla współczesnego terroryzmu. Europejscy dżihadyści zaczęli wyjeżdżać w rejony konfliktów w Iraku i Afganistanie. Spektakularny powrót dżihadystycznego terroryzmu do Francji nastąpił w marcu 2012 r.[10] Zbiegł się on z początkiem wielkiej kampanii, która doprowadziła do wybrania Françoisa Hollande'a na urząd prezydenta. Do jego zwycięstwa przyczynili się częściowo muzułmanie

---

6 J. Balicki, *Imigranci z krajów muzułmańskich*…, s. 27.

7 W języku francuskim potoczny termin na określenie osób urodzonych w Europie, których rodzice lub dziadkowie byli imigrantami z krajów Maghrebu.

8 G. Keppel, *Święta wojna. Ekspansja i upadek fundamentalizmu muzułmańskiego*, Warszawa 2003, s. 204–205.

9 A. Pamuła, *Wrzenie. Francja na krawędzi*, Warszawa 2020, s. 369.

10 W dniach 11, 15 i 19 marca 2012 r. Mohammad Merah zastrzelił w Tuluzie siedem osób, a dwie ciężko ranił.

masowo głosujący na jego korzyść. Po tej kampanii nastąpiły wybory parlamentarne, w których po raz pierwszy pojawiło się ponad 400 kandydatów wywodzących się ze środowiska imigranckiego, w zdecydowanej większości muzułmanów. Wyznawcy islamu głosowali tym razem na swoich kandydatów. Odczuł to wyraźnie deputowany Jacques Myard, rodowity Francuz, który starał się o reelekcję w podparyskim departamencie Yvelines. W mieście Satrouville, gdzie mieszka duża liczba ludzi pochodzących z krajów Maghrebu, Myard odwiedził miejscowy bazar. Tu zaczepił go Arab, który pouczył deputowanego: *Nie ma pan tu nic do roboty. To jest ziemia arabska. Teren należący do muzułmanów, to nie jest ziemia francuska. Pan jest rasistą, syjonistą i powinien pan stąd sobie iść*[11]. W sposób wyraźny ujawniły się więc rezultaty politycznej edukacji, a nie integracji społecznej. We Francji powstało równoległe społeczeństwo. Mniejszość muzułmańska domagała się nieskrępowanego dostępu do obywatelstwa, takich samych praw, jakie mieli chrześcijanie i żydzi, ale z zachowaniem religijnej odrębności i wynikających z niej przywilejów, oczywiście z pominięciem uznawania zasad laickiego państwa[12]. Te przywileje były przyznawane w okresie prezydentury Hollande'a (2012–2017), co zasadniczo różniło ją od prezydentury Nicolasa Sarkozy'ego (2007–2012), który próbował przywrócić względną „normalność" w stosunkach z mniejszością muzułmańską i zapanować nad jej roszczeniami. Przede wszystkim proponował skończyć z tradycyjną definicją laickości państwa, oznaczającą po prostu wykluczanie chrześcijaństwa z przestrzeni publicznej. Zdaniem Sarkozy'ego Francja nie powinna być dłużej odcinana od chrześcijańskich korzeni. Na laickości państwa korzystali wyznawcy islamu, gdyż pomagało im to w szerzeniu jego idei. Co prawda w 2004 r. zakazano w szkołach noszenia symboli religijnych, w tym muzułmańskich chust, ale wprowadzano inne elementy muzułmańskiej obyczajowości, m.in. żywność halal w placówkach oświatowych, separacja płci na lekcjach wychowania fizycznego, burkini na pływalniach i plażach czy przymykanie oczu na bigamię i obrzezanie dziewczynek. Te praktyki upowszechniły się w okresie prezydentury Hollande'a. Ówczesny socjalistyczny minister spraw wewnętrznych Manuel Valls mówił w parlamencie wyłącznie o islamofobii i antysemityzmie. W tym samym czasie bagatelizowano lub przemilczano akty profanacji obiektów chrześcijańskich. Jeśli zdarzyła się profanacja meczetu, krzyczano o rasizmie i islamofobii, jeśli obiektem wandalizmu były synagogi lub cmentarze żydowskie – o antysemityzmie. Dewastowano i profanowano kościoły i chrześcijańskie cmentarze, co przechodziło bez większego rozgłosu. Z roku na rok wzrasta liczba aktów antysemityzmu. W 2014 r. zanotowano ich we Francji ponad 850, czyli dwa razy więcej niż w poprzednim roku. Antysemityzm w wykonaniu wyznawców islamu różni się od działań skrajnej prawicy. Prawicowcy koncentrują się głównie na antyżydowskiej propagandzie, muzułmanie stosują rozboje, przemoc z torturami, a nawet zabójstwa. Nic dziwnego, że między 2000 a 2017 r. do Izraela wyjechało ok. 50 tys. francuskich żydów, najwięcej (prawie 20 tys.) po zamachach w supermarkecie

[11] B. Dobosz, *Emiraty francuskie*, Warszawa 2016, s. 176.

[12] G. Keppel, A. Jardin, *Terror we Francji. Geneza francuskiego dżihadu*, Warszawa 2017, s. 43.

Hyper Cacher w styczniu, 2015 r.[13] W tym samym, 2015 roku (13 1istopada) doszło w Paryżu do zamachów na redakcję tygodnika „Charlie Hebdo" i serii najbardziej krwawych ataków. Tak więc cała laickość państwa, zamiast stanowić obronę przed przemocą ze strony wyznawców islamu, obróciła się przeciwko Francji i jej mieszkańcom. Dostrzegali to francuscy intelektualiści, jednak ich wypowiedzi i publikacje spotykały się z wrogością muzułmańskich aktywistów i lewicowych polityków oraz ekspertów[14].

W Niemczech mieszka druga pod względem liczebności w UE społeczność muzułmańska. Nieoficjalne statystyki, uwzględniające nielegalnych i niezarejestrowanych muzułmanów, mówią nawet o ponad 7 mln. Imigranci w tym kraju nie mogą pamiętać jego kolonialnej przeszłości[15]. Niemcy zaś otworzyły się na imigrantów, chcąc w ten sposób zadośćuczynić obcym za zbrodnie i krzywdy hitleryzmu. Politycy zadbali, żeby w konstytucji ich kraju znalazły się zapisy zapewniające szeroko pojętą tolerancję. Niemcy prowadziły również najbardziej liberalną politykę azylową na świecie. Grupom uznawanym za terrorystyczne pozwalano na prowadzenie działalności, zbiórki funduszy oraz rekrutację nowych członków, pod warunkiem jednak, że byli to terroryści zagraniczni, a nie rdzenni, niemieccy. Nawet planowanie operacji terrorystycznych nie było samo w sobie niezgodne z prawem, o ile atak miał nastąpić za granicą. Policja miała skupiać swoje wysiłki na tropieniu lokalnych prawicowych ekstremistów, nie zwracała zaś specjalnej uwagi na grupki obcokrajowców. Między Niemcami a radykałami zamieszkującymi ich kraj obowiązywał cichy układ, zgodnie z którym obcokrajowcy mogli robić, co chcieli, jeśli nie atakowali obywateli swojej przybranej ojczyzny. Próbując się odciąć od własnej przeszłości, Niemcy szeroko otworzyły drzwi dla obcych.

Większość muzułmanów u naszych zachodnich sąsiadów to obywatele Turcji oraz Niemcy tureckiego pochodzenia w drugim i trzecim pokoleniu – dzieci i wnukowie tureckich robotników przybyłych do Niemiec w latach 60. i 70. XX w. Wśród tej społeczności dużą sympatią od początku cieszy się ruch Hizmet (Służba) założony

---

[13] A. Pamuła, *Wrzenie. Francja na…*, s. 351.

[14] Należy wymienić Georges'a Bensoussana i jego książkę z 2002 r.: *Les Territoires perdus de la République – antisémitisme, racisme et sexisme en milieu scolaire* (*Stracone terytoria republiki – antysemityzm, rasizm i seksizm w szkole*). Autor pisze w niej o antysemityzmie francuskiej młodzieży szkolnej pochodzenia arabskiego. W kolejnej publikacji tego autora: *Une France soumis* (*Francja uległa*), opublikowanej w 2017 r., przedstawia on smutny obraz państwa pozwalającego na wszystko swojej imigranckiej społeczności. Renaud Camus w pracy: *Le Grand Remplacement* (*Wielka Wymiana*), wydanej w 2011 r., zapowiedział zastąpienie białych Europejczyków przez zwiększającą się liczbę przybyszów z Bliskiego Wschodu i Afryki. Bernard Rougier w opracowaniu: *Les territoires conquis de l'islamisme* (*Podbite terytoria islamizmu*), opublikowanym w 2020 r., zwraca uwagę na dzielnice imigranckie kontrolowane przez muzułmańskich radykałów. W tym samym roku Patrick Stefanini opublikował książkę pt.: *Immigration – Ces réalités qu'on nous cache* (*Imigracja – realia, które ukrywamy*). Należy również wspomnieć o pracach Michela Houellebecqa i Gillesa Kepela tłumaczonych na język polski oraz o publikacjach polskich autorów wymienionych w przypisach: Bogdana Dobosza, Marka Orzechowskiego i Anny Pamuły.

[15] Po I wojnie światowej Niemcy utraciły następujące kolonie w Afryce: Togo, Kamerun, Niemiecką Afrykę Południowo-Zachodnią (obecnie Namibia) i Niemiecką Afrykę Wschodnią – Tanganikę, czyli obecnie kontynentalną część Tanzanii.

przez znanego kaznodzieję Fethullaha Gülena. Międzynarodową misję szerzenia islamu w ideologii typowej dla Braci Muzułmanów realizował on pod hasłami: *Budujmy szkoły, nie meczety* oraz *Nasz dżihad to edukacja*. Gülen działał w sposób stwarzający pozory wspierania dialogu międzyreligijnego i międzykulturowego, usypiając czujność władz. W Niemczech ruch działał po cichu, lecz skutecznie. Tworzył specjalne szkoły, prywatne gimnazja i uczelnie wyższe, lokalne centra studiów nad *Koranem* oraz tzw. latarnie (niem. *Lichthäuser*), czyli męskie kolektywy, w których obowiązywały ścisła dyscyplina, całkowite posłuszeństwo, przymusowe czytanie *Koranu* i wspólne modlitwy pięć razy dziennie. Gülen dbał o kreowanie publicznego wizerunku ekumenicznego ruchu islamskiego zabiegającego o dialog międzynarodowy – założył w Niemczech 15 stowarzyszeń dialogu[16]. Na marginesie należy dodać, że ruch Gülena powołał w Polsce prywatne placówki edukacyjne: międzynarodową szkołę Meridian (w Warszawie – szkołę podstawową, gimnazjum i liceum, a w Łodzi – przedszkole i szkołę podstawową) oraz Wyższą Szkołę Ekonomiczno-Informatyczną. Właścicielem tych instytucji oświatowych jest firma „Meridian" sp. z o.o., która ma swoje oddziały w wielu państwach[17]. Zwolennicy Gülena nie przygotowywali się do zbrojnego dżihadu, lecz do dżihadu języka, czyli aktywności misyjnej. Ich działalność jest subtelna i wyrafinowana, żeby uniknąć oskarżenia o szerzenie nienawiści religijnej i przemocy. Ma to być rozciągnięta w czasie misja krzewienia islamu, zgodnie z treścią kazania wygłoszonego kiedyś przez Gülena do uczniów. To harmonijne – wydawałoby się – współistnienie Niemców i muzułmanów oraz ich integracja, mające charakter bardziej życzeniowy niż zgodny z realiami, zostało zaakcentowane przez prezydenta Christiana Wulfa, który podczas doniosłych uroczystości związanych z 20. rocznicą zjednoczenia kraju wypowiedział pamiętne słowa: *Bez wątpienia chrześcijaństwo należy do Niemiec. Bez wątpienia judaizm należy do Niemiec. To jest nasza wspólna chrześcijańsko-żydowska historia. Ale islam też już należy do Niemiec*. Najpierw wywołały one zdumienie, jednak dzięki propagandowym zabiegom mediów i wypowiedziom polityków zostały społecznie zaakceptowane i przez pięć kolejnych lat były analizowane[18].

Pierwszą prominentną osobą w Niemczech, która nie zawahała się skrytykować istniejącego stanu, był Thilo Sarrazin. W 2010 r. ukazała się jego książka pt. *Deutschland schafft sich ab: Wie wir unser Land aufs Spiel setzen* (*Samolikwidacja Niemiec: Jak wystawiamy nasz kraj na ryzyko*), w której stwierdził, że imigranci z krajów muzułmańskich przysparzają państwu więcej kosztów socjalnych, niż dostarczają korzyści dla gospodarki. Odmówił on uznania za równoprawnych obywateli tych imigrantów, którzy żyją ze świadczeń państwa, a jednocześnie odrzucają to państwo

---

[16] *Media w USA ostro o przejęciu „Zaman": „Zamach Erdogana na prasę"*, 8 III 2016 r., https://wiadomosci.wp.pl/media-w-usa-ostro-o-przejeciu-zaman-zamach-erdogana-na-prase-6027417304052353a [dostęp: 19 VII 2016].

[17] A. Rusinek, *Nurt radykalny wśród społeczności muzułmańskich w wybranych państwach Unii Europejskiej*, Warszawa 2012, s. 213.

[18] M. Orzechowski, *Mój sąsiad islamista. Tunis–Paryż–Bruksela…*, wyd. 2 zaktualizowane, Warszawa 2016, s. 211–212.

i nie troszczą się o wykształcenie dzieci. Winą za to obarczył islam, który, jego zdaniem, stoi w opozycji do liberalnych wartości Europy. Publikacja stała się bestsellerem (do końca 2010 r. sprzedano 1,5 mln egzemplarzy) i wywołała ogólnonarodową debatę o imigrantach. Autor poniósł dotkliwe konsekwencje. Został wykluczony ze swojej partii SPD i zmuszony do ustąpienia z funkcji członka Bundesbanku. Jednocześnie prorządowe media i stowarzyszenia muzułmańskie przystąpiły do ataku na Sarrazina, który został nazwany, jak wielu mu podobnych, islamofobem i rasistą. Jednak zdobył on społeczne poparcie[19].

W 2013 r. Recep Tayyip Erdoğan, jeszcze jako premier Turcji, podczas wizyty w Niemczech przestrzegał ponad trzymilionową mniejszość turecką przed integrowaniem się z Niemcami, gdyż islam zakazuje (zgodnie z doktryną) współżycia z niewiernymi. Z kolei podczas wizyty w 2015 r. w jednej z hal targowych w Karlsruhe, w której zgromadziło się blisko 14 tys. zwolenników tureckiego przywódcy, Erdoğan pytał zebranych: *Czy chcecie, abyśmy, zaczynając od Niemiec, rozpoczęli dzieło budowy nowej Turcji?* W odpowiedzi usłyszał gromkie: *Tak!* Erdoğan podkreślał wtedy, że panturecką tożsamość wspierają język oraz islam. Tłumaczył swoim rodakom: *Nie możecie się uczyć niemieckiego czy angielskiego, jeśli najpierw nie opanujecie dobrze tureckiego*[20]. W czasie wystąpienia kilkanaście razy wzywał też imię Allaha i apelował, żeby wspólnoty tureckie w Niemczech działały na rzecz umacniania ogólnoświatowych wpływów Turcji, która wysłała do Niemiec 900 imamów. Każdy z nich może przez pięć lat legalnie przebywać i pracować w gminach muzułmańskich na terenie Niemiec. Niektórzy niemieccy politycy ostrzegali wówczas, że tureccy imamowie i kaznodzieje w Niemczech realizują politykę tureckich władz i są lojalni wobec własnego kraju, a nie państwa pobytu. Politycy żądali również zaprzestania finansowania działalności islamskich wspólnot religijnych z zagranicy. Jednak Centralna Rada Muzułmanów w Niemczech twardo sprzeciwiła się wezwaniom, aby powstrzymać przysyłanie imamów z Turcji. Nie pozostaje tajemnicą, że ci imamowie stoją na straży tureckości i strzegą islamskiej odrębności. Z minbarów (kazalnic) meczetów potępiają i wyklinają Zachód, a niewiernych porównują do popsutych owoców, które czuć zgnilizną[21]. Jednocześnie, gdy od października 2014 r. obywatele Niemiec uczestniczyli w Dreźnie w cotygodniowych marszach Pegidy (niem. Patriotische Europäer gegen die Islamisierung des Abendlandes – Patriotyczni Europejczycy przeciw Islamizacji Zachodu), byli wyzywani przez lewicowych polityków i prorządowe media od islamofobów, nazistów i ludzi stawiających Niemcy w złym świetle. Oddolny ruch sprzeciwu był za słaby, aby powstrzymać kanclerz Angelę Merkel od otwarcia Niemiec dla setek tysięcy, a docelowo – milionów – imigrantów. Tylko niewielką część przybyszów stanowili uchodźcy. W tej ludzkiej

---

[19] P. Madajczyk, *Między fundamentalizmem a asymilacją. Muzułmanie w Niemczech*, Warszawa 2015, s. 178–181.

[20] AEW, *Jak Turcja kontroluje islam w Niemczech*, 27 IV 2016 r., https://euroislam.pl/jak-turcja-kontroluje-islam-w-niemczech/ [dostęp: 27 IV 2016].

[21] Tamże.

fali podążającej przez Bałkany do UE byli przeważnie młodzi, silni mężczyźni wyposażeni w smartfony. Kwaterowano ich w hotelach, niedawno odnowionych pałacach i zamkach, w opuszczonych zabytkowych klasztorach i prywatnych domkach letniskowych, często nie pytając właścicieli o zgodę. Nowi lokatorzy szybko doprowadzali te obiekty do zniszczenia[22]. Niemiecka polityka proimigracyjna została przeniesiona do Europarlamentu, w którym forsowano zasadę przymusowego rozdziału imigrantów pomiędzy państwa członkowskie. Z najbardziej krótkowzrocznym pomysłem w 2016 r. wystąpiła Ska Keller, wiceprzewodnicząca frakcji Zielonych w Parlamencie Europejskim, która chciała przenosić do Europy Wschodniej całe wioski z Syrii, gdyż tylko w ten sposób, jej zdaniem, imigranci lepiej będą się mogli zintegrować[23].

Niemcy mają jeszcze jeden poważny problem, który pojawił się także w Szwecji. Chodzi o gangi przestępcze pochodzenia arabskiego, które mają strukturę klanową. Przed kilku laty liczbę klanów przestępczych działających w Berlinie szacowano na ok. 20, a liczbę ich członków na 10 tys. Obecnie niemieckie źródła policyjne wymieniają aż 100 arabskich klanów przestępczych funkcjonujących w samej tylko Nadrenii Północnej-Westfalii. W ciągu ostatnich dwóch lat zarejestrowano tam ok. 6450 podejrzanych osób, które popełniły 14 225 przestępstw, co stanowi 25 proc. ogólnej liczby zdarzeń o charakterze przestępczym. W Zagłębiu Ruhry i w Bremie arabskie klany odpowiadają za 30 proc. przestępstw. Rywalizują pomiędzy sobą o terytoria i strefy wpływów, opanowując całe dzielnice wielu niemieckich miast. Wchodzą z członkami klubów rockowych i motocyklowych w konflikty, które często kończą się krwawymi porachunkami. Arabskie grupy przestępcze Abu Czaker i Miri, a także Omeirat, Remmo, Rabih, Al-Kadi, Serhan, Nemr, Tamr i Kurdi są znane z kryminalnej działalności również w Szwecji, Belgii i Holandii, czyli w krajach, do których napłynęła duża liczba muzułmańskich imigrantów. Te klany prowadzą wszystkie rodzaje przestępczości. Ich członków trudno namierzyć, inwigilować i zidentyfikować, ponieważ nie są oni zarejestrowani w urzędach do spraw cudzoziemców, posługują się fałszywymi dokumentami, mogą też liczyć na pomoc ze strony grupy lub współwyznawców. Wieloletnia polityka tolerancji i poprawności politycznej wobec obcych religijnie i kulturowo przybyszów doprowadziła w Niemczech do obecnej sytuacji, w której klanowe struktury przestępcze rozwinęły się w równoległe społeczeństwo, prawie niemożliwe do przeniknięcia i likwidacji[24]. Sytuację pogarszają braki kadrowe w niemieckiej policji ograniczające skuteczne działania przeciwko przestępczości zorganizowanej.

W literaturze przedmiotu Wielka Brytania jest zwykle postrzegana jako pierwowzór modelu wielokulturowości. Zjednoczone Królestwo dbało o zachowanie różnic kulturowych mniejszości, wręcz je dowartościowywało. Udzielało schronienia wszystkim

---

[22] U. Ulfkotte, *Niemcy jako Mekka. Cicha islamizacja Europy*, Wrocław 2019, s. 211–212.

[23] K. Izak, *Dokumenty, tożsamość, służby i politycy*, „Człowiek i Dokumenty" 2017, nr 46, s. 59.

[24] A. Dworak, *Ulica należy do klanu. Arabscy gangsterzy opanowali miasta Niemiec*, „Polska Times", 1 II 2019 r., https://polskatimes.pl/ulica-nalezy-do-klanu-arabscy-gangsterzy-opanowali-miasta-niemiec/ar/c1-13853448 [dostęp: 1 II 2019].

prześladowanym w swoich krajach. Nie mogło być zatem zaskoczenia, że głównym centrum islamskiego radykalizmu stała się stolica kraju, nazywana niekiedy „Londonistanem". Szukali tu schronienia i otwarcie głosili swoje poglądy ekstremiści wydalani z państw muzułmańskich, ale także z Francji. Londyn stał się ważnym ośrodkiem islamskiego ekstremizmu oddziałującego na cały świat. W Wielkiej Brytanii znajdują się redakcje arabskojęzycznych gazet: „Al-Arab" („Arabia"), „Al-Hajat" („Życie"), „Al-Kuds al-Arabi" („Arabska Jezozolima") i „Asz-Szark al-Awsat" („Bliski Wschód"), redakcje czasopism radykalnych organizacji islamskich: „Filistin al-Muslima" („Muzułmańska Palestyna"), magazyn Hamasu, czy „Risalet al-Ichwan" („Przesłanie Braci") – Braci Muzułmanów, a także siedziby ważnych muzułmańskich instytucji i wielkich zgromadzeń islamskich aktywistów. Mieszkało tu lub nadal mieszka wielu radykalnych imamów głoszących antyzachodnie kazania. Mimo wyraźnej agresji werbalnej, a niekiedy i fizycznej, muzułmanie cieszą się w Wielkiej Brytanii dużą swobodą i wciąż mogą liczyć na pobłażanie. Przyczyną tego jest system prawny, do którego w 1997 r. została włączona Europejska Konwencja Praw Człowieka z 1989 r. Na tej podstawie można zostać ukaranym za nawet najmniejszą krytykę muzułmańskich mniejszości, w tym za określenie „islamski terroryzm", oceniane jako islamofobia. Nawet po zamachach w Londynie z 7 lipca 2005 r., w których zginęło ponad 50 osób, a 700 zostało rannych, media i politycy używali pojęcia „terroryzm", bez religijnych konotacji, aby nie wzbudzić niezadowolenia i napięcia w środowiskach brytyjskich muzułmanów. Do dziś ich organizacje skupiające obywateli Zjednoczonego Królestwa w różnych częściach globu mogą liczyć na pomoc finansową. Islamscy ideolodzy mieli przyzwolenie na propagowanie najbardziej wojowniczych idei pod warunkiem, że nie będą próbowali wcielać ich w życie na terytorium Wielkiej Brytanii (podobnie jak w Niemczech). Co prawda po zamachach z 11 września 2001 r. uchwalono w Wielkiej Brytanii zbiór przepisów antyterrorystycznych, jednak przez długi czas pozostawały one jedynie na papierze. Dopiero po zamachach w Londynie w lipcu 2005 r. podjęto bardziej stanowcze działanie wymierzone w muzułmańskich kaznodziejów nienawiści, ale upłynęły kolejne lata zanim udało się ich wydalić z kraju. Mustafa Kemal Mustafa alias Abu Hamza al-Masri został ekstradowany do USA dopiero w październiku 2012 r., a Omara Mahmuda Osmana alias Abu Katada al-Filastiniego przekazano Jordanii dopiero w lipcu 2013 r. Obaj po usłyszeniu niekorzystnych dla siebie wyroków odwoływali się do sądów wyższej instancji i Europejskiego Trybunału Praw Człowieka. W ich obronie stawały międzynarodowe organizacje humanitarne, mimo że dopuścili się zbrodni terroryzmu i mieli na rękach krew niewinnych ludzi. Te przykłady nie wpisały się w regularne działania brytyjskich organów ścigania. Nadal stosowano politykę udobruchania (ang. *appeasement*) islamu, czyli stosowania ustępstw i przywilejów wobec muzułmanów. Nadawano im szczególne uprawnienia kosztem innych grup społecznych. Ten specjalny status zwalniał muzułmanów z przestrzegania norm, których naruszenie przez członków innych grup społecznych jest zagrożone sankcjami. W Wielkiej Brytanii, jako jedynym już byłym państwie UE, pozwolono mniejszościom muzułmańskim na stosowanie szariatu w sprawach cywilnych (m.in. małżeństwa i sprawy spadkowe).

Program wspierania wielokulturowości zakładał powstrzymanie niezadowolenia wśród przybyszów, przede wszystkim z krajów muzułmańskich, i osłabienia ich krytycznego stosunku do nowej ojczyzny. Te kalkulacje jednak całkowicie zawiodły, a przyjazna polityka kolejnych rządów doprowadziła tylko do wzrostu islamskiego ekstremizmu[25]. Problemy pogłębiły się po wielkiej fali migracyjnej w 2015 r. Brytyjska policja, podobnie jak w innych krajach zachodnich, notorycznie ukrywała przed opinią publiczną przestępstwa popełniane przez mniejszości muzułmańskie. Strach przed oskarżeniem o rasizm wręcz paraliżuje działania zachodnich sił bezpieczeństwa. Przykładem tego jest skrzętne skrywanie przez policję wykorzystania seksualnego przez pakistańskie gangi ok. 1400 brytyjskich dziewcząt, które ciągnęło się przez 10 lat. Dopiero gdy sprawy nie dało się już tuszować, w raporcie napisano m.in., że powodem zaniechania wyjaśnienia, wyciszania i bagatelizowania tych przestępstw była obawa organów ścigania przed zarzutami o rasizm, a także przed politycznymi konsekwencjami zwrócenia się przeciwko mniejszości etnicznej[26].

Przez pewien czas model społeczeństwa wielokulturowego, obowiązujący w Wielkiej Brytanii, był popierany także przez Szwecję. Państwo szwedzkie jest postrzegane jako jedno z najbardziej liberalnych i przyjaznych imigrantom. W 2015 r. kraj ten przyjął ponad 160 tys. imigrantów, najwięcej w Europie, biorąc pod uwagę ogólną liczbę mieszkańców (10 mln). Szwecja plasowała się na drugim (po Belgii) miejscu w UE pod względem liczby ochotników *per capita*, którzy wyjechali walczyć na Bliski Wschód. Było to 32 dżihadystów na milion mieszkańców. Wyjazdy ochotników do Państwa Islamskiego i udział w walkach nie były traktowane jako przestępstwo. Szwedzcy *foreign fighters* (zagraniczni bojownicy – przyp. red.) mogli bezpiecznie powrócić do kraju, wyleczyć rany i znowu wyjechać na front dżihadu. Również w Finlandii uczestniczenie *foreign fighters* w walkach zbrojnych za granicą nie było przestępstwem, podobnie jak i samo członkostwo w organizacjach uznanych za terrorystyczne. Szwecja od dawna jest jednym z najbardziej atrakcyjnych krajów dla imigrantów, gdyż oprócz wielu przyznanych im świadczeń mogli oni tutaj czuć się całkowicie bezkarni[27]. Panuje tu daleko posunięta polityczna poprawność. Szwedzkie elity chyba najbardziej w UE posunęły się w swojej oikofobii, czyli niechęci do własnej tożsamości i cywilizacji, oraz ksenofilii – preferowaniu obcych kultur. W 2006 r. premier Szwecji Fredrik Reinfeldt z liberalno-konserwatywnej Umiarkowanej Partii Koalicyjnej oświadczył: *Tylko barbarzyństwo*

---

[25] G. Wilk-Jakubowski, *Sytuacja społeczna muzułmanów w Wielkiej Brytanii*, Kraków 2013, s. 152–153. Obszernie na temat antybrytyjskiej aktywności środowisk muzułmańskich i polityki brytyjskiego rządu wobec tych mniejszości pisze M. Phillips. Zob. tenże, *Londonistan. Jak Wielka Brytania stworzyła państwo terroru*, Warszawa 2010.

[26] G. Drymer, *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów*, „Rzeczpospolita", 30 IX 2017 r., https://www.rp.pl/Spoleczenstwo/309289949-Afery-seksualne-w-Wielkiej-Brytanii-Gwalty-muzulmanskich-gangow.html [dostęp: 1 X 2017].

[27] K. Izak, *Ograniczenia i problemy w zwalczaniu terroryzmu i przestępczości imigrantów w Europie*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 118–120.

jest autentycznie szwedzkie. Cały dalszy rozwój został przyniesiony z zewnątrz[28]. W tej kulturze samokrytyki klasę polityczną wspierały szwedzkie kościoły. Zarówno arcybiskup Antje Jackelén, jak i inni znani duchowni przekonywali, że szwedzka polityka imigracyjna musi uwzględniać to, że sam Jezus był uchodźcą. Później było już tylko gorzej. W grudniu 2014 r. ten sam premier (Reinfeldt - przyp. red.) udzielił wywiadu telewizyjnego, w którym powiedział, że Szwedzi są „nieciekawi", że granice to „fikcyjne" twory oraz że Szwecja należy do ludzi, którzy tam przyjechali w poszukiwaniu lepszego życia, nie zaś do tych, którzy tam mieszkają od pokoleń. W czasie fali migracyjnej w 2015 r. politycy oraz rzekomi i prawdziwi islamofile, wywodzący się często z kręgów dziennikarskich i naukowych, posuwali się nawet do stwierdzeń, że imigranci (…) *ubogacą chylącą się ku upadkowi kulturę europejską*[29]. Zapewniali, że ludności nie będzie przeszkadzało, jeśli zastąpią ich przybysze z innych regionów świata. Chociaż sytuacja w 2015 r. z pewnością nie była normalna, władze wielu państw UE udawały, że nic złego się nie dzieje. Na przykład w październiku 2015 r. rząd Szwecji zorganizował konferencję zatytułowaną „Szwecja razem", promującą jego politykę migracyjną. W konferencji wzięła udział para królewska i większość elity politycznej, a wystąpienie miała m.in. Ingrid Lomfors, szefowa Living History Forum (instytucji szerzącej wiedzę o Holokauście). W swoim powszechnie chwalonym przemówieniu Lomfors postawiła trzy tezy: 1. Imigracja do Szwecji to nic nowego; 2. Każdy jest migrantem; 3. Nie ma czegoś takiego, jak szwedzka kultura[30]. Ta ostatnia teza świadczy o absurdalnych poglądach zwolenników mieszania różnych nacji, kultur i religii. Taką postawę prezentuje klasa polityczna Szwecji, mimo niezaprzeczalnych faktów – m.in. odnotowanej w 2015 r. najwyższej na świecie po Lesotho liczbie gwałtów na tysiąc mieszkańców. Szwedzka prasa rzadko informowała o takich zdarzeniach, a jeśli już to robiła, to celowo przeinaczała fakty. Ponadto policję w Szwecji obowiązuje klauzula 291. Pod tym numerem kryje się zakaz informowanie mediów o wszelkich incydentach z udziałem imigrantów. Nic zatem dziwnego, że w 2016 r. Adly Abu Hajar, imam z Malmö, stwierdził, że Szwecja jest najlepszym islamskim państwem[31].

Zmiana w postrzeganiu „dobrodziejstwa" imigracji i wielokulturowości

Po zamachach z 13 listopada 2015 r. w Paryżu (w których zginęło 131 osób, a ponad 300 zostało rannych) prezydent François Hollande powiedział, że Francuzi muszą pozostać silni wobec terroryzmu. Były premier François Fillon stwierdził natomiast, że wojna

---

[28] D. Murray, *Przedziwna śmierć Europy. Imigracja. Tożsamość. Islam*, Poznań 2017, s. 325.

[29] Tamże, s. 164.

[30] Tamże, s. 165–166.

[31] A. Gromkowska-Melosik, *Mniejszość muzułmańska w Szwecji: między ekstremistycznym izolacjonizmem a procesami reprodukcji ekonomicznej*, „Studia Edukacyjne" 2013, nr 26, www. repozytorium.amu.edu.pl, s. 64.

już u nich jest. Policja prosiła paryżan o pozostanie w domach dla ich bezpieczeństwa. W odpowiedzi na ataki tymczasowo zamknięto granice Francji, a siły zbrojne zostały postawione w stan gotowości. W całym kraju ogłoszono stan wyjątkowy, który kilkakrotnie przedłużano (został zniesiony 1 listopada 2017 r.)[32]. Nie uchroniło to jednak kraju od następnych zamachów. Do kolejnego krwawego ataku doszło w dniu święta narodowego, 14 lipca 2016 r. Terrorysta rozpędzonym samochodem ciężarowym rozjeżdżał ludzi spacerujących deptakiem. Zginęło 87 osób, a ponad 200 zostało rannych. Premier Manuel Valls podczas ogłaszania żałoby narodowej wypowiedział słowa: *Francja będzie musiała nauczyć się żyć z terroryzmem*, które utkwiły w pamięci Francuzów. Wielu z nich potraktowało je jako wyraz arogancji rządu, który nie wywiązuje się z obowiązku zapewnienia ochrony swoim obywatelom, natomiast zwalcza wszelkie przejawy nacjonalizmu, islamofobii i rasizmu. Władze nie podjęły konsekwentnych działań wymierzonych w radykalne środowiska muzułmańskie, natomiast zareagowało francuskie społeczeństwo. Po raz pierwszy w tak dużej liczbie zagłosowało w wyborach prezydenckich na Marine Le Pen, przywódczynię skrajnie prawicowego Frontu Narodowego. Zakwalifikowała się ona do drugiej tury wyborów, w której uzyskała prawie 34 proc. poparcia, ale przegrała z Emmanuelem Macronem. W programie obiecywała m.in. pierwszeństwo dla Francuzów na rynku pracy, większe opodatkowanie dla firm zatrudniających cudzoziemców, walkę z nielegalną imigracją oraz zmniejszenie jej do zera, a także deportację wszystkich osób, które nielegalnie wjechały na teren kraju, cudzoziemców z wyrokami sądowymi oraz osób figurujących w kartotece „Fiches S", czyli stanowiących poważne zagrożenie bezpieczeństwa narodowego[33]. W tamtych wyborach muzułmanie z drugiego pokolenia imigrantów stanowili 8 proc. elektoratu Le Pen, mimo jej antyimigranckiego programu wyborczego. Nie ukrywają oni, że ich rodaków powinna obowiązywać zasada: integracja lub powrót do kraju. Zdają sobie sprawę z tego, że Francuzi coraz gorzej postrzegają Arabów. Wszystkich traktują jednakowo, ze szkodą dla zasymilowanych imigrantów, którzy z kolei przez współwyznawców są uważani za zdrajców. Wielu zasymilowanych imigrantów uważa również, że osoby z ich nowego pokolenia, które unikają pracy, wyłudzają świadczenia, głoszą antyfrancuskie hasła czy popełniają przestępstwa, powinni być deportowane[34].

Po objęciu funkcji prezydenta Emmanuel Macron powoli zaostrzał politykę wobec nielegalnych imigrantów. Z jednej strony oficjalnie głosił poparcie dla akcji humanitarnych i zgadzał się na przyjmowanie kolejnych osób przepływających przez Morze Śródziemne do Europy, ale z drugiej – urzędnicy utrudniali legalizację ich pobytu. Przez

---

[32] *Francja zamyka granice. Stan wyjątkowy w całym kraju*, TVN24, 14 XI 2015 r., https://tvn24.pl/swiat/francja-zamyka-granice-i-wprowadza-stan-wyjatkowy-ra594403-3318007 [dostęp: 14 XI 2015].

[33] „Fiches S" to kartoteka osób, które potencjalnie zagrażają bezpieczeństwu państwa, sporządzona przez Direction Générale de la Sécurité Intérieure, DGSI (Dyrekcję Generalną Bezpieczeństwa Wewnętrznego). W 2015 r. premier Manuel Valls poinformował, że w kartotece figuruje 20 tys. osób, w tym 10,5 tys. związanych z ekstremizmem islamskim. Pozostali to członkowie ruchów ultraprawicowych, lewackich itp.

[34] A. Pamuła, *Wrzenie. Francja na…*, s. 150–152.

zaskoczenie, aby nie prowokować członków organizacji humanitarnych oraz organizacji działających na rzecz praw człowieka, likwidowano nielegalne obozowiska imigrantów w Calais (słynna „dżungla"), w Paryżu i w innych wielkich miastach. Policja zaczęła przewozić na włoską stronę granicy imigrantów zatrzymanych na terytorium Francji, którzy nie mieli dokumentów, a na teren Francji przedostali się z Włoch drogą przez miasto Ventimiglia lub przez Alpy. Po raz pierwszy było widać, że władze coraz częściej stosują rozwiązania siłowe, a nie słowną perswazję i obietnice. Rekordowa liczba imigrantów we Francji nadwyrężyła działanie systemu pomocy społecznej, wygenerowała olbrzymie koszty zarówno dla mieszkalnictwa socjalnego, jak i funduszy oferujących zapomogi. Merowie siedmiu francuskich miast: Nantes, Lille, Bordeaux, Grenoble, Rennes, Tuluzy i Strasburga podpisali się pod listem otwartym skierowanym do rządu z prośbą o ratunek przed społeczną katastrofą wywołaną olbrzymią liczbą imigrantów, manifestowali również przeciw organizowaniu przez muzułmanów modlitw na ulicach miast. Ekspert ds. imigracji Patrick Weil z Centre national de la recherche scientifique (Narodowego Centrum Badań Naukowych, odpowiednik Polskiej Akademii Nauk) stwierdził, że podejście Macrona wobec imigrantów jest (…) *najbardziej ekstremalnym od czasów wojny*[35]. W przeprowadzonym sondażu 60 proc. Francuzów wyraziło opinię, że imigracja negatywnie wpłynęła na sposób ich życia. W raporcie francuskiego senatu dotyczącym walki z radykalizacją wyznawców islamu autorzy stwierdzili wprost, że muzułmańscy imigranci nie są w stanie zintegrować się ze społeczeństwem, a kwota 100 mln euro wydatkowana przez państwo w ostatnich latach na prewencję i ośrodki wychowawcze przyniosła niewielkie efekty. Minister spraw wewnętrznych Gerard Collomb stwierdził w grudniu 2017 r., że Francji grozi poważny kryzys, ponieważ sytuacja już teraz jest wybuchowa[36].

Zmieniło się nastawienie władz do islamskich ekstremistów osadzonych w zakładach karnych. Stwierdzono, że byli oni w stanie wywierać wpływ na innych więźniów, co skutkowało zorganizowaniem strajków w 2014 i 2016 r. W 2014 r. więźniowie domagali się prawa do brania prysznica w bieliźnie i do nierewidowania ich przez strażników, co argumentowali religijną skromnością i obowiązującym ich zakazem kontaktu z „nieczystymi" niewiernymi. Gdyby władze więzienne zgodziły się na te żądania, umożliwiłoby to swobodne przekazywanie sobie przez więźniów dowolnych przedmiotów. Natomiast w 2016 r. doszło do kilkutygodniowych zamieszek w więzieniach, a następnie 200 więźniów w różnych zakładach (na rozkaz kilku terrorystów, którzy powrócili z Państwa Islamskiego) odmówiło powrotu do cel. Odpowiedzią władz

---

[35] O. Górzyński, *Macron robi „porządek" z migrantami. Le Pen triumfuje*, 27 XII 2017 r., https://wiadomosci.wp.pl/macron-robi-porzadek-z-migrantami-le-pen-triumfuje-6202896011315329a [dostęp: 27 XII 2017]; J. Muller, *„Kryzys na niespotykaną skalę". Burmistrzowie 7 miast Francji przeciw fali imigrantów*, 19 XII 2017 r., https://www.o2.pl/artykul/kryzys-na-niespotykana-skale-burmistrzowie--miast-francji-przeciw-fali-imigrantow 6200161017976449a [dostęp: 19 XII 2017].

[36] B. Dobosz, *Francja marnotrawi setki milionów euro na asymilację muzułmanów. Przywłaszczenia to codzienność*, 13 VII 2017 r., http://www.pch24.pl/francja-marnotrawi-setki-milionow-euro-na--asymilacje-muzulmanow-przywlaszczenia-to-codziennosc,53044,i.html [dostęp: 13 XII 2017].

więziennych było stworzenie specjalnych oddziałów, tak zwanych Unité de prévention de la radicalisation, UPRA (Odziałów Zapobiegających Radykalizacji). Ich zadaniem było prowadzenie różnych zajęć dla najbardziej zradykalizowanych więźniów. W ten sposób podjęto próbę ich zderadykalizowania. To rozwiązanie okazało się zawodne po tym, jak Bilal Taghi, francusko-marokański dżihadysta skazany za podróż do Państwa Islamskiego w Syrii, który został uznany za zderadykalizowanego, próbował zamordować dwóch strażników. Po ataku Taghiego minister spraw wewnętrznych zapowiedział wzmocnienie procedur bezpieczeństwa, aby chronić strażników. Jednak w 2018 r. doszło do kolejnej próby zamordowania trzech strażników, których zaatakował dżihadysta pochodzący z Niemiec. Po tym ataku doszło do strajku personelu więziennego i wprowadzono jeszcze surowsze zasady bezpieczeństwa. Wobec tego zrezygnowano z ambitnego celu „deradykalizacji" dżihadystów i zastąpiono go skromniejszym „powstrzymaniem przed stosowaniem przemocy". Utworzono nową służbę specjalną o nazwie Service national du renseignement pénitentiaire, SNRP (Krajowy Wywiad Więzienny). Przede wszystkim zradykalizowanych więźniów, którzy dotychczas przebywali głównie w czterech więzieniach regionu paryskiego, przeniesiono do 79 więzień o specjalnej procedurze i z odpowiednio przeszkolonymi strażnikami, rozproszonych na terenie całego kraju. W miejsce UPRA utworzono siedem oddziałów Quartiers d'évaluation de la radicalisation, QER (Oddziały Oceny Radykalizacji), w których przygotowano 140 miejsc. Zradykalizowani więźniowie są przez cztery miesiące obserwowani nie tylko przez specjalnie przeszkolonych strażników więziennych, lecz także przez specjalistów ds. zwolnień warunkowych, psychologów i pedagogów. W ten sposób skończono z tolerancją i przywilejami dla osadzonych muzułmanów[37].

W dniu 25 września 2020 r. imigrant ciężko ranił nożem dwie osoby. Zdarzenie miało miejsce w pobliżu dawnej siedziby redakcji tygodnika satyrycznego „Charlie Hebdo", w którym 1 września ponownie zamieszczono karykatury proroka Muhammada. Terrorysta uważał, że atakuje dziennikarzy magazynu, tymczasem ofiarami byli dziennikarze agencji Premieres Lignes. Zamachowiec nie wiedział, że po atakach terrorystycznych z 7 stycznia 2015 r. satyryczny tygodnik zmienił siedzibę, a jego nowy adres jest utrzymywany w tajemnicy. Po wrześniowym ataku 2 października 2020 r. prezydent Macron przedstawił plan walki z islamistycznym separatyzmem, zawarty w pięciu punktach. Ogłosił zamiar „uwolnienia" islamu we Francji od obcych wpływów i stworzenia islamu „oświeconego". Zapowiedział też, że z końcem roku zostanie uchwalona specjalna ustawa, której założeniem ma być obrona laickości Republiki przed rosnącym w siłę konserwatywnym i politycznym islamem. Powiedział również, że Francja musi się zmierzyć z islamistycznym separatyzmem i określił go jako: (…) *świadomy,*

[37] G. Lindenberg, *Najwięcej ekstremistów we francuskich więzieniach*, 4 X 2020 r., https://euroislam.pl/najwiecej-ekstremistow-we-francuskich-wiezieniach/ [dostęp: 4 X 2020]. W połowie 2020 r. we francuskich więzieniach przebywało 3 tys. osób „uważanych za zradykalizowane lub podejrzewanych o radykalizację". Z tej liczby 522 osoby zostały skazane za przestępstwa związane z terroryzmem islamskim, a 900 to radykalni muzułmanie skazani za przestępstwa pospolite.

teoretyczny, polityczno-religijny projekt[38] mający na celu powstanie kontrspołeczeństwa opartego na zasadach niezgodnych z obowiązującym prawem. Państwo ma przejąć kontrolę nad kształceniem imamów oraz finansowaniem organizacji muzułmańskich. W ten sposób ulegnie likwidacji system obowiązujący od 1977 r., który powoduje, że do francuskich meczetów są wysyłani radykalni imamowie z takich państw, jak Algieria, Maroko czy Turcja. Łatwiejsza będzie wówczas walka nie tylko z radykalnym islamem, lecz także z agentami wpływu. Do szkół (również prywatnych) zostanie wprowadzone obowiązkowe wychowanie w duchu wartości republikańskich. Dzieci, które pozostają w systemie edukacji domowej, będą musiały wrócić do szkolnych ław. Dotyczy to 62 tys. uczniów. Zaplanowano zamknięcie nielegalnych szkół, często zarządzanych przez religijnych ekstremistów. Francja chce stworzyć wersję islamu „oświeconego", który da się pogodzić z laickimi wartościami Republiki. Drogą do osiągnięcia tego celu ma być ograniczenie wpływów szkół koranicznych i innych szkół kształcących dzieci i młodzież w duchu islamskim. Macron dodał, że certyfikacja imamów w kraju zmieni się wraz ze sformalizowaniem ich kształcenia przez Conseil français du culte musulman, CFCM (Francuską Radę Kultu Muzułmańskiego)[39]. Władze uzasadniły wprowadzenie nowego prawa potrzebą walki z islamskim separatyzmem, w którym są faworyzowane prawa religijne kosztem laickich wartości Republiki Francuskiej. Macron określił islam jako religię, która jest obecnie w kryzysie na całym świecie. W swoim przemówieniu skupił się na walce z islamskim radykalizmem we Francji. Zapowiedział także nadzór nad finansowaniem meczetów. Przyznał też, że państwo francuskie jest częściowo odpowiedzialne za „gettoizację" muzułmańskich mieszkańców. Organizacje religijne wykorzystały błędy w polityce integracyjnej do własnych celów, mi.in. nasilania antagonizmów społecznych. Macron powiedział również, że kolonialna przeszłość Francji, w tym kolonizacja Algierii, zostawiła blizny w świadomości społecznej, które czasami utrudniają integrację imigrantów z byłych kolonii. Zaznaczył: *Nie uporaliśmy się z naszą przeszłością*[40]. Wiceminister spraw wewnętrznych Marlene Schiappa, odpowiedzialna za sprawy

---

[38] https://religie.wiara.pl/doc/6553063.Macron-Nowe-prawo-i-ostrzejsze-zasady-wobec-separatyzmu [dostęp: 3 X 2020].

[39] Rada powstała w grudniu 2002 r. z inicjatywy Nicolasa Sarkozy'ego, ówczesnego ministra spraw wewnętrznych, który chciał mieć jednego partnera do rozmów z rozdrobnionym środowiskiem muzułmańskim. Radę utworzono w wyniku złożonej procedury. Chcąc utrzymać równowagę w Radzie, państwo zadbało, aby jej przewodniczącym został Dalil Bubaker, rektor Instytutu Muzułmańskiego przy paryskim Wielkim Meczecie, najstarszej instytucji muzułmańskiej w kraju, znajdującej się pod silnym wpływem Algieru (przedstawiciele Instytutu Muzułmańskiego uzyskali słaby wynik w wyborach do władz CFCM, dlatego francuskie MSW wyznaczyło Bubakera na jej przewodniczącego). Wpływową osobą był jej wiceprzewodniczący Fuad Alawi, wówczas sekretarz generalny Union des organisations islamiques de France, UOIF (Unii Organizacji Muzułmańskich Francji). W 2013 r. UOIF opuściła CFCM, a w lutym 2017 r. przekształciła się w organizację Musulmans de France (Muzułmanie Francji), uzurpując sobie prawo to reprezentowania całej mniejszości muzułmańskiej w kraju. Obecnie CFCM jest reprezentantem dziewięciu federacji i stowarzyszeń muzułmańskich.

[40] O. Bault, *Francuska dziwna wojna z islamizmem*, „Do Rzeczy", 29 X 2020 r., https://dorzeczy.pl/swiat/158991/francuska-dziwna-wojna-z-islamizmem.html [dostęp: 29 X 2020]; P. Kryszak,

obywatelstwa, zapowiedziała deportowanie z Francji poligamistów. Nie uchroni ich przed tym to, że są już obywatelami kraju ani że posiadają pozwolenie na pobyt. Będą mogli w nim pozostać jedynie wtedy, gdy podporządkują się francuskiemu prawu. Minister poinformowała również, że sporządzanie „certyfikatów dziewictwa" dla kobiet i dziewcząt będzie zabronione. Nie mogą one być traktowane jak „krowy na targu"[41].

Punktem zwrotnym w postrzeganiu „dobrodziejstwa" imigracji i wielokulturowości było brutalne zamordowanie nauczyciela historii Samuela Paty'ego przez 18-letniego zradykalizowanego Czeczena Abdullaha Anzorowa. Do zbrodni doszło 16 października 2020 r. Śledztwo wykazało, że w zamach byli zamieszani inni młodzi muzułmanie oraz ich rodzice. To wydarzenie po raz pierwszy spotkało się ze zdecydowanym działaniem władz. Minister spraw wewnętrznych Gerald Darmanin nakazał policji deportację 231 nielegalnych imigrantów znanych z ekstremalnych poglądów religijnych oraz zaostrzenie kontroli osób ubiegających się o pozwolenie na pobyt we Francji pod kątem ich stosunku do państwa przyjmującego i do islamu. Polecił również policji zaostrzenie kontroli osób chcących uzyskać status uchodźcy i dokładniejsze badanie wniosków w tej sprawie, aby wykluczyć kolejnych islamskich ekstremistów, a także przygotowanie listy organizacji i instytucji muzułmańskich znanych z krzewienia radykalnych idei. Zapowiedziano podjęcie działań mających na celu wykorzenienie mowy nienawiści w mediach społecznościowych. W dniu 20 października władze nakazały zamknięcie na pół roku Wielkiego Meczetu Pantin w Seine-Saint-Denis na przedmieściach Paryża, w którym były wygłaszane kazania pełne nienawiści do Francji i Europy. W odpowiedzi na działania władz głos zabrał Collectif contre l'islamophobie en France, CCIF (Kolektyw Przeciwko Islamofobii we Francji). Poczuł się on zaniepokojony presją polityczną wywieraną przez polityków najwyższego szczebla oraz kampanią zastraszania skierowaną przeciw organizacji, której zadaniem jest zwalczanie dyskryminacji obywateli muzułmańskich i przestępstw z nienawiści wobec nich. Na to oświadczenie ostro zareagował minister Darmanin, który zapowiedział zdelegalizowanie CCIF. Rozwiązanie miało dotyczyć 50 innych organizacji i instytucji muzułmańskich, np. BarakaCity[42]. Jej założyciel, Idris Sihamedi, został wcześniej oskarżony o nękanie, publiczne obrażanie i kierowanie gróźb karalnych pod adresem dziennikarki stacji radiowej RMC Zohry Bitan, która rzekomo miała się dopuścić obrazy proroka Muhammada. Francuskie władze zdecydowały o rozwiązaniu Kolektywu im. Szejka Jasina, wspierającego Hamas, kierowanego przez radykała Abdelhakima Sefriuiego. Został on aresztowany wraz

Narasta konflikt Francji z Turcją, „Gazeta Polska Codziennie" z 26 października 2010 r.; P. Ślusarczyk, *Prezydent Francji zapowiada walkę z islamskim separatyzmem*, https://euroislam.pl/prezydent-francji-zapowiada-walke-z-islamskim-separatyzmem/ [dostęp: 5 X 2020].

41 P. Petrović, *Francja walczy z islamskim separatyzmem*, „Gazeta Polska Codziennie" z 7 października 2020 r.

42 Francuska muzułmańska organizacja pozarządowa o charakterze humanitarnym, https://pl.wikipedia.org/wiki/Barakacity [dostęp: 2 III 2021] – przyp. red.

z innymi osobami za udział w zorganizowaniu nagonki w mediach społecznościowych na Samuela Paty'ego, co skończyło się jego zabójstwem[43].

W dniu 29 października doszło do kolejnego zamachu. Tunezyjski imigrant, uzbrojony w nóż, zaatakował w bazylice Notre Dame w Nicei. Zginęły trzy osoby, jedną z nich (kobietę) terrorysta zdekapitował. Po tym zdarzeniu zaostrzono kontrolę granicy francusko-włoskiej i zorganizowano wspólne patrole służb granicznych obu krajów w celu wyłapywania nielegalnych imigrantów próbujących przedostać się do Francji. Kolejną reakcją Pałacu Elizejskiego na wzrost zagrożenia terrorystycznego było zlecenie CFCM opracowania kodeksu etyki imamów. Władze w porozumieniu z CFCM postanowiły powołać Conseil national des imams, CNI (Narodową Radę Imamów), która miała odpowiadać za kształcenie muzułmańskich kaznodziejów (arab. *chatib*) i imamów. Pracownicy CNI byliby zobowiązani do nadzorowania ich pracy oraz pozbawiania praw do wykonywania zawodu tych imamów i kaznodziejów, którzy głoszą radykalne treści i sympatyzują z islamskimi ekstremistami. Wspomniany kodeks etyki imamów ma być oparty na zbiorach zasad podobnych do tych, które obowiązują lekarzy i adwokatów. Wśród postulatów kodeksu znalazło się stwierdzenie, że islam jest religią, a nie ruchem politycznym i nie może ulegać obcej ingerencji w sprawy wspólnot muzułmańskich na terenie Francji. Podczas spotkania z przedstawicielami CFCM prezydent Macron przedstawił Charte des valeurs républicaines (*Kartę wartości republikańskich*) z prośbą o jej akceptację w ciągu 15 dni. Rząd miał wywierać presję, aby kartę podpisały organizacje i instytucje powiązane z ruchem Braci Muzułmanów oraz wspólnoty pochodzące z Turcji, które wykorzystują religię do nacisków politycznych w Europie. Dopełnieniem działań władz państwowych okazało się opublikowanie w listopadzie 2020 r. książki pt. *Immigration - Ces réalités qu'on nous cache* (*Imigracja – realia, które ukrywamy*). Jej autorem jest Patrick Stefanini, członek Rady Stanu i były prefekt. Stefanini przez lata zajmował się problemem imigracji. Jego książka to pierwsze tego typu rzetelne opracowanie. Zawiera szczegółowe informacje i dane statystyczne, których kolejne francuskie rządy przez 30 lat nie chciały ujawniać przed społeczeństwem[44]. W tym samym miesiącu CCIF ogłosił decyzję o samorozwiązaniu. Dnia 9 grudnia 2020 r. na posiedzeniu Rady Ministrów premier Jean Castex zaprezentował projekt ustawy dotyczącej walki z islamistycznym separatyzmem. W dokumencie szczegółowo rozpisano zadania stojące przed administracją rządową i wspólnotami muzułmańskimi, które miały na celu ograniczenie wpływu islamskich radykałów, stanowiących obecnie największe zagrożenie bezpieczeństwa obywateli i spójności państwa[45]. Jednocześnie dekretem Rady

---

[43] J. Bielecki, *Emmanuel Macron w końcu wypowiada wojnę islamistom*, „Rzeczpospolita", 20 X 2020 r.; https://www.rp.pl/Polityka/201029902-Emmanuel-Macron-w-koncu-wypowiada-wojne-islamistom.html [dostęp: 22 X 2020].

[44] B. Dobosz, *Islamski terroryzm przestaje być tabu*, „Najwyższy czas" 2020, nr 50–51.

[45] J. Kowalkowska, *Macron tworzy muzułmańską kurię*, „Gazeta Polska Codziennie" z 23 listopada 2020 r.; AFP, *„Séparatismes": un projet de loi „pas contre les religions", selon Jean Castex* https://www.france24.com/fr/france/20201209-séparatismes-le-gouvernement-présente-son-projet-

Ministrów rozwiązano CCIF (prawdopodobnie, aby jego działacze nie podjęli za jakiś czas decyzji o wznowieniu działalności), ale w obronie organizacji stanęły Human Rights Watch i Human Rights League, które potępiły tę decyzję, a Council on American-Islamic Relations, CAIR (Rada ds. Stosunków Amerykańsko-Islamskich), która znajduje się pod silnymi wpływami Braci Muzułmanów, zaoferowała swoje wsparcie. Mając za sobą poparcie tych instytucji były CCIF złożył skargę do Trybunału Sprawiedliwości przeciwko ministrowi spraw wewnętrznych o nieuzasadnione oskarżenie dotyczące bezpośredniego udziału CCIF w zabójstwie Samuela Paty'ego i ogłosił, że kwestionuje dekret Rady Ministrów dotyczący jego delegalizacji. Dochodzenie nie podtrzymało hipotezy o udziale organizacji w zabójstwie nauczyciela[46]. W dniu 29 grudnia rektor Wielkiego Meczetu Paryża Chems Eddine Hafiz ogłosił wycofanie swojego udziału w spotkaniach mających na celu powołanie CNI. Ponadto islamistyczne komórki mające wpływy w CFCM skutecznie blokowały podpisanie *Karty wartości republikańskich*[47]. Do jej akceptacji doszło 17 stycznia 2021 r., mimo że kilka federacji muzułmanów było przeciwnych stwierdzeniom, że islam można pogodzić z francuskimi prawami i wartościami. Podpisanie dokumentu przez przedstawicieli władz organizacji zrzeszonych w CFCM nie oznacza jednak, że zawarte w nim zapisy będą realizowane. Dopiero teraz bowiem ma się rozpocząć dyskusja z imamami i przywódcami gmin muzułmańskich we Francji nad uzyskaniem jak najszerszego poparcia dla *Karty*[48].

W Niemczech fala migracji z 2015 r. doprowadziła dwa lata później do kryzysu politycznego. Decyzję Angeli Merkel o szerokim otwarciu Niemiec na uchodźców z Bliskiego Wschodu można uznać za drugą tak przełomową, po zjednoczeniu kraju w 1989 r. Hasło polityczne: „Damy radę" („*Wir schaffen das*"), ukute przez samą kanclerz, rzeczywiście dobrze oddawało nadzieję i optymizm panujący wówczas w kręgach władzy co do możliwości opanowania kryzysu uchodźczego. Poparcie dla przyjmowania kolejnych uchodźców jednak z miesiąca na miesiąc topniało. W listopadzie 2016 r. badania sondażowe wskazały, że aż 69 proc. respondentów w Niemczech opowiadało sie za natychmiastowym wstrzymaniem przyjmowania uchodźców. Przemoc wobec przybyszów i rosnący w siłę ruch antyislamski stawały się coraz bardziej widocznymi elementami niemieckiego społeczeństwa i niemieckiej polityki. Z perspektywy czasu coraz bardziej widać, że decyzja o niekontrolowanym przyjęciu uchodźców była raczej wyrazem myślenia życzeniowego niż racjonalnym rozstrzygnięciem, uwzględniającym

-de-loi-contre-l-islamisme-radical [dostęp: 9 XII 2020].

46 https://en.wikipedia.org/wiki/Collective_Against_Islamophobia_in_France [dostęp: 20 XII 2020].

47 *La grande Mosquée de Paris annonce son retrait du projet de Conseil national des imams*, „Le Monde" z 29 grudnia 2020 r., https://www.lci.fr/societe/la-grande-mosquee-de-paris-annonce-son-retrait-du-projet-de-conseil-national-des-imams-2174082.html [dostęp: 30 XII 2020].

48 *Francuska Rada Kultu Muzułmańskiego akceptuje zasady Macrona*, https://euroislam.pl/rada-muzulmanow-akceptuje-zasady-macrona/ [dostęp: 18 I 2021].

rzeczywistą sytuację polityczną[49]. Milionowa fala imigrantów, która przybyła do Europy, spowodowała dynamiczny wzrost notowań ugrupowań skrajnie prawicowych i populistycznych. Mimo to w 2018 r. niemieckie władze przygotowały do realizacji kolejny wielki projekt – przyjęcie kilkuset tysięcy imigrantów w ramach łączenia rodzin z tymi, którzy uzyskali już prawo pobytu.

Pomimo zwiększenia liczby pracowników w placówka konsularnych, okres oczekiwania na niemieckie wizy wydłużył się do siedmiu miesięcy, a nawet do roku, co wzbudziło niezadowolenie zwolenników przyjmowania imigrantów. Zasiadająca wówczas w rządzie partia Zielonych domagała się wprowadzenia nowych rozwiązań. Jej zdaniem podania o wizę mogłyby być rozpatrywane także przez personel Ministerstwa Spraw Zagranicznych w Berlinie, a nie tylko przez niemieckie ambasady i konsulaty. Byłaby to sytuacja bez precedensu, wymyślona przez kogoś, kto całkowicie stracił kontakt z rzeczywistością. Według informacji niemieckiego MSW do końca 2017 r. wnioski o azyl złożyło ok. 180 tys. uchodźców z Iraku i Syrii, a w roku następnym – ponad drugie tyle. Przy liczebności arabskich rodzin oznaczało to sprowadzenie kilkakrotnie większej liczby ludzi, oczywiście na koszt państwa – przy założeniu, że będą to wyłącznie członkowie najbliższej rodziny, a nie dalsi krewni. Na te nowe grupy imigrantów, które miały przybywać do Niemiec od 2018 r., nie chciała się zgodzić centroprawicowa i liberalna Freie Demokratische Partei, FDP (Partia Wolnych Demokratów), która w listopadzie 2017 r. zerwała rozmowy na temat utworzenia koalicji rządowej. Warto dodać, że w 2018 r. wygasł zakaz łączenia rodzin uchodźców i azylantów, który został wprowadzony w następstwie kryzysu imigracyjnego w 2015 r. Nowy rząd powstał dopiero w połowie marca 2018 r. z koalicji trzech urgupowań: Christlich Demokratische Union Deutschlands, CDU (Unii Chrześcijańsko–Demokratycznej), Christlich-Soziale Union in Bayern, CSU (Unii Chrześcijańsko-Społecznej w Bawarii) i Sozialdemokratische Partei Deutschlands, SPD (Socjaldemokratycznej Partii Niemiec). W tym czasie można było zaobserwować również coraz większą polaryzację społeczeństwa, której skutkiem były pro- i antyimigranckie manifestacje, wzrost poparcia dla organizacji skrajnie prawicowych, w tym obecność sympatyków nazizmu w armii i policji, propagujących w cyberprzestrzeni nazistowskie hasła i symbole. Władze jednak uznały, że większe zagrożenie stanowi skrajna prawica niż muzułmańskie getta i klany przestępcze. Taką opinię wydano w wyniku sukcesu wyborczego antyimigranckiej i ksenofobicznej Alternative für Deutschland, AfD (Alternatywy dla Niemiec), która w wyborach parlamentarnych w 2017 r. uzyskała trzecie miejsce (12,5 proc. głosów i 94 mandaty). Ta partia odniosła także liczne sukcesy w wyborach lokalnych. Zajęcie przez nią miejsca na oficjalnej scenie politycznej przyczyniło się do dalszej radykalizacji wszystkich ugrupowań skrajnej prawicy. Taki sam proces następuje również w szeregach AfD, czego dowodem może być powtórny wybór Björna Höckego, który jest znany z sympatii neonazistowskich, na szefa partii w Turyngii. Towarzyszą temu informacje o działalności

[49] M. Sulkowski, *Polityczne konsekwencje kryzysu imigracyjnego w Niemczech*, „Chrześcijaństwo-Świat-Polityka. Zeszyty Społecznej Myśli Kościoła" 2016, nr 20, s. 59.

grup rasistowskich w armii i policji, a nawet w wojskowej jednostce antyterrorystycznej. Bundeskriminalamt, BKA (Federalny Urząd Kryminalny) poinformował, że ponad 13 tys. osób powiązanych ze skrajną prawicą jest gotowych do użycia przemocy, a co najmniej 65 z nich stanowi bezpośrednie zagrożenie terrorystyczne. Cezurą zachowania rządu w stosunku do prawicowej ekstremy był zamach na szefa administracji okręgu Kassel Waltera Lubkego, zamordowanego w czerwcu 2018 r.[50]

Żaden z polityków nie chciał jednak przyznać, że źródłem zaostrzenia wewnętrznej sytuacji w kraju było otwarcie niemieckich granic dla setek tysięcy imigrantów. Dlatego dużym zaskoczeniem mogło być wezwanie partii Zielonych do nasilenia walki z zagrożeniem islamistycznym i morderczą ideologią, która za nim stała. Szef Zielonych Robert Habeck w jedenastu punktach przedstawił plan działania pod hasłem „Islamizm jest wciąż jednym z najpoważniejszych zagrożeń bezpieczeństwa wewnętrznego wszystkich wolnych społeczeństw". Jednym z elementów planu jest zwiększenie sił bezpieczeństwa w miejscach, w których trzeba prowadzić 24-godzinny nadzór nad ekstremistami. Wezwano także do deportacji osób stanowiących zagrożenie. Oczekuje się też, że zostanie wprowadzony zakaz działalności organizacji salafickich oraz że finansowanie tych grup będzie monitorowane. Zieloni chcą stworzenia rozbudowanej, ogólnokrajowej sieci przeciwdziałania radykalizacji. Miałaby się ona opierać na prewencyjnej współpracy z meczetami i społecznościami muzułmańskimi. W obliczu coraz większej grupy terrorystów, którzy mają opuścić więzienia, partia chce monitorować ich działania na wolności. Inicjatywa partii jest zaskakująca dla tych, którzy kojarzą lewicę głównie z polityką proimigracyjną, wielokulturowością i ustępstwami wobec mniejszości muzułmańskich. Na Zachodzie często mówi się o muzułmańsko-lewicowym sojuszu. Niemieckich Zielonych nie da się jednak tak łatwo zaklasyfikować. Robert Habeck przez lata uchodził w partii za osobę, która poza promowaniem tolerancyjnego społeczeństwa ostrzegała przed zagrożeniem, jakie stanowi muzułmański radykalizm. Przez wiele lat szefem partii Zielonych był Cem Özdemir, z pochodzenia Turek, zadeklarowany przeciwnik islamu politycznego i islamistów rządzących obecnie Turcją[51]. Dotychczas jednak niemieccy Zieloni popierali proimigrancką politykę rządu. Sprzeciwiali się deportacji nielegalnych imigrantów i często blokowali start samolotów z nimi na pokładzie.

W listopadzie 2019 r. rząd zaprezentował projekt ustawy, zgodnie z którą duchowni przybywający do Niemiec z krajów spoza UE muszą wykazać się znajomością języka niemieckiego. Chociaż zapisy ustawy dotyczą duchownych wszystkich wyznań, nie ulega wątpliwości, że władze chcą w ten sposób uregulować przede wszystkim pobyt muzułmańskich imamów i kaznodziejów. Z najnowszych danych przedstawionych przez Fundację Adenauera wynika, że w Niemczech znajduje się obecnie ok. 2 tys. meczetów, a 90 proc. pracujących tam imamów pochodzi z zagranicy. W styczniu 2019 r.

---

[50] Zob. P. Jendroszczyk, *Rosnący lęk przed skrajną prawicą*, „Rzeczpospolita" z 26 listopada 2020 r.

[51] J. Wójcik, *Niemieccy Zieloni: „Islamizm jest zagrożeniem"*, https://euroislam.pl/niemieccy-zieloni-islamizm-jest-zagrozeniem/ [dostęp: 18 X 2020].

niemieckie MSW poinformowało, że tylko w gminach podlegających Diyanet İşleri Türk-İslam Birliği, DITIB (Turecko-Islamskiej Unii Instytucji Religijnych) było zatrudnionych 1049 imamów i kaznodziejów. W projekcie ustawy zakłada się, że duchowni, którzy będą chcieli mieszkać i pracować w Niemczech, będą musieli w ciągu roku od przybycia do Niemiec udowodnić, że znają język niemiecki na tyle dobrze, aby móc rozmawiać. Niemiecki minister spraw wewnętrznych podkreślił wręcz, że znajomość języka jest koniecznością, aby integracja była skuteczna. Propozycja rządu spotkała się z krytyką ze strony Zielonych. Ich przedstawicielka Filitz Polat wyraziła zaniepokojenie, że ustawa pogorszy problem z niedoborem muzułmańskich duchownych niemieckiego pochodzenia. Niekiedy organizacje podkupują już wykształconych imamów, którzy z różnych przyczyn zmieniają swoją przynależność organizacyjną, np. po wygaśnięciu kontraktu imamowie z DITIB-u przechodzą do organizacji o nazwie Milli Görüs (Narodowa Świadomość/Wizja) i tam odbywają dodatkowe przeszkolenie uzupełniające. W listopadzie 2019 r. kanclerz Angela Merkel i minister spraw wewnętrznych Horst Seehofer przedstawili postulat, aby Niemcy sami kształcili imamów[52].

W 9-milionowej Austrii mieszka 700 tys. muzułmanów, z czego ponad 300 tys. w Wiedniu i okolicach. Przez wiele lat władze prowadziły liberalną politykę w stosunku do imigrantów i wyznawców islamu. W 2014 r. Sebastian Kurz, ówczesny minister spraw zagranicznych, przedstawił projekt nowej ustawy dotyczącej islamu. Znalazł się w nim m.in. zakaz finansowania meczetów i imamów z funduszy zagranicznych. Celem zmian było zwiększenie liczby imamów wykształconych w Austrii i mających austriackie obywatelstwo. Islamu mieli nauczać imamowie, którzy nie tylko poznali austriacką kulturę, lecz także byli świadkami problemów młodych muzułmanów w tym kraju. W ustawie stwierdzono wprost, że austriackie prawo ma priorytet przed szariatem. Ponadto zobowiązywano w niej wspólnoty muzułmańskie do przedłożenia swojej wykładni wiary i przekładu na język niemiecki dziewięciu wersji *Koranu*, będących w użyciu. W ustawie zakazywano imamom jakiegokolwiek uzasadniania przemocy. Środowiska muzułmańskie od razu oprotestowały projekt tej ustawy, twierdząc, że ze wszystkich muzułmanów czyni ona potencjalnych zamachowców. Jednocześnie austriaccy muzułmanie winą za radykalizację współwyznawców obciążyli… władze kraju i ich politykę (ale nie wyjaśnili, w czym tkwiła ich wina). Podobnie zareagowały niektóre media i politycy, twierdząc, że muzułmańskie organizacje bez trudu przyciągały młodych muzułmanów obietnicami lepszego życia. Proponowały walkę w gronie prawdziwych mężczyzn, możliwość uwolnienia od grzechów itp. W rezultacie w 2014 r. z Austrii do Syrii wyjechało ponad 160 dżihadystów. Problemem, tak jak i w innych krajach Europy, było finansowanie muzułmańskich stowarzyszeń oraz instytucji przez podmioty państwowe i organizacje pozarządowe z zagranicy: Arabii Saudyjskiej, ZEA, Kataru czy Turcji. W 2015 r. sytuacja uległa pogorszeniu, gdy

[52] A. Rusinek, *Nurt radykalny wśród społeczności*…, s. 73; *Niemcy: imamowie będą musieli udowodnić, że znają niemiecki*, 7 XI 2019 r., https://www.dw.com/pl/niemcy-imamowie-będą-musieli-uwodnić-że-znają-niemiecki/a-51148977 [dostęp: 7 XI 2019].

na zaproszenie Angeli Merkel do UE ruszyły setki tysięcy imigrantów z Bliskiego Wschodu i Afryki. Tylko w 2015 r. do Austrii przybyło ok. 100 tys. osób. Władze austriackie nie miały pojęcia, kim są i – podobnie jak pozostałe kraje przyjmujące – nie były w stanie zweryfikować ich tożsamości (ponad 70 proc. przybyszów poza smartfonami nie miało żadnych dokumentów). W tym czasie Sebastian Kurz domagał się zamknięcia szlaku bałkańskiego i zapowiadał stanowcze działania wobec osób związanych z radykalnym islamem[53].

Po objęciu przywództwa nad Österreichische Volkspartei, ÖVP (Austriacką Partią Ludową), i funkcji kanclerza w 2017 r. Kurz zasugerował masowe zawracanie imigrantów do Afryki i zabezpieczenie południowych granic UE, co spotkało się z ostrą krytyką państw zachodnich i organizacji pozarządowych. W czerwcu tego samego roku powstał 50-stronicowy raport, ale nie przewidywano jego publikacji. Został on sporządzony w celu sprawdzenia, czy obcokrajowcy nie są dyskryminowani w urzędzie zatrudnienia (Arbeitsmarktservice, AMS) i na rynku pracy. Dokument jednak wyciekł do mediów na początku 2018 r. Nie stwierdzono w nim żadnej dyskryminacji obcokrajowców, ale opisano kulturowe i religijne bariery w integracji osób, których językiem ojczystym nie jest język niemiecki. Chodziło szczególnie o Czeczenów i Afgańczyków. Zwrócono uwagę, że pracownicy urzędu pracy bali się sugerować Czeczenom podjęcie zatrudnienia czy wzięcie udziału w kursach edukacyjnych. Czeczeni mieli też zastraszać urzędników AMS. Syryjczycy, Czeczeni i Afgańczycy, zdaniem autorów raportu, mieli problem z podjęciem pracy w takich zawodach, jak opieka społeczna i gastronomia, ponieważ idea obsługiwania innych osób jest przez nich odrzucana. Mężczyźni, ojcowie i mężowie wyznania muzułmańskiego utrudniali również zatrudnienie lub edukację swoich żon i córek. Po opublikowaniu tego raportu poprawne politycznie media domagały się zwolnienia dyrekcji AMS[54]. W połowie 2018 r. kanclerz wydał polecenie wydalenia z kraju kilku imamów, którzy byli finansowani z zagranicy, i zapowiedział zamknięcie siedmiu meczetów. Przedstawił też Komisji Europejskiej rozwiązanie problemu imigrantów, zanim dotrą oni do granic państw UE. Zaproponował utworzenie zamkniętych ośrodków dla imigrantów w Albanii i Kosowie. Tam obcokrajowcy spoza kontynentu byliby sprawdzani i dzieleni na tych, którzy rzeczywiście są uchodźcami oraz na imigrantów ekonomicznych. Ci ostatni byliby deportowani do swoich krajów. Plan Austrii nieoficjalnie poparli przedstawiciele Danii, Holandii i Niemiec[55].

---

[53] B. Wieliński, *Austria zwalcza islamskich agentów zagranicy*, „Gazeta Wyborcza", 26 II 2015 r., https://wyborcza.pl/1,75399,17490678,Austria_zwalcza_islamskich_agentow_zagranicy.html [dostęp: 27 II 2015]; M. Dębski, *Atak spowodowany nienawiścią wobec chrześcijańskich wartości*, „Warszawska Gazeta", 11 XII 2020 r., https://warszawskagazeta.pl/swiat/item/7050-atak-spowodowany-nienawiscia-wobec-chrzescijanskich-wartosci [dostęp: 11 XII 2020].

[54] *Austria: Czeczeni ponadprzeciętnie agresywni*, 20 III 2018 r., https://euroislam.pl/czeczeni-ponadprzecietnie-agresywni-raport-austriackiego-urzedu-pracy-wyciekl-do-mediow/ [dostęp: 20 III 2018].

[55] T. Orszulak, *Austria zamknie siedem meczetów i wydali imamów. Sebastian Kurz idzie na wojnę z islamem*, 8 VI 2018 r., https://wiadomosci.wp.pl/austria-zamknie-siedem-meczetow-i-wydali-imamow-sebastian-kurz-idzie-na-wojne-z-islamem-6260497626355329a [dostęp: 8 VI 2018].

Pozostał on jednak na papierze. Pozbawiono natomiast obywateli tureckich mieszkających w Austrii i Austriaków tureckiego pochodzenia możliwości zdawania egzaminów na prawo jazdy w języku tureckim, co dotychczas było praktykowane. Ma to ich skłonić do nauki języka niemieckiego. Po zamachu w stolicy z 2 listopada 2020 r., w którym zginęły cztery osoby, a 23 zostały ranne, kanclerz Kurz nie kierował się poprawnością polityczną i jednoznacznie stwierdził, że atak był aktem islamskiego terroryzmu spowodowanym nienawiścią wobec podstawowych wartości austriackiego stylu życia i demokracji. Zaznaczył, że nie jest to wojna między Austriakami a imigrantami bądź chrześcijanami a muzułmanami, mimo że od 2018 r. doszło do kilku ataków na kościoły, których dokonali młodzi wyznawcy islamu[56].

W dniu 16 grudnia rząd zaproponował wprowadzenie zmian w prawie, określonym jako „pakiet antyterrorystyczny". Mimo wcześniejszych zapowiedzi jednak zabrakło w nim wyrażonego wprost zakazu funkcjonowania politycznego islamu i zapisów o możliwości przedłużenia więzienia terrorystom po odbyciu przez nich wyroku. Zaproponowano natomiast środki zastępcze w postaci elektronicznego monitoringu osób skazanych za przestępstwa terrorystyczne po opuszczeniu przez nich więzienia. Przepis ma być neutralny religijnie i dotyczyć sprawców wszystkich przestępstw terrorystycznych, bez względu na rodzaj motywacji religijnej czy politycznej. Zaakcentowano, że niezmienne pozostają cele ich walki z islamizmem, a prawo zostało jedynie dostosowane do wymogów konstytucji. Minister ds. integracji Susanne Raab stwierdziła, że ktokolwiek będzie chciał wprowadzić sądy szariackie w Austrii, musi liczyć się z tym, że stanie przed sądem kryminalnym. W Austrii rozpoczęła się debata nad tym, czy w ogóle precyzowanie ekstremizmu religijnego w przepisach jest konieczne. Konstytucjonalista Heinz Mayer przypomniał, że w prawie karnym istnieją przepisy o ruchach wywrotowych, które mogą być stosowane w takich przypadkach. Raab stwierdziła jednak, że „pakiet antyterrorystyczny" w tej formie jest konieczny. Broniła doprecyzowanej regulacji, ponieważ chodzi o (…) *przestępstwo kryminalne, którego celem jest stworzenie nowego, opartego na religii porządku społecznego*[57]. Minister spraw wewnętrznych Karl Nehammer potwierdził konieczność kontynuowania walki z islamizmem, ale wskazał także na potrzebę zwalczania ekstremizmu prawicowego. Zapowiedział zmiany w przepisach dotyczących symboli, które będą się odnosiły również do organizacji skrajnie prawicowych. Zakazane będą symbole zarówno skrajnie prawicowego ruchu identytarystów, jak i Państwa Islamskiego oraz tureckiej Partiya Karkerên Kurdistanê, PKK (Partii Pracujących Kurdystanu), uznawanej za terrorystyczną. Przyspieszenie ścieżki pozbawiania podwójnego obywatelstwa nie zostawia natomiast wątpliwości co do intencji ustawodawców, gdyż prawie w całości będzie dotyczyć muzułmańskich radykałów. Stowarzyszenia i meczety rozpowszechniające skrajne poglądy będą mogły być zamykane w szybkim trybie w razie pojawienia się w nich propagandy terrorystycznej. Raab chce

[56] T. Wójcik, *Mordercy, ISIS i pustosłowie*, „Tygodnik Solidarność" 2020, nr 46.

[57] Zdaniem ekspertów i prawników akt terrorystyczny nie jest „zwykłym" przestępstwem kryminalnym i wymaga szczególnej regulacji prawnej.

też uzyskać informacje o imamach i meczetach. Powstaną ich rejestry ze wskazaniem osób i obiektów, na które należy zwrócić szczególną uwagę. Jeszcze bardziej w stosunku do poprzedniego prawa rząd zacieśni kontrolę nad finansowaniem organizacji religijnych, dzięki czemu uniemożliwi obchodzenie zakazu finansowania ich działalności za pośrednictwem stowarzyszeń i fundacji dobroczynnych. Wprowadzony zostanie również dożywotni zakaz posiadania broni przez osoby skazane za przestępstwo terrorystyczne oraz zakaz pracy w zawodach związanych z ochroną[58]. Dnia 1 stycznia 2021 r. wszedł w życie nakaz zarejestrowania się wszystkich imamów w Austrii w spisie Islamskiej Wspólnoty Religijnej. Jednocześnie austriacka minister ds. UE Karolin Edstadier zaapelowała do UE o pójście za przykładem Wiednia i wprowadzenie obowiązkowej rejestracji wszystkich imamów nauczających na terenie Wspólnoty. Zwróciła również uwagę na konieczność wzmożonej kontroli przydzielania zapomóg organizacjom i instytucjom muzułmańskim, aby pieniądze nie trafiały do stowarzyszeń wspierających radykalny islam[59]. Śledząc zmiany planowane we francuskim i austriackim prawie, władze Szwajcarii noszą się z zamiarem wprowadzenia najbardziej drastycznego prawa antyterrorystycznego na Zachodzie. Miałoby ono również zastosowanie do nieletnich, co naruszałoby Europejską Konwencję Praw Człowieka. Ale rząd Szwajcarii jest zdeterminowany wprowadzić nowe zasady, mimo ostrej krytyki przedstawiciela ONZ ds. Praw Człowieka, który potępił już działania władz za odebranie szwajcarskiego obywatelstwa obywatelowi Syrii na początku 2020 r. Był to pierwszy taki przypadek od II wojny światowej. Gdyby zmian w prawie nie udało się przegłosować w referendum do lutego 2021 r., osoby zradykalizowane i podejrzane o stwarzanie zagrożenia terrorystycznego będą umieszczane bez nakazu sądu w areszcie domowym[60].

W 2017 r. Myndigheten för samhällsskydd och beredskap, MSB (Szwedzka Agencji Ochrony Cywilnej) opublikowała raport pt.: *Muslimska brödraskapet i Sverige* (*Bractwo Muzułmańskie w Szwecji*). Stwierdziła w nim, że organizacje muzułmańskie działające w Szwecji oficjalnie tworzą własne równolegle społeczeństwo i mają powiązania z ruchem Braci Muzułmanów, którzy stanowią wyzwanie dla społecznej spójności kraju. Autor opracowania Magnus Norell, politolog i ekspert ds. terroryzmu, wskazał, że Bracia Muzułmanie nawołują w Szwecji do transformacji w kierunku społeczeństwa islamskiego. Ekspert przekonywał, że szczególnej opiece powinny być poddane dziewczęta. Muzułmanina obowiązują bowiem inne zasady religijne niż pozostałych obywateli. Według raportu Bracia Muzułmanie wywierają wpływ na sztokholmskie oddziały następujących organizacji charytatywnych: Islamic Relief (Muzułmańska Pomoc), Studieförbundet Ibn Rushd (Szwedzki Związek Studentów Ibn Ruszda),

---

[58] J. Wójcik, *Austria przedstawia pakiet antyterrorystyczny*, 17 XII 2020 r., https://euroislam.pl/austria-przedstawia-pakiet-antyterrorystyczny/ [dostęp: 17 XII 2020].

[59] J. Kowalkowska, *Austria chce unijnego rejestru imamów*, „Gazeta Polska Codziennie" z 9 stycznia 2021 r.

[60] L. Bias, *Die Schweiz ist im Begriff, das härteste Antiterror-Gesetz des Westens einzuführen*, 23 XI 2020 r., https://www.swissinfo.ch/ger/-die-schweiz-ist-im-begriff--das-haerteste-anti-terror-gesetz-des-westens-einzufuehren- /46168700 [dostęp: 23 XI 2020].

Islamiska unionen (Związek Islamski) oraz stowarzyszenie Sveriges unga muslimer, SUM (Szwedzcy Młodzi Muzułmanie). W dokumencie podkreślono, że wymienione organizacje otrzymują od państwa miliony koron dotacji. To różnego rodzaju granty przyznawane przez samorządy oraz urzędy centralne na działalność kulturalną, edukacyjną oraz integracyjną. Norell przekonywał, że Bracia Muzułmanie budują wpływy w partiach politycznych, organizacjach pozarządowych, instytucjach akademickich i innych organizacjach społeczeństwa obywatelskiego. Oskarżał też elity polityczne o zmowę milczenia dyktowaną polityczną poprawnością i rzekomą, jego zdaniem, walką z rasizmem i islamofobią. Bracia Muzułmanie mieli wsparcie partii lewicowych oraz Zielonych. W 2016 r. organizacja otrzymała na swoją działalność 1,36 mln koron (142 tys. euro) oraz dodatkowe fundusze na projekt przeciwko rasizmowi. Można dojść do wniosku, że polityczno-religijna działalność Braci Muzułmanów w Europie została wbudowana w model integracji i może być interpretowana jako standardowa praca na rzecz dialogu. Norell podkreślił jednak, że w Szwecji Bracia Muzułmanie mogli przez lata liczyć na wsparcie ze strony części środowisk opowiadających się za wielokulturowością, partii lewicowych oraz Zielonych. Raport stwierdzał, że członkowie SUM wyjeżdżali na front walki w Syrii i brali udział w próbie zamachu na szwedzkiego artystę Larsa Vilksa, twórcę karykatury Mahometa. Organizacja na swoim profilu społecznościowym propaguje również przemoc i nienawiść wobec innych religii[61].

Raport Norella spotkał się z ostrą krytyką ze strony grupy szwedzkich religioznawców. W liście otwartym zarzucili oni autorowi m.in. brak oparcia na faktach oraz jednakowe potraktowanie całej grupy szwedzkich muzułmanów. Anneli Bergholm Söder, przedstawicielka MSB, która zamówiła raport, w oświadczeniu dla mediów stwierdziła, że dokument będzie analizowany, a za jego treść odpowiada autor[62]. Norell miał chyba rację, ponieważ SUM nie otrzymali rządowego subsydium w 2017 r. z uwagi na (…) *brak poszanowania idei demokratycznych*. Myndigheten för ungdoms-och civilsamhällesfrågor, MUCF (Urząd ds. młodzieży oraz społeczeństwa obywatelskiego) nie przyznał im także dotacji w następnym roku. W 2018 r. dotacji pozbawiono także polonijną organizację Kongres Polaków w Szwecji. MUCF ocenił, że działalność Kongresu jest sprzeczna z ideami demokratycznymi. Na poparcie takiego wniosku podano przykłady poglądów wyrażanych na łamach „Gońca Katolickiego", periodyku wydawanego wspólnie ze „Słowem Kongresu". Według szwedzkich urzędników w „Gońcu Katolickim" w latach 2016–2017 publikowano (…) *generalizujące i krzywdzące stwierdzenia na temat muzułmanów, które określają tę grupę jako zagrożenie dla społeczeństwa*. W gazecie padają także opinie, że (…) *należy z islamem walczyć, a nie z nim pertraktować*. W artykułach były używane niewłaściwe określenia,

---

[61] M. Czarnecki, *Skandynawia halal. Islam w krainie białych nocy*, Warszawa 2019, s. 127–129.

[62] *Muzułmańskie organizacje tworzą własne społeczeństwo. Mocny raport Szwedzkiej Agencji Ochrony Cywilnej*, 3 III 2017 r., https://wiadomosci.wp.pl/muzulmanskie-organizacje-tworza-wlasne-spoleczenstwo-mocny-raport-szwedzkiej-agencji-ochrony-cywilnej-6097105667277953a [dostęp: 3 III 2017].

jak: „rasa" i „Murzyn"[63]. W lutym 2021 r. władze Göteborga podjęły decyzję o wstrzymaniu dofinansowania Stowarzyszenia Edukacji Ibn Rushd z powodu związków tej organizacji z radykalnymi ugrupowaniem Milli Görus i Braćmi Muzułmanami[64].

Dwa kolejne lata nieco zmieniły nastawienie do poprawności politycznej lansowanej w Szwecji. Media ujawniły, że na początku 2019 r. ponad 19 proc. całej populacji mieszkającej w tym kraju stanowili imigranci, przy czym większość przybyła tam w ciągu ostatnich 20 lat. Do tego okazało się, że aż 90 proc. marokańskich „nastolatków" ubiegających o azyl w ciągu ostatnich siedmiu lat to pełnoletni mężczyźni. Dopiero w ostatnim czasie politycy zaczynają dostrzegać, że wszelkie założenia dotyczące polityki integracji okazały się utopią. We wrześniu 2020 r. o zagrożeniach ze strony imigrantów otwarcie wypowiedzieli się Mats Loefving, zastępca komendanta szwedzkiej policji, i Edi Mord, komendant policji w Göterborgu. Przekazali oni opinii publicznej informacje, za których ujawnienie jeszcze dwa lata wcześniej zostaliby oskarżeni o rasizm i straciliby pracę. Okazało się, że w Szwecji działa co najmniej 40 rodzinnych gangów pochodzących z krajów muzułmańskich i mających strukturę podobną do klanów przestępczych w Niemczech. Ich członkowie przybyli do Szwecji wyłącznie w celu zorganizowania się i prowadzenia działalności przestępczej. Pieniądze zdobywają głównie z handlu narkotykami oraz podczas napadów i wymuszeń. W latach 2018–2019 w mafijnych porachunkach ginęło ok. 30 mężczyzn rocznie.

W klanach obowiązuje muzułmańska obyczajowość. Ich członkowie odrzucają integrację, nie chcą być częścią szwedzkiego społeczeństwa. Klany przestępcze prezentują zupełnie inną kulturę i trudno je zwalczać przy użyciu typowych procedur policyjnych. Politycy dopiero obecnie zaczęli pracować nad zmianami w prawie, które umożliwiłyby m.in. przesłuchiwanie członków gangów mimo że nie doszło jeszcze do poważnego przestępstwa, a także bez uzyskania zgody prokuratora, która do tej pory była konieczna. Jak dotychczas klany przestępcze doskonale sobie radzą. Sprzyjają im zarówno przepisy prawa, których w Szwecji nie dostosowano do zmieniającej się rzeczywistości, jak i wyjątkowa łagodność szwedzkiego prawa wobec młodocianych przestępców (pozostają oni całkowicie bezkarni). Imigranci w Szwecji nadal korzystają z wielu przywilejów, w tym ze szwedzkiego prawa, które zezwala oskarżonym na wybranie sobie najbardziej dogodnego terminu odbywania kary pozbawienia wolności. Oskarżony opuszcza gmach sądu i ślad po nim ginie, a policja nie ma sił i środków, aby go poszukiwać[65].

---

[63] *Muzułmańska organizacja bez dotacji od szwedzkiego państwa*, 11 IV 2018 r., https://religie.wiara.pl/doc/4633953.Muzulmanska-organizacja-bez-dotacji-od-szwedzkiego-panstwa [dostęp: 11 IV 2018].

[64] *Göteborg wstrzymuje finansowanie islamistów*, https://euroislam.pl/goteborg-wstrzymuje-finansowanie-islamistow/ [dostęp: 25 II 2021].

[65] M. Dębski, *Muzułmański potop w Szwecji*, „Warszawska Gazeta", 20 XI 2020 r., https:// warszawskagazeta.pl/swiat/item/ 7050-muzułmański-potop-w-szwecji [dostęp: 20 XI 2020].

Wnioski

Kryzys imigracyjny silnie wpływa na politykę w Europie i staje się motorem dla ruchów i partii negujących dotychczasowy porządek polityczny, także tych, które nie ukrywają swoich ksenofobicznych haseł i ideologii. Angela Merkel pod hasłami otwartości i wielokulturowości otworzyła granice dla imigrantów, ale tym samym wywołała wzrost ksenofobii, od której UE i Niemcy – jak się wydawało – zdołały się uwolnić. Europa znalazła się w niebezpiecznej sytuacji, w której z jednej strony rosną w siłę ruchy ksenofobiczne, a z drugiej – radykalny islam. Każda z tych formacji legitymizuje swoje istnienie i metody działania istnieniem drugiej, próbuje również doprowadzić do polaryzacji społeczeństwa i stworzenia takiej sytuacji, która wymusi na obywatelach opowiedzenie się po którejś ze stron. Paradoksalnie, decyzja kanclerz Merkel znacznie zwiększyła ryzyko wystąpienia takiego scenariusza, dlatego też niemieckie władze postrzegają zarówno islamski, jak i prawicowy ekstremizm jako stwarzające jednakowe zagrożenie bezpieczeństwa państwa.

Ataki terrorystyczne przeprowadzone w październiku i listopadzie 2020 r. we Francji i Austrii po raz kolejny postawiły UE w stan alarmowy. Tym razem zmieniła się retoryka klasy politycznej i mediów. Po raz pierwszy zamachy powiązano z politycznym islamem, a nie z osobami niedostosowanymi, niezrównoważonymi czy wrogami społeczeństwa i demokracji, co wynikało z poprawności politycznej, która nie pozwalała łączyć terroryzmu z islamem. Jak bardzo istotna okazała się ta zmiana narracji, świadczą antyeuropejskie (szczególnie antyfrancuskie i antyaustriackie) wypowiedzi polityków z państw muzułmańskich, często wulgarne i pełne nienawiści. Prezydent Macron stał się też celem arabskich ulic, ponieważ odważył się wyrazić opinię na temat motywacji zamachowców, a także zapowiedział podjęcie środków, które mają w przyszłości przeciwdziałać eksportowi antyzachodnich idei z państw muzułmańskich do UE. Warto dodać, że sojusznikiem muzułmańskich polityków okazała się telewizja Al-Dżazira. Wyemitowała ona 3-częściowy film pt. *Blood and Tears: French Decolonisation* (*Krew i łzy: francuska dekolonizacja*), w którym próbowano m.in. wytłumaczyć, że podłożem zamachów we Francji jest trauma Algierczyków wyniesiona z czasów wojny narodowowyzwoleńczej, ich dyskryminacja i rasizm Francuzów. Podobne opinie wyrażali także eksperci, m.in. Asma Barlas z Nowego Jorku czy Ludwika Włodek, autorka ostatnio wydanej książki pt. *Gorsze dzieci Republiki. O Algierczykach we Francji*[66], na których wypowiedzi autor artykułu zwrócił uwagę.

Zmiany w prawie i zaostrzenie przepisów mogą okazać się niewystarczające do zmiany sytuacji. Korzystne mogłoby się okazać zredefiniowanie polityki multikulturalizmu, integracji, nie mówiąc już o asymilacji mniejszości muzułmańskich. Jeśli nie

[66] PAP, *Ekspertka o przyczynach islamizacji migrantów we Francji: dżihad, rasizm i dyskryminacja*, 1 XII 2020 r., https://www.pap.pl/aktualnosci/news%2C767547%2Cekspertka-o-przyczynach-islamizacji-migrantow-we-francji-dzihad-rasizm-i [dostęp: 1 XII 2020]; A. Barlas, *On freedom of speech and „Islamist separatism"*, Aljazeera, 11 XI 2020 r., https://www.aljazeera.com/opinions/2020/11/11/on-freedom-of-speech-and-islamist-separatism [dostęp: 11 XI 2020].

można dokonać zmiany wykładni *Koranu* i hadisów oraz gruntownego zreformowania dogmatów islamu, być może należałoby czynić wysiłki na rzecz zmiany świadomości mniejszości muzułmańskich w Europie. Dodatkowo w sposób restrykcyjny można zakreślić obszar norm i wartości, które przy zachowaniu różnej kultury i obyczajowości będą decydowały o przyznaniu prawa pobytu na terenie UE. Demokratyczne społeczeństwo nie może akceptować imigrantów, którzy nie uznają jego podstawowych zasad. Rozwiązaniem może być zmuszenie ich do przyjęcia niektórych norm lub do powrotu do kraju pochodzenia. Harmonijne współżycie mniejszości i społeczeństw przyjmujących jest uzależnione od rozsądnych decyzji politycznych i długofalowych, konsekwentnych działań. Nie mogą one być podporządkowane partyjnej ideologii i bieżącym korzyściom politycznym, tzn. proimigracyjnej polityce lewicy i antyimigracyjnej polityce prawicy. Decydującym warunkiem powinno być akceptowanie przez przybyszów europejskich praw, norm i wartości oraz zdolność do integracji. Ważne jest, aby UE jako całość, a nie poszczególne jej kraje, była gotowa stawić czoła temu problemowi.

Pokładanie nadziei w edukacji imamów przebywających w państwach Europy jako sposobie na rozwiązanie problemu radykalizacji muzułmanów jest, zdaniem autora, zbyt optymistyczne. Już w 2011 r. powstało pierwsze Centrum Teologii Islamskiej na Uniwersytecie w Tybindze, a rok później w Osnabrück i Frankfurcie. Okazało się, że studia zostały zdominowane przez kobiety, a wielu mężczyzn mających dyplomy ukończenia 5-letnich studiów nie zamierzało podejmować pracy w meczetach. Imamami zostało zaledwie kilku muzułmańskich teologów wykształconych w Niemczech[67]. Błędne jest też założenie, że kaznodzieje będą wygłaszali kazania w którymś z języków europejskich, a imamowie w tym samym języku będą prowadzić modlitwy. Jest to po prostu niezgodne z islamem. Mniej kosztowne i bardziej racjonalne będzie ścisłe monitorowanie duchownych przybyłych do Europy z krajów muzułmańskich, a przede wszystkim ich opiniowanie przez służby konsularne i sprawdzenie przez służby specjalne przed wydaniem wizy. Otrzymanie wizy pracowniczej powinno być obowiązkowe dla zagranicznych duchownych muzułmańskiego pochodzenia, którzy zamierzają podjąć działalność w UE. Ważność wizy można ograniczyć do roku lub dwóch lat, z możliwością jej przedłużenia, a nie – jak w Niemczech gdzie jest ona ważna minimum pięć lat.

Można mieć nadzieję, że władze Francji będą na tyle zdeterminowane, aby zrealizować wszystkie zapowiedziane działania wymierzone w islamskich radykałów. Relacje między rządem i organizacjami muzułmańskimi działającymi w tym kraju dawno nie były tak napięte, jak obecnie. Z trudem udaje się skłonić te organizacje do jakiejkolwiek współpracy. Jak do tej pory CFCM nie zaakceptowała *Karty wolności obywatelskich*, choć miała na to 15 dni, i nie wiadomo, czy to w ogóle nastąpi. Coraz bardziej wątpliwe wydaje się również utworzenie CNI. Mogą zatem upaść sztandarowe projekty prezydenta Macrona z przywróceniem państwu „separatystycznych" dzielnic na obrzeżach

[67] S. Ripperger, M. Matzke, *Pierwsze centrum kształcenia imamów w Niemczech*, 10 X 2011 r., https://www.dw.com/pl/pierwsze-centrum-kształcenia-imamów-w-niemczech/a-15449531 [dostęp: 10 X 2011].

wielkich miast. Lata zaniechań, uległości, przyjmowanie kolejnych rzesz imigrantów, mimo fiaska polityki integracji, doprowadziły do chaosu. Wystarczy tylko iskra, aby doszło do otwartego buntu przeciw władzom.

Czy zasadne jest więc poszukiwanie porozumienia z ruchem Braci Muzułmanów? To ugrupowanie głęboko zakorzeniło się w wielu państwach Europy i zaadaptowało do naszych warunków kulturowych. Wykazuje ono szczególną dbałość o zachowanie pozorów przy budowaniu poprawnego wizerunku jako organizacji będącej w dobrych relacjach z władzami, w prowadzeniu dialogu społecznego i w prezentowaniu się jako ruch zintegrowany z europejskim społeczeństwem. Tymczasem powoli, ale systematycznie i z uporem buduje swoje wpływy w instytucjach i wspólnotach muzułmańskich oraz władzach lokalnych. Od lat kontroluje wiele stowarzyszeń i centrów islamu.

Odpowiadając zatem na pytanie postawione na wstępie, czy działania podejmowane przez władze mogłyby odnieść pożądany skutek i przyczynić się do uspokojenia nastrojów społecznych, autor twierdzi, że tylko chwilowo. Projekty wymierzone w tzw. polityczny islam tworzone ostatnio przez władze „starych" państw UE mają charakter doraźny i wymiar propagandowy. Bez zmiany mentalności tych mniejszości muzułmańskich, które są nastawione negatywnie do Europy, wszelkie inicjatywy na rzecz integracji są skazane na porażkę. W niedalekiej perspektywie napięcia społeczne prawdopodobnie wybuchną ze zdwojoną siłą.

Bibliografia

Balicki J., *Imigranci z krajów muzułmańskich w Unii Europejskiej. Wyzwania dla polityki integracyjnej*, Warszawa 2010, Wydawnictwo Uniwersytetu Kardynała Stefana Wyszyńskiego.

Czarnecki M., *Skandynawia halal. Islam w krainie białych nocy*, Warszawa 2019, Agora.

Dobosz B., *Emiraty francuskie*, Warszawa 2016, 3S Media.

Dobosz B., *Islamski terroryzm przestaje być tabu*, „Najwyższy Czas" 2020, nr 50–51.

Izak K., *Dokumenty, tożsamość, służby i politycy*, „Człowiek i Dokumenty" 2017, nr 46, s. 52–64.

Izak K., *Ograniczenia i problemy w zwalczaniu terroryzmu i przestępczości imigrantów w Europie*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 104–137.

Jendroszczyk P., *Rosnący lęk przed skrajną prawicą*, „Rzeczpospolita" z 26 listopada 2020 r.

Keppel G., *Święta wojna. Ekspansja i upadek fundamentalizmu muzułmańskiego*, Warszawa 2003, Dialog.

Keppel G., Jardin A., *Terror we Francji. Geneza francuskiego dżihadu*, Warszawa 2017, Dialog.

Kowalkowska J., *Austria chce unijnego rejestru imamów*, „Gazeta Polska Codziennie" z 9 stycznia 2021 r.

Kowalkowska J., *Macron tworzy muzułmańską kurię*, „Gazeta Polska Codziennie" z 23 listopada 2020 r.

Kryszak P., *Narasta konflikt Francji z Turcją*, „Gazeta Polska Codziennie" z 26 października 2010 r.

Kubera J., *Francuzi, Algierczycy? Relacje między identyfikacjami Francuzów algierskiego pochodzenia*, Toruń 2017, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

Madajczyk P., *Między fundamentalizmem a asymilacją. Muzułmanie w Niemczech*, Warszawa 2015, Instytut Studiów Politycznych Polskiej Akademii Nauk.

Murray D., *Przedziwna śmierć Europy. Imigracja. Tożsamość. Islam*, Poznań 2017, Zysk i S-ka Wydawnictwo.

Orzechowski M., *Mój sąsiad islamista. Tunis–Paryż–Bruksela…*, wyd. 2 zaktualizowane, Warszawa 2016, MUZA SA.

Pamuła A., *Wrzenie. Francja na krawędzi*, Warszawa 2020, Wydawnictwo Agora.

Petrović P., *Francja walczy z islamskim separatyzmem*, „Gazeta Polska Codziennie" z 7 października 2020 r.

Phillips M., *Londonistan. Jak Wielka Brytania stworzyła państwo terroru*, Warszawa 2010, Sprawy Polityczne.

Rusinek A., *Nurt radykalny wśród społeczności muzułmańskich w wybranych państwach Unii Europejskiej*, Warszawa 2012, Wydawnictwa Uniwersytetu Warszawskiego.

Ulfkotte U., *Niemcy jako Mekka. Cicha islamizacja Europy*, Wrocław 2019, Wektory.

Widy M., *Życie codzienne w muzułmańskim Paryżu*, Warszawa 2005, Wydawnictwo Akademickie Dialog.

Wilk-Jakubowski G., *Sytuacja społeczna muzułmanów w Wielkiej Brytanii*, Kraków 2013, Zakład Wydawniczy Nomos.

Wójcik T., *Mordercy, ISIS i pustosłowie*, „Tygodnik Solidarność" 2020, nr 46.

Źródła internetowe

AEW, *Jak Turcja kontroluje islam w Niemczech*, https://euroislam.pl/jak-turcja-kontroluje-islam-w-niemczech/ [dostęp: 27 IV 2016].

Austria: Czeczeni ponadprzeciętnie agresywni, 20 III 2018 r., https://euroislam.pl/czeczeni-ponadprzecietnie-agresywni-raport-austriackiego-urzedu-pracy-wyciekl-do-mediow/ [dostęp: 20 III 2018].

Barlas A., *On freedom of speech and „Islamist separatism"*, Aljazeera, 11 XI 2020 r., https://www.aljazeera.com/opinions/2020/11/11/on-freedom-of-speech-and-islamist-separatism [dostęp: 11 XI 2020].

Bault O., *Francuska dziwna wojna z islamizmem*, „Do Rzeczy", 29 X 2020 r., https://dorzeczy.pl/swiat/158991/francuska-dziwna-wojna-z-islamizmem.html [dostęp: 29 X 2020].

Bias L., *Die Schweiz ist im Begriff, das härteste Antiterror-Gesetz des Westens einzuführen*, 23 XI 2020 r., https://www.swissinfo.ch/ger/-die-schweiz-ist-im-begriff--das-haerteste-anti-terror-gesetz-des-westens-einzufuehren- /46168700 [dostęp: 23 XI 2020].

Bielecki J., *Emmanuel Macron* w końcu wypowiada wojnę islamistom, „Rzeczpospolita" z 20 października 2020 r., https://www.rp.pl/Polityka/201029902-Emmanuel-Macron--w-koncu-wypowiada-wojne-islamistom.html [dostęp: 22 X 2020].

Bielecki J., *Nie przyjaźnię się z żadnym muzułmaninem*, https://www.rp.pl/artykul/1171826-Nie--przyjaznie-sie-z-zadnym-muzulmaninem.html [dostęp: 16 I 2015].

Dębski M., *Atak spowodowany nienawiścią wobec chrześcijańskich wartości*, „Warszawska Gazeta", 11 XII 2020 r., https://warszawskagazeta.pl/swiat/item/7050-atak-spowodowany-nienawiscia-wobec-chrzescijanskich-wartosci [dostęp: 11 XII 2020].

Dębski M., *Muzułmański potop w Szwecji*, „Warszawska Gazeta", 20 XI 2020 r., https://warszawskagazeta.pl/swiat/item/7050-muzułmański-potop-w-szwecji [dostęp: 20 XI 2020].

Dobosz B., *Francja marnotrawi setki milionów euro na asymilację muzułmanów. Przywłaszczenia to codzienność*, 13 VII 2017 r., http://www.pch24.pl/francja-marnotrawi-setki-milionow-euro-na-asymilacje-muzulmanow-przywlaszczenia-to-codziennosc,53044,i.html [dostęp: 13 XII 2017].

Dworak A., *Ulica należy do klanu. Arabscy gangsterzy opanowali miasta Niemiec*, „Polska Times", 1 II 2019 r., https://polskatimes.pl/ulica-nalezy-do-klanu-arabscy-gangsterzy--opanowali-miasta-niemiec/ar/c1-13853448 [dostęp: 1 II 2019].

Drymer G., *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów*, „Rzeczpospolita", 30 IX 2017 r., https://www.rp.pl/Spoleczenstwo/309289949-Afery-seksualne-w-Wielkiej-Brytanii-Gwalty-muzulmanskich-gangow.html [dostęp: 1 X 2017].

Francja zamyka granice. Stan wyjątkowy w całym kraju, TVN24, 14 XI 2015 r., https://tvn24.pl/swiat/francja-zamyka-granice-i-wprowadza-stan-wyjatkowy-ra594403-3318007 [dostęp: 14 XI 2015].

Francuska Rada Kultu Muzułmańskiego akceptuje zasady Macrona, https://euroislam.pl/rada--muzulmanow-akceptuje-zasady-macrona/ [dostęp: 18 I 2021].

Göteborg wstrzymuje finansowanie islamistów, https://euroislam.pl/goteborg-wstrzymuje--finansowanie-islamistow/ [dostęp: 25 II 2021].

Górzyński O., *Macron robi „porządek" z migrantami. Le Pen triumfuje*, 27 XII 2017 r., https://wiadomosci.wp.pl/macron-robi-porzadek-z-migrantami-le-pen-triumfuje--6202896011315329a [dostęp: 27 XII 2017].

Gromkowska-Melosik A., *Mniejszość muzułmańska w Szwecji: między ekstremistycznym izolacjonizmem a procesami reprodukcji ekonomicznej*, „Studia Edukacyjne" 2013, nr 26, www.repozytorium.amu.edu.pl.

https://religie.wiara.pl/doc/6553063.Macron-Nowe-prawo-i-ostrzejsze-zasady-wobec-separatyzmu [dostęp: 3 X 2020].

https://en.wikipedia.org/wiki/Collective_Against_Islamophobia_in_France [dostęp: 20 XII 2020].

Kowalkowska J., *Macron tworzy muzułmańską kurię*, „Gazeta Polska Codziennie" z 23 listopada 2020 r., https://www.leparisien.fr/politique/le-cfcm-promet-a-macron-une-charte-des--valeurs-republicaines-dans-les-15-jours-18-11-2020-8409157.php [dostęp: 20 XI 2020].

La grande Mosquée de Paris annonce son retrait du projet de Conseil national des imams, 29 XII 2020 r., https://www.lci.fr/societe/la-grande-mosquee-de-paris-annonce-son-retrait-du--projet-de-conseil-national-des-imams-2174082.html [dostęp: 30 XII 2020].

Lindenberg G., *Najwięcej ekstremistów we francuskich więzieniach*, 4 X 2020 r., https://euroislam.pl/najwiecej-ekstremistow-we-francuskich-wiezieniach/ [dostęp: 4 X 2020].

Media w USA ostro o przejęciu „Zaman": „Zamach Erdogana na prasę", 8 III 2016 r., https://wiadomosci.wp.pl/media-w-usa-ostro-o-przejeciu-zaman-zamach-erdogana-na-prase--6027417304052353a [dostęp: 19 VII 2016].

Muller J., *„Kryzys na niespotykaną skalę". Burmistrzowie 7 miast Francji przeciw fali imigrantów*, 19 XII 2017 r., https://www.o2.pl/artykul/kryzys-na-niespotykana-skale-burmistrzowie--miast-francji-przeciw-fali-imigrantow 6200161017976449a [dostęp: 19 XII 2017].

Muzułmańska organizacja bez dotacji od szwedzkiego państwa, 11 IV 2018 r., https://religie.wiara.pl/doc/4633953.Muzulmanska-organizacja-bez-dotacji-odszwedzkiego-panstwa [dostęp: 11 IV 2018].

Muzułmańskie organizacje tworzą własne społeczeństwo. Mocny raport Szwedzkiej Agencji Ochrony Cywilnej, 3 III 2017 r., https://wiadomosci.wp.pl/muzulmanskie-organizacje--tworza-wlasne-spoleczenstwo-mocny-raport-szwedzkiej-agencji-ochrony-cywilnej--6097105667277953a [dostęp: 3 III 2017].

Niemcy: imamowie będą musieli udowodnić, że znają niemiecki, 7 XI 2019 r., https://www.dw.com/pl/niemcy-imamowie-będą-musieli-uwodnić-że-znają-niemiecki/a-51148977 [dostęp: 7 XI 2019].

Orszulak T., *Austria zamknie siedem meczetów i wydali imamów. Sebastian Kurz idzie na wojnę z islamem*, 8 VI 2018 r., https://wiadomosci.wp.pl/austria-zamknie-siedem-meczetow-i-wydali-imamow-sebastian-kurz-idzie-na-wojne-z-islamem-6260497626355329a [dostęp: 8 VI 2018].

PAP, *Ekspertka o przyczynach islamizacji migrantów we Francji: dżihad, rasizm i dyskryminacja*, 1 XII 2020 r., https://www.pap.pl/aktualnosci/news%2C767547%2Cekspertka-o-przyczynach-islamizacji-migrantow-we-francji-dzihad-rasizm-i [dostęp: 1 XII 2020].

Ripperger S., Matzke M., *Pierwsze centrum kształcenia imamów w Niemczech*, 10 X 2011 r., https://www.dw.com/pl/pierwsze-centrum-kształcenia-imamów-w-niemczech/a-15449531 [dostęp: 10 X 2011].

„Séparatismes": un projet de loi „pas contre les religions", selon Jean Castex, https://www.france24.com/fr/france/20201209-séparatismes-le-gouvernement-présente-son-projet-de-loi-contre-l-islamisme-radical [dostęp: 9 XII 2020].

Sulkowski M., *Polityczne konsekwencje kryzysu imigracyjnego w Niemczech*, „Chrześcijaństwo-Świat-Polityka. Zeszyty Społecznej Myśli Kościoła" 2016 r, s. 59–72.

Ślusarczyk P., *Prezydent Francji zapowiada walkę z islamskim separatyzmem*, 5 X 2020 r., https://euroislam.pl/prezydent-francji-zapowiada-walke-z-islamskim-separatyzmem/ [dostęp: 5 X 2020].

Wieliński B., *Austria zwalcza islamskich agentów zagranicy*, „Gazeta Wyborcza", 26 II 2015 r., https://wyborcza.pl/1,75399,17490678,Austria_zwalcza_islamskich_agentow_zagranicy.html [dostęp: 27 II 2015].

Wójcik J., *Austria przedstawia pakiet antyterrorystyczny*, 17 XII 2020 r., https://euroislam.pl/austria-przedstawia-pakiet-antyterrorystyczny/ [dostęp: 17 XII 2020].

Wójcik J., *Niemieccy Zieloni: „Islamizm jest zagrożeniem"*, https://euroislam.pl/niemieccy-zieloni-islamizm-jest-zagrozeniem/ [dostęp: 18 XI 2020].

Abstrakt

Kryzys imigracyjny w 2015 r. stał się motorem dla ruchów i partii negujących dotychczasowy porządek polityczny, także tych, które nie ukrywają swoich ksenofobicznych haseł i idei. Z perspektywy czasu jest coraz więcej oznak, że decyzja o niekontrolowanym przyjęciu uchodźców była bardziej wyrazem myślenia życzeniowego niż racjonalnym rozstrzygnięciem uwzględniającym rzeczywistą sytuację polityczną. Tym samym Europa znalazła się w niebezpiecznej sytuacji, kiedy to z jednej strony rosną w siłę ruchy skrajnie prawicowe, a z drugiej – radykalny islam. Każda z tych formacji legitymizuje swoje istnienie i metody działania istnieniem drugiej strony, a także

próbuje doprowadzić do polaryzacji społeczeństwa i stworzenia takiej sytuacji, która niejako wymusi na obywatelach opowiedzenie się po stronie którejś z tych formacji. Paradoksalnie, decyzja kanclerz Merkel znacznie zwiększyła ryzyko wystąpienia takiego scenariusza, dlatego też niemieckie władze postrzegają i islamski, i prawicowy ekstremizm jako stwarzające jednakowe zagrożenie bezpieczeństwa państwa. Jednak dopiero ostatnie zamachy terrorystyczne w październiku i listopadzie 2020 r. we Francji i Niemczech przyczyniły się do zmiany politycznej narracji.

Słowa kluczowe: imigracja, integracja, islam, politycy, poprawność polityczna, radykalizm, wielokulturowość.

Changes in the perception of immigration, integration, multiculturalism and threats of Islamic radicalism in certain EU member states

Abstract

The 2015 immigration crisis became a driving force for movements and parties that negate the current political order, including those that do not conceal their xenophobic slogans and ideas. In retrospect, there are more and more signs that the decision to accept the uncontrolled refugee influx was more an expression of wishful thinking than a rational decision, taking into account the actual political situation. Thus, Europe finds itself in a dangerous situation with far-right movements on the one hand, and radical Islam on the other. Each of these formations legitimizes its existence and methods of operation by the existence of the other side, trying to polarize society and create a situation that will somehow force citizens to opt for one of the two options. Paradoxically, Chancellor Merkel's decision significantly increased the risk of such a scenario, hence the perception of Islamic and right-wing extremism by the German authorities as posing an equal threat to state security. However, it was only the recent terrorist attacks in October and November 2020 in France and Germany that changed the political narrative.

Keywords: immigration, integration, Islam, politicians, political correctness, radicalism, multiculturalism.

MAŁGORZATA KUDZIN-BORKOWSKA
ORCID: 0000-0002-5816-3676

DOI: 10.4467/20801335PBW.21.009.13566

Cyberbezpieczeństwo w Grupie Wyszehradzkiej – koncepcje i strategie

Impulsem do podjęcia rozważań dotyczących problematyki cyberbezpieczeństwa w Grupie Wyszehradzkiej (dalej: Grupa V4), która od początku swojego istnienia jest postrzegana jako najbardziej dynamiczne ugrupowanie w Europie Środkowej, jest okrągła, trzydziesta rocznica jej utworzenia, przypadająca w 2021 r. Bezpieczeństwo cybernetyczne we wszystkich czterech państwach członkowskich tej Grupy stanowi ważny element działań politycznych, militarnych, społecznych i gospodarczych. Upowszechnianie się cybertechnologii spowodowało konieczność wprowadzenia zmian w prawie oraz zarządzaniu bezpieczeństwem teleinformatycznym, zwłaszcza w pierwszej dekadzie XXI w. Praca ma charakter przyczynkarski i jest próbą uwypuklenia wybranych zagadnień dotyczących koncepcji cyberbezpieczeństwa i cyberstrategii w poszczególnych państwach członkowskich Grupy V4. Najważniejszym celem autorki było scharakteryzowanie definicji i podstawowych pojęć związanych z cyberbezpieczeństwem oraz przybliżenie różnic i podobieństw w postrzeganiu tego zagadnienia w wybranych dokumentach strategicznych.

W naukach o bezpieczeństwie można znaleźć wiele terminów dotyczących bezpieczeństwa informacyjnego, jednak w ostatnich latach w dokumentach strategicznych oraz w ustawach dominuje kategoria pojęciowa cyberbezpieczeństwo (*cybersecurity*[1]). Celem badań przeprowadzonych w ramach niniejszej pracy jest przeanalizowanie inicjatyw w zakresie cyberbezpieczeństwa podejmowanych w Grupie V4 oraz przedstawienie głównych działań realizowanych w tym zakresie przez Unię Europejską i Organizację Traktatu Północnoatlantyckiego (dalej: NATO). Z wykorzystaniem

[1] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje za każdym razem tej informacji. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski (przyp. red.).

metody *desk research*[2] oraz krytycznego przeglądu literatury autorka podjęła próbę refleksji teoretyczno-metodologicznej nad siatką pojęciową stosowaną w nauce oraz w dokumentach strategicznych, aby określić skończony zbiór pojęć synonimicznych oraz bliskoznacznych pojęciu „cyberbezpieczeństwo". Dokonała analizy treści i analizy porównawczej dokumentów strategicznych państw członkowskich Grupy V4. Kwestie dotyczące cyberbezpieczeństwa wymagają rozwiązań nie tylko wewnątrzkrajowych, lecz także międzynarodowych. Z tego względu celem autorki jest poszukanie odpowiedzi na następujące pytania: czy istnieje współpraca państw Grupy V4 w tym zakresie, czy występują zasadnicze różnice w dokumentach strategicznych dotyczących cyberbezpieczeństwa przygotowanych przez poszczególne państwa członkowskie oraz czy w tych dokumentach jest deklarowana współpraca w ramach Grupy V4? Autorka zakłada, że konceptualizacje cyberbezpieczeństwa w dokumentach strategicznych poszczególnych państw Grupy V4 istotnie różnią się od siebie, nie można zatem mówić o wspólnej i spójnej polityce cyberbezpieczeństwa tej Grupy.

Od drugiej połowy XX w. podstawowym czynnikiem rozwoju cywilizacji są procesy zarządzania informacją, a więc jej wytwarzania, przechowywania, wyszukiwania, przekształcania i przesyłania[3]. Gigantyczny przepływ informacji i ciągły rozwój technologii cyfrowych wydają się nie mieć żadnych ograniczeń i stanowią o istocie współczesnej techniki, gospodarki czy wojskowości. Tak jak w przypadku innych obszarów życia społecznego i gospodarczego oraz aktywności ludzkiej również w sferze zarządzania informacją pojawiają się rozmaite zagrożenia, którym trzeba przeciwdziałać, aby zapewnić bezpieczeństwo komunikowania i korzystania z informacji[4].

Wyróżnia się kilka kategorii pojęciowych odnoszących się do różnych obszarów i zagadnień z zakresu bezpieczeństwa, które są wykorzystywane w dziedzinie zarządzania informacją. Najbardziej ogólną jest bezpieczeństwo informacyjne (*information security, information safety*)[5], przez które najczęściej rozumie się ochronę informacji przed niepożądanym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania, a podejmowane środki bezpieczeństwa mają zapewnić poufność, integralność oraz dostępność informacji[6]. Pojęcie bezpieczeństwo

---

[2] Metoda badawcza polegająca na kompilacji, analizowaniu oraz przetwarzaniu danych i informacji pochodzących z istniejących źródeł, a następnie formułowaniu na ich podstawie wniosków dotyczących badanego problemu. Za: Encyklopedia Zarządzania, mfiles.pl/index.php/Desk_research [dostęp: 26 I 2021] – przyp. red.

[3] R. Borkowski, *Cywilizacja, technika, ekologia. Wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku*, Kraków 2001, s. 64.

[4] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012.

[5] Oba terminy funkcjonują w języku angielskim i są zamiennie stosowane przez anglosaskich autorów i ekspertów.

[6] Zob. K. Liedel, *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, s. 45–62; tenże, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2014; J. Jańczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013; O. Strnád, *Riadenie rizík informačnej bezpečnosti*, Ostrava 2010.

informacji (*security of information*) wiąże się z kolei z zagadnieniami ochrony informacji niejawnych, tajemnicy państwowej, tajemnicy biznesowej oraz zagrożeniami wywiadu wojskowego,politycznego i przemysłowego[7]. Trzy kolejne kategorie pojęciowe stosowane w literaturze przedmiotu są ze sobą ściśle powiązane i w dużej mierze dotyczą zagadnień z zakresu technologii informatycznych, technicznych zabezpieczeń i ochrony przestrzeni przetwarzania informacji oraz interakcji zachodzących w sieciach teleinformatycznych. Rozumienie pojęcia bezpieczeństwo informatyczne najczęściej jest zawężane do oprogramowania służącego do zapewnienia bezpieczeństwa, w tym rozwiązań antywirusowych, zapór sieciowych (*firewalls*) oraz systemów wykrywania włamań (*intrusion detection system*, IDS), a także do przestrzegania przez użytkowników odpowiednich procedur bezpieczeństwa podczas korzystania z oprogramowania[8]. Z kolei o bezpieczeństwie systemów informatycznych (komputerowych) mówi się, mając na myśli m.in. eliminację błędów już na etapie projektowania i tworzenia oprogramowania oraz w fazie testowania urządzeń[9]. Przez bezpieczeństwo teleinformatyczne i teleinformacyjne, a także przez bezpieczeństwo Internetu rozumie się natomiast zbiór zagadnień z zakresu telekomunikacji i informatyki koncentrujących się na analizie ryzyka i kontrolowaniu zagrożeń związanych z korzystaniem z komputerów, sieci komputerowych oraz urządzeń przesyłowych[10]. Ogromnego znaczenia nabrała w ostatnim czasie inżynieria ochrony danych, którą Krzysztof Liderman definiuje jako metodykę i narzędzia stosowane podczas projektowania i wdrażania mechanizmów ochrony danych[11].

Wiele pojęć, pomimo ich używania w dokumentach państwowych oraz w wojskowości, ma, jak podkreśla Cezary Banasiński, charakter nieostry i zgoła nienaukowy, a ich definicje pojawiły się w literaturze pięknej[12]. Do takich pojęć należą: rzeczywistość wirtualna (*virtual reality*), cyberprzestrzeń (*cyberspace*) oraz wspomniane już „cyberbezpieczeństwo". To ostatnie pojęcie jest obecnie stosowane najczęściej, o czym już nadmieniono, i wypiera z dyskursu publicznego inne kategorie pojęciowe[13]. Przez „cyberprzestrzeń" rozumie się najczęściej globalną infrastrukturę

---

7 *Ochrona informacji niejawnych w XXI wieku*, S. Topolewski (red.), Siedlce 2016, s. 5.

8 Zob. K. Liderman, *Bezpieczeństwo informacyjne – nowe wyzwania*, Warszawa 2017, s. 152–153, 160–161; tenże, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009; R. Pręgiel, P. Buchwald, *Internet w społeczeństwie informacyjnym – nowoczesne systemy informatyczne i ich bezpieczeństwo*, Dąbrowa Górnicza 2014.

9 J. Jaźwiński, K. Ważyńska-Fiok, *Bezpieczeństwo systemów*, Warszawa 1993.

10 *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009.

11 K. Liderman, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003, s. 9.

12 *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018, s. 23–27.

13 Zob. M. Lakomy, *Dylematy polityki cyberbezpieczeństwa Polski*, w: *Dylematy polityki bezpieczeństwa Polski na początku drugiej dekady XXI wieku*, K. Czornik, M. Lakomy (red.), Katowice 2014, s. 425–454; J.L. Bayuk i in., *Cyber Security Policy Guidebook*, Hoboken 2012; K. Liedel, *Cyberbezpieczeństwo – wyzwania przyszłości. Działania społeczności międzynarodowej*, w: *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2011, s. 437–448.

informacyjną, a więc przestrzeń komunikacyjną tworzoną przez system powiązań internetowych albo też wszechogarniającą świat domenę informacyjną, w której nośnikiem danych jest spektrum elektromagnetyczne[14]. Posługując się kategorią pojęciową „rzeczywistość wirtualna", można zdefiniować „cyberprzestrzeń" jako wirtualne środowisko mniej lub bardziej otwartego komunikowania się za pośrednictwem połączonych systemów komputerowych oraz powiązań informacyjnych i informatycznych[15].

Badacze internetu oraz społeczeństwa informacyjnego, jak Sherry Turkle czy Clay Shirky, głoszą pogląd, że globalna sieć nie jest już tylko produktem rozwoju technologii i jednym z elementów cywilizacji naukowo-technicznej, lecz sama stała się istotą cywilizacji. Jest bowiem zbiorem narzędzi, zasobów i praktyk kulturowych organizujących życie współczesnego człowieka, zarówno w wymiarze rzeczywistości materialnej, jak i symbolicznej. Próba wyobrażenia sobie świata bez internetu jest *de facto* wyobrażeniem świata bez cywilizacji i stanowi często kanwę powieści oraz obrazów filmowych o charakterze postapokaliptycznym[16]. Zagrożenia w cyberprzestrzeni i ochrona przed nimi stały się istotnym problemem współczesnego świata, w którym wciąż postępują cyfryzacja różnych dziedzin życia oraz rozwój technologii ICT (*information and communication technologies*). Zdaniem wielu badaczy problematyki, podzielanym przez Cezarego Banasińskiego, cyberbezpieczeństwo jest zagadnieniem charakteryzującym się złożonością, interdyscyplinarnością oraz multidyscyplinarnością, łączącym obszary badawcze z zakresu informatyki, socjologii internetu, psychologii i zarządzania. Dlatego jego badanie mieści się w obszarze securitologii, będącej nauką transdycyplinarną[17].

Warto zwrócić uwagę, że przedrostek „cyber-" pochodzi od słowa „cybernetyczny", a cybernetyka to nauka o sterowaniu, organizacji i zarządzaniu, a w mniejszym stopniu – o przetwarzaniu informacji[18]. Stąd też kategoria pojęciowa „cyberbezpieczeństwo" odnosiłaby się raczej do bezpieczeństwa sterowania, co w przypadku bezpieczeństwa informacji oznaczałoby sterowanie procesami przepływu informacji. Pojęcie informacja pochodzi od łacińskiego słowa *informatio* oznaczającego 'wizerunek', 'obraz', 'pojęcie oraz od czasownika *informo* oznaczającego 'wyobrażać', 'tworzyć' lub 'kształtować'. Pomimo wątpliwości semantycznych przedrostek „cyber-" upowszechnił się w mass mediach w odniesieniu do zagadnień związanych z technologiami informatycznymi i, jak podkreśla Tomasz Pączkowski, obecnie pod pojęciem cyberzagrożenia

[14] *Cyberbezpieczeństwo*…, s. 24–25.

[15] Tamże.

[16] Zob. E. Bendyk, P. Rutkowski, *Poranek bez sieci*, „Polityka" 2019, nr 16, s. 44–46; S. Turkle, *Life on the Screen: Identity in the Age of Internet*, New York 2011; C. Shirky, *Here Comes Everybody: The Power of Organizing without Organizations*, New York–London 2009; B. Snow, *What Would a World Without Internet Look Like? A thought experiment*, „The Atlantic", 5 IV 2016 r., www.theatlantic.com/technology/archive/2016/04/a-world-without-internet/476907/ [dostęp: 18 II 2021].

[17] Zob. *Cyberbezpieczeństwo*…, s. 37; L.F. Korzeniowski, *Securitologia: nauka o bezpieczeństwie człowieka i organizacji społecznych*, Chorzów 2009.

[18] Zob. *Słownik pojęć współczesnych*, A. Bullock i in. (red.), Katowice 1999; J. Kossecki, *Cybernetyka społeczna*, Warszawa 1981, s. 10.

rozumie się wszelkie niebezpieczeństwa związane z korzystaniem z internetu[19]. Można zatem uznać, że używanie określenia *cybersecurity* jest przejawem mody językowej i wynika z powszechnej dominacji terminologii anglojęzycznej. W wojskowości stosuje się pojęcia: cyberaktywność militarna, cyberoperacja militarna, cyberatak, cyberwojna i cyberobrona. Wprowadzono również pojęcie cyberterroryzm na określenie nowego rodzaju terroryzmu. Z kolei w medioznawstwie mówi się o cyberkomunikowaniu. Notabene pojęcia cyberprzestrzeń oraz rzeczywistość wirtualna pojawiły się w literaturze *science fiction* w 1984 r., a ich twórcą był William Gibson[20]. Kategoria „cyberbezpieczeństwo" nie jest więc synonimem pojęć „bezpieczeństwo informacyjne" i bezpieczeństwo cyfrowe (*digital security*), można natomiast przyjąć, że jest tożsama z pojęciem bezpieczeństwo komunikowania w cyberprzestrzeni. W literaturze pojawia się także pojęcie e-bezpieczeństwo (*e-safety*), tj. bezpieczeństwo elektroniczne[21].

W dokumencie *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, opublikowanym 7 lutego 2013 r., stwierdza się, że bezpieczeństwo cybernetyczne odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci oraz tę infrastrukturę uszkodzić. Z kolei przez pojęcie polityka bezpieczeństwa informacji (*information security policy*) należy rozumieć zbiór reguł i procedur, zgodnie z którymi państwo, siły zbrojne, służby lub korporacje tworzą i udostępniają zasoby informacyjne i zarządzają nimi oraz określają, które zasoby i w jaki sposób mają być chronione.

Z kolei w dokumentach strategicznych NATO używa się pojęć cyberobrona i zapewnianie bezpieczeństwa w cyberprzestrzeni, nie definiuje się natomiast samej kategorii „cyberbezpieczeństwo". W amerykańskich koncepcjach dotyczących bezpieczeństwa narodowego przyjęto zwięzłą definicję cyberbezpieczeństwa jako możliwość ochrony lub obrony cyberprzestrzeni przed cyberatakami[22]. W koncepcji strategicznej NATO obowiązującej na lata 2010–2020, uzgodnionej w Lizbonie 17 listopada 2010 r., cyberataki zostały sklasyfikowane na drugiej pozycji (po terroryzmie międzynarodowym) jako globalne zagrożenie światowego bezpieczeństwa. W natowskim dokumencie podkreślono, że do ataków w przestrzeni cyfrowej dochodzi coraz częściej, są one coraz lepiej zorganizowane i coraz bardziej kosztowne. Cyberbezpieczeństwo stało się bardzo ważne dla NATO zwłaszcza po cyberataku serbskich

---

[19] T. Pączkowski, *Słownik cyberbezpieczeństwa*, Katowice 2017, s. 10.

[20] Por. W. Gibson, *Neuromancer*, przeł. P. Cholewa, Opole 1992.

[21] Por. np. *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, M. Zwierżdżyński i in. (red.), Kraków 2015.

[22] *Glossary of Key Information Security Terms*, R. Kissel (red.), NIST Interagency or Internal Report (NISTIR) 7298, 2013 r., revision 2, s. 58, https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [dostęp: 14 VIII 2020].

hakerów na strony natowskie w 1999 r., a także po ataku, jakiego w 2007 r. doświadczyła Estonia, a w 2008 r. – Gruzja. Również atak hakerski (najprawdopodobniej izraelski lub izraelsko-amerykański) przeprowadzony w 2010 r. na irańskie wirówki jądrowe pokazał, jak niewielkim kosztem można zadać poważne ciosy, wykorzystując narzędzia cyberwojny w postaci oprogramowania typu *malware* – w tym przypadku robaka komputerowego Stuxnet[23]. Tego rodzaju incydenty skłoniły NATO do podjęcia prac nad przygotowaniem odpowiednich strategii przeciwdziałania nowym zagrożeniom, czego pierwszym efektem było opracowanie w 2010 r. dokumentu *Polityka NATO w dziedzinie cyberobrony* (*The NATO Policy on Cyber Defence*).

Cyberprzestrzeń może być wykorzystana w wojnie psychologicznej, przede wszystkim do zakłócania przebiegu procesów wyborczych i wpływania na opinię publiczną w okresie wyborów. Jest to najczęściej wskazywana możliwość oddziaływania za pośrednictwem internetu na nastroje społeczne. Oprócz wywierania wpływu na bieg życia politycznego jako najbardziej prawdopodobne przyszłe zagrożenie wskazuje się wywoływanie zakłóceń w prawidłowym funkcjonowaniu Internetu rzeczy (*Internet of Things*, IoT). Coraz bardziej powszechne są połączenia przedmiotów, instalacji, obiektów i infrastruktury. Budzi to obawy ekspertów dotyczące możliwości przeprowadzenia ataków hakerskich na Internet rzeczy i dokonywania zniszczeń fizycznych przez wywoływanie awarii oraz katastrof technicznych. Jako jedno z głównych zagrożeń często wskazuje się również cyberterroryzm[24], chociaż jest to niewłaściwy i mylący termin, z którego, zdaniem coraz większej grupy ekspertów, należałoby zrezygnować na rzecz określeń „aktywność terrorystów w Internecie" oraz „cyberataki". Taki pogląd został zaprezentowany m.in. podczas konferencji CyberSec (European Cybersecurity Forum – Europejskie Forum Cyberbezpieczeństwa) w 2017 r., jak również w raporcie Europolu w 2018 r.[25]

Wykorzystanie narzędzi cybernetycznych do celów przestępczych jest określane jako „cyberprzestępczość" i najczęściej jest związane z działaniem transnarodowych grup przestępczości zorganizowanej (TPZ)[26]. Polega ono na dokonywaniu różnych

---

[23] Szerzej na temat cyberwojny zob. m.in.: P. Łuczuk, *Cyberwojna. Wojna bez amunicji*, Kraków 2017; M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015; P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar. What Everyone Needs to Know*, Oxford 2014.

[24] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, A. Podraza, P. Potakowski, K. Wiak (red.), Warszawa 2013; E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, s. 63–80; A. Bógdał-Brzezińska, F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

[25] *Internet Organised Crime Threat Assessment (IOCTA) 2018*, Europol, Bruksela 2018, s. 52, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 [dostęp: 18 II 2021].

[26] Zob. D. Farbaniec, *Cyberwojna. Metody działania hakerów*, Gliwice 2018, s. 163, 199, 219–228; R. Borkowski, M. Kudzin-Borkowska, *Transnarodowa przestępczość zorganizowana*, w: *Zagrożenia i instytucje bezpieczeństwa międzynarodowego*, E. Cziomer (red.), Kraków 2016, s. 85–100; *Przestępczość w XXI wieku: zapobieganie i zwalczanie: problemy technologiczno-informatyczne*,

rodzajów oszustw, kradzieży informacji (*stealing*) i wyłudzeń (*phishing*), szantażowaniu (*ransomware*), dokonywaniu włamań do systemów komputerowych (*cracking*), stosowaniu botnetów, bomb logicznych, fałszywych alarmów (*hoax*), niszczeniu zasobów informacji przez wirusy komputerowe (*malware*), przekształcaniu oraz wprowadzaniu fałszywej informacji. Również rozwój Darknetu niesie niebezpieczeństwo wzrostu przestępczości zorganizowanej, zarówno o charakterze cyfrowym, jak i klasycznym.

W Polsce koncepcje strategiczne w zakresie cyberbezpieczeństwa są zawarte w pięciu dokumentach strategicznych. Są to: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020* (opracowana przez Ministerstwo Cyfryzacji w 2016 r.), *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* (opracowana przez Ministerstwo Cyfryzacji w 2017 r.), *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej* (wydana przez Biuro Bezpieczeństwa Narodowego w 2015 r.), *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (opracowana w Ministerstwie Administracji i Cyfryzacji oraz Agencji Bezpieczeństwa Wewnętrznego w 2013 r.) oraz *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* (opracowany przez Ministerstwo Spraw Wewnętrznych i Administracji w 2010 r.).

W *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* cyberbezpieczeństwo jest zdefiniowane jako bezpieczeństwo sieci i systemów informatycznych oraz bezpieczeństwo teleinformatyczne i (…) *oznacza odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne*[27]. Strategia zakłada intensywną współpracę międzynarodową nie tylko w sferze politycznej, lecz także na poziomie operacyjno-technicznym, co będzie realizowane m.in. z pomocą sieci CSIRT (Computer Security Incident Response Team) w ramach Unii Europejskiej i NATO oraz Grupy V4.

Z kolei w *Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej* cyberprzestrzeń jest traktowana jako piąte pole walki, gdyż według jej autorów jest polem konfliktu, na którym przychodzi zmierzyć się nie tylko z innymi państwami, lecz także z wrogimi organizacjami, m.in. z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi. Doktryna definiuje cyberprzestrzeń bardzo obszernie jako:

> (…) przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także

E. Pływaczewski, W. Filipkowski, Z. Rau (red.), Warszawa 2015; J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015.

[27] Ministerstwo Cyfryzacji, Warszawa 2017, www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351a-a025be09 [dostęp: 11 VI 2019].

> wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Cyberbezpieczeństwo jest tu zdefiniowane jako (…) *proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni*[28]. Autorzy dokumentu stwierdzają:

> Szansą dla wzmocnienia cyberbezpieczeństwa RP jest wykorzystanie potencjału wynikającego z członkostwa Polski w sojuszniczych strukturach obrony i ochrony cybernetycznej (NATO, UE), ukierunkowane na potrzeby państwa zaangażowanie w prace organizacji międzynarodowych, aktywność na forum gremiów zajmujących się bezpieczeństwem w cyberprzestrzeni, a także bilateralna współpraca z państwami bardziej zaawansowanymi w sprawach cyberbezpieczeństwa.

W omawianym dokumencie nie ma natomiast żadnej wzmianki o współpracy w ramach Grupy Wyszehradzkiej.

W *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* cyberprzestrzeń jest definiowana jako (…) *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*. W tym dokumencie jest mowa również o bezpieczeństwie cyberprzestrzeni rozumianym jako (…) *zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni*[29]. Wprawdzie autorzy dokumentu stwierdzili, że istotnym elementem jest utrzymanie i rozwijanie współpracy międzynarodowej w tym zakresie, ale nie wspomnieli o partnerach tej współpracy.

W *Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* cyberprzestrzeń określono jako (…) *cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Autorzy operują pojęciem bezpieczeństwo w cyberprzestrzeni, ale go nie definiują, podają natomiast definicję pojęcia ochrona cyberprzestrzeni, która jest rozumiana jako (…) *zespółprzedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo*

---

[28] Biuro Bezpieczeństwa Narodowego, Warszawa 2015, http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 14 VIII 2020].

[29] https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [dostęp: 29 IX 2018].

cyberprzestrzeni[30]. W zadeklarowanej współpracy międzynarodowej wskazuje się Unię Europejską i NATO, ale nie wspomina się o Grupie V4.

Jak widać, w różnych dokumentach strategicznych cyberbezpieczeństwo jest ujmowane i definiowane w sposób odmienny. W *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* jest opisywane jako stan bezpieczeństwa sieci i systemów informatycznych oraz stanowi synonim bezpieczeństwa teleinformatycznego, rozumianego również jako odporność systemów. W *Doktrynie Cyberbezpieczeństwa RP* z 2015 r. jest pojmowane z kolei jako proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa i jego instytucji. Widoczne jest zatem, że w RP nie wypracowano dotychczas spójnej, długofalowej koncepcji polityki cyberbezpieczeństwa, a poszczególne instytucje państwa tworzą własne koncepcje. Różnią się one od siebie, zależnie od organu administracji publicznej tworzącego dokument oraz od zachodzących zmian politycznych.

Na Węgrzech jedynym obowiązującym dokumentem państwowym dotyczącym *cybersecurity* jest *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról* (*Strategia Cyberbezpieczeństwa Węgier*) z 2013 r. Cyberprzestrzeń jest w nim określona jako globalnie połączone, zdecentralizowane, zwiększające się zasoby informacji, elektroniczne systemy i dane. Cyberbezpieczeństwo zostało natomiast dość szeroko zdefiniowane jako polityczne, prawne i techniczne narzędzia umożliwiające skuteczne utrzymanie akceptowalnego poziomu ryzyka w cyberprzestrzeni. Strategia zawiera odniesienia do koncepcji strategicznych NATO oraz Unii Europejskiej w zakresie polityki bezpieczeństwa cyberprzestrzeni, nie ma w niej natomiast żadnego nawiązania do Grupy V4. Znajduje się jedynie zapis mówiący o tym, że Węgry poświęcają szczególną uwagę regionowi Europy Środkowej i Wschodniej.

W Republice Czeskiej inicjatywy dotyczące opracowania cyberstrategii podjęto dwukrotnie, przyjmując *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012–2015* (*Strategię w zakresie cyberbezpieczeństwa Republiki Czeskiej na lata 2012–2015*), a następnie *Národní strategie kybernetické bezpečnosti naźobdobí let 2015 až 2020* (*Narodową strategię bezpieczeństwa cybernetycznego na lata od 2015 do 2020*). Ani w pierwszym, ani w drugim dokumencie nie zdefiniowano pojęć „cyberbezpieczeństwo" oraz „cyberprzestrzeń" [31]. Jeśli chodzi o współpracę międzynarodową, to w pierwszym z nich zadeklarowano współdziałanie w ramach Unii Europejskiej, NATO, Organizacji Narodów Zjednoczonych, Organizacji Współpracy Gospodarczej i Rozwoju (dalej: OECD), Międzynarodowej Unii Telekomunikacyjnej oraz innych organizacji międzynarodowych, a w strategii aktualnie obowiązującej podkreśla się znaczenie współpracy międzynarodowej, ale w sposób wyjątkowo ogólny, i w ogóle nie

[30] Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 17 X 2020].

[31] Národní úřad pro kybernetickou a informační bezpečnost, https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf [dostęp: 9 III 2020].

wspomina się o Grupie V4[32]. Deklaruje się aktywne wspieranie partnerów międzynarodowych w zapobieganiu cyberatakom i promowanie cyberbezpieczeństwa oraz współpracy w dziedzinie obronności, jak również budowanie dialogu dotyczącego tych kwestii między krajami środkowoeuropejskimi. W towarzyszących planach działania (czes. *Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012–2015* oraz *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*) problematyka współpracy Republiki Czeskiej z Grupą V4 została nakreślona jako współdziałanie w ramach Środkowoeuropejskiej Platformy Cyberbezpieczeństwa (Central European Cyber Security Platform, CECSP) utworzonej przez Austrię i Czechy.

Na Słowacji jako pierwszą przyjęto strategię o nazwie *Národná stratégia pre informačnú bezpečnosť v Slovenskej republike 2008* (*Narodowa strategia na rzecz bezpieczeństwa informacyjnego Republiki Słowacji 2008*). Siedem lat później został ogłoszony obowiązujący do dziś dokument zatytułowany *Koncepcia kybernetickej bezpecnosti Slovenskej republiky na roky 2015–2020* (*Koncepcja bezpieczeństwa cybernetycznego Republiki Słowacji na lata 2015–2020*)[33]. W pierwszej strategii pojęcie „cyberbezpieczeństwo" w ogóle nie występuje, mówi się natomiast o aspekcie cybernetycznym, elektronicznym oraz infrastruktury krytycznej w odniesieniu do bezpieczeństwa informacyjnego, ale nie definiuje się żadnego z tych pojęć. Wskazuje się na znaczenie współpracy międzynarodowej w ramach UE, OECD, ISO (Międzynarodowa Organizacja Normalizacyjna) oraz z Republiką Czeską, nie wymienia się natomiast Grupy V4. W koncepcji obowiązującej aktualnie pojęcie „cyberbezpieczeństwo" jest zdefiniowane obszernie i zawile jako system ciągłego podnoszenia świadomości politycznej, prawnej i ekonomicznej, a także system podnoszenia poziomu bezpieczeństwa i obrony oraz zwiększania skuteczności przyjętych i stosowanych techniczno-organizacyjnych środków zarządzania ryzykiem w cyberprzestrzeni. W ten sposów zmierza sie do jej przekształcenia w środowisko godne zaufania, które pozwoli na bezpieczne funkcjonowanie społeczne i gospodarcze.

Jeżeli chodzi o wspólne działania czterech państw regionu na rzecz cyberbezpieczeństwa i bezpieczeństwa teleinformatycznego, to już w Deklaracji Wyszehradzkiej z 15 lutego 1991 r. znajduje się zapowiedź, że państwa członkowskie skoordynują rozwój swoich systemów energetycznych i sieci telekomunikacyjnych. Z biegiem czasu, wraz z ewolucją zagrożeń w sferze bezpieczeństwa wynikającą m.in. z członkostwa w NATO, komponent cyberprzestrzenny zyskała również współpraca wojskowa i policyjna[34]. Państwa Grupy V4 wypracowały swoje własne strategie cyberbezpieczeństwa na podstawie światowych wzorców w tej dziedzinie. W tych dokumentach zgłaszają

---

[32] Národní bezpečnosti úřad, https://www.cybersecurity.cz/data/navratil2014.pdf [dostęp: 5 IX 2020].

[33] Národný bezpečnostný úrad, https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf [dostęp: 22 XII 2019].

[34] *Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje*, J. Świątkowska (red.), Kraków 2012.

wprawdzie gotowość szerokiej współpracy międzynarodowej, w tym środkowoeuropejskiej, jednak można zauważyć, że każdy z krajów członkowskich ma ambicje odgrywania roli lidera w regionie.

W czasie poszczególnych prezydencji w Radzie UE kraje członkowskie Grupy V4 deklarowały rozmaite wspólne inicjatywy. Postulat współpracy w dziedzinie cyberbezpieczeństwa został po raz pierwszy wyeksponowany w 2007 r., podczas prezydencji Republiki Czeskiej. W 2012 r. Polska, podczas swojej prezydencji, zapowiedziała konsultacje w sprawie bezpieczeństwa z udziałem również państw bałtyckich oraz Bułgarii i Rumunii, co stanowiło wyraźny przejaw dążenia do tworzenia tzw. Międzymorza. Z kolei Węgry w 2014 r. zaproponowały powołanie grupy roboczej poświęconej cyberobronie (Cyber Defence Working Group).

Wśród form działania na rzecz intensyfikacji polityki bezpieczeństwa cybernetycznego Grupy V4 trzeba wskazać wspólne ćwiczenia i warsztaty w rodzaju Cyber Visegrad Workshop, a także inicjatywy podejmowane w szerszym wymiarze, jak Europejskie Forum Cyberbezpieczeństwa. Strona polska aspiruje do roli regionalnego lidera i dąży do tego, aby rekomendacje wypracowywane w trakcie CyberSec pozwalały na wzmocnienie współpracy między państwami Grupy V4, Morza Bałtyckiego oraz innymi państwami Europy Centralnej na rzecz ochrony cyberprzestrzeni. Efektem konferencji, która odbyła się w 2016 r., było powołanie w Krakowie Cybersec Hub w celu stworzenia efektywnego sektora produktów i usług w obszarze cyberbezpieczeństwa oraz szkolenia światowej klasy cyberspecjalistów.

Bilans dotychczasowej współpracy na rzecz wypracowania wspólnej polityki bezpieczeństwa Grupy V4 w cyberprzestrzeni okazuje się jednak skromny. Największe osiągnięcia można dostrzec w zwalczaniu cyberprzestępczości, co wynika przede wszystkim z dobrze rozwiniętej regionalnej współpracy policyjnej w zwalczaniu przestępczości zorganizowanej. Znacznie mniej skuteczne są jest walka ze szpiegostwem w sieci oraz przeciwdziałanie zagrożeniom militarnym w cyberprzestrzeni. Na przeszkodzie do osiągnięcia spójności działań stoi wzajemna rywalizacja polityczna każdego z czterech państw oraz partykularne interesy elit rządzących. Zarówno Polska, jak i Węgry, Czechy czy Słowacja starają się rozwijać bezpośrednią współpracę z wiodącymi ośrodkami na Zachodzie, pomijając w tych staraniach wspólnotę wyszehradzką. Polska skupia swoje wysiłki na współpracy z państwami bałtyckimi, w tym przede wszystkim z wiodącym natowskim ośrodkiem CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence) w Tallinie. Konkurencja, której skutkiem jest brak wspólnej wizji polityki cyberbezpieczeństwa, osłabia Grupę Wyszehradzką i powoduje, że staje się ona trzeciorzędnym graczem w obszarze *cybersecurity*. Symptomatyczne, że nawet Środkowoeuropejska Platforma Cyberbezpieczeństwa utworzona w 2013 r. nie była przedsięwzięciem podjętym w ramach Grupy V4, lecz powstała z inicjatywy Austrii i Czech, do których dołączyły później Słowacja, Polska i Węgry. W istocie kraje Grupy V4 wykazują bierność – realizują kierunki rozwoju cyberbezpieczeństwa wytyczone rekomendacjami zawartymi w dokumentach strategicznych NATO oraz Unii Europejskiej i rozwijają swoją cyberobronę m.in. z pomocą narodowych zespołów

reagowania na zagrożenia komputerowe, czyli CERT-ów (Computer Emergency Response Team), ale nie robią nic ponadto[35]. Jak twierdzi Bogusław Olszewski, można postawić tezę, że w sferze cyberbezpieczeństwa Grupa V4 stanowi wtórną platformę współpracy państw Europy Środkowej, przy czym każde z państw członkowskich ma ambicje zaistnienia w tej dziedzinie i zamiast pełnego współdziałania w regionie jest widoczna wyraźna konkurencja[36].

Symptomatyczna dla braku konsolidacji w obszarze *cybersecurity* w Grupie V4 jest tzw. afera Huawei. Z całą ostrością uwidoczniły sie tu nie tylko kwestie związane z cyberbezpieczeństwem, lecz także ze stosunkiem do polityki amerykańskiej, co doprowadziło do licznych międzynarodowych napięć. Koncern utworzony w latach 80. XX w. we współpracy z chińskimi wojskami inżynieryjnymi jest obecnie największym na świecie producentem sprzętu telekomunikacyjnego, a także dostawcą technologii IT. Stany Zjednoczone, Australia i Kanada uznały w 2012 r., że współpraca z Huawei stanowi zagrożenie ich cyberbezpieczeństwa i oskarżyły koncern o cyberszpiegostwo przez umieszczanie w swoich urządzeniach oprogramowania umożliwiającego ich zdalną kontrolę. Wielka Brytania, USA, Japonia, Australia i Nowa Zelandia zdecydowały o zablokowaniu prac Huawei nad rozwojem sieci 5G na swoich rynkach cyfrowych. Prezydent USA dodatkowo zadekretował zakaz korzystania z technologii koncernów Huawei i ZTE przez administrację amerykańską i firmy z nią współpracujące. Departament Sprawiedliwości USA przedstawił Huawei 13 zarzutów, dotyczących m.in. łamania amerykańskich sankcji nałożonych na Iran, a także oszustw bankowych i elektronicznych oraz szpiegostwa przemysłowego. Stany Zjednoczone wystąpiły również z formalnym wnioskiem o ekstradycję wiceprezes koncernu Meng Wanzhou aresztowanej w Kanadzie, oskarżanej o oszustwa.

Na rynku środkowoeuropejskim firma Huawei jest obecna od 2011 r. W Polsce miała wspierać rozwój sieci 5G przez dostarczenie komponentów do budowy jej infrastruktury i podjęcie w 2018 r. współpracy z operatorami Orange i T-Mobile. Podobnie działo się w Czechach, gdzie chińskie inwestycje i współpraca Huawei z koncernem telekomunikacyjnym PPF oraz energetycznym ČEZ cieszą się poparciem prezydenta państwa Miloša Zemana. Jednakże pod koniec 2018 r. Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego Republiki Czeskiej (NUKIB) wydał ostrzeżenie o możliwym zagrożeniu bezpieczeństwa państwa związanym z urządzeniami produkowanymi przez firmy Huawei i ZTE. Premier Czech Andrej Babisz zwołał posiedzenie Rady Bezpieczeństwa Państwa, która krytycznie odniosła się do enuncjacji NUKIB, zalecając Krajowemu Urzędowi ds. Bezpieczeństwa Sieci i Informacji (NUCK) wydawanie ostrzeżeń dotyczących wyłącznie systemów sklasyfikowanych

---

[35] J. Dereń, A. Rabiej, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (red.), Warszawa 2014, s. 202–221; *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, Warszawa 2015.

[36] B. Olszewski, *Perspektywy regionalizacji cyberbezpieczeństwa w ramach Grupy Wyszehradzkiej*, w: *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, H. Chałupczak, M. Pietraś, J. Misiągiewicz (red.), Zamość 2016, s. 203–215.

jako infrastruktura krytyczna lub ważne systemy informacyjne, lecz nie w odniesieniu do zwykłych użytkowników oraz urządzeń końcowych. Ostatecznie premier opowiedział się za tym, aby kwestię obecności Huawei na rynku europejskim rozwiązywała Unia Europejska. Tymczasem Węgry odrzuciły amerykańską propozycję przyłączenia się do walki z chińskim szpiegostwem cybernetycznym. Premier Viktor Orbán oświadczył, że zamierza prowadzić neutralną politykę zagraniczną na wzór Austrii, a nie spełniać żądania USA. Analogiczne stanowisko zajęła Słowacja, która nie podjęła żadnych kroków przeciwko Huawei. Premier Peter Pellegrini ogłosił, że brakuje dowodów na szpiegowską działalność chińskiego koncernu, w związku z czym Słowacja nie uznaje go za zagrożenie bezpieczeństwa i nie nałoży na niego restrykcji, dopóki nie pojawią się przeciwko niemu konkretne dowody. Podkreślił też, że słowackie organy nadzorcze i służby bezpieczeństwa nie wydały podobnego ostrzeżenia jak służby czeskie. Eksperci wskazują, że afera Huawei jest elementem rozgrywki w amerykańsko-chińskich sporach handlowych. W tym miejscu warto przypomnieć, że w styczniu 2019 r. w Polsce Agencja Bezpieczeństwa Wewnętrznego zatrzymała dwie osoby pod zarzutem z art. 130 ust. 1 *Kodeksu karnego*[37], który mówi o szpiegostwie przeciw RP. Wśród zatrzymanych był dyrektor polskiego oddziału Huawei, który w latach 2006–2011 piastował stanowisko w konsulacie generalnym Chińskiej Republiki Ludowej w Gdańsku. Zdaniem dr Justyny Szczudlik (kierownik programu Azji i Pacyfiku w Polskim Instytucie Spraw Międzynarodowych): (…) *firma Huawei prawdopodobnie realizuje interesy chińskiego rządu i może być narzędziem wpływu stosowanym przez Chiny w innych państwach. Nie można wykluczyć scenariusza, że nasza część Europy może stać się miejscem rywalizacji USA i Chin*[38].

Polityczny charakter rywalizacyjnych posunięć Warszawy, Pragi, Bratysławy i Budapesztu powoduje, że nie ma spójnej i konsekwentnej współpracy Grupy V4 w dziedzinie cyberbezpieczeństwa. Przyczyn słabości należy szukać w różnicach polityki wobec Rosji i Ukrainy, polityki energetycznej i zakupów gazu ziemnego oraz polityki wobec Brukseli. Widoczne jest, że Polska skłania się do regionalizacji cyberbezpieczeństwa w kierunku północnym, a nie wyszehradzkim, tj. do współpracy z państwami bałtyckimi, z wiodącym centrum CCDCOE w Tallinie, które jest wielonarodowym, interdyscyplinarnym ośrodkiem cyberobrony. Konceptualizacje cyberbezpieczeństwa w dokumentach strategicznych poszczególnych państw Grupy V4 różnią się od siebie i dotychczas nie podjęto żadnej próby ujednolicenia podejścia do tego problemu w obrębie Grupy. Nie można więc mówić o jej wspólnej i spójnej polityce dotyczącej cyberbezpieczeństwa. Współpraca w tym zakresie jest słabo rozwinięta i nawet w sferze deklaratywnej nie widać wyraźnej woli elit państw tej Grupy, aby ją budować, rozwijać i pogłębiać.

---

[37] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

[38] *Dyrektor Huawei i były funkcjonariusz ABW zatrzymani pod zarzutem szpiegostwa*, „Newsweek", 11 I 2019 r., https://www.newsweek.pl/polska/dyrektor-huawei-i-byly-funkcjonariusz-abw-zatrzymani-pod-zarzutem-szpiegostwa/rp8vxq5 [dostęp: 29 VI 2020].

Bibliografia

Banasiński C., *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, Wolters Kluwer.

Bayuk J.L. i in., *Cyber Security Policy Guidebook*, Hoboken 2012, Wiley-Blackwell.

Bezpieczeństwo teleinformatyczne państwa, M. Madej, M. Terlikowski (red.), Warszawa 2009, Polski Instytut Spraw Międzynarodowych.

Borkowski R., *Cywilizacja, technika, ekologia. Wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku*, Kraków 2001, Wydawnictwa AGH.

Bógdał-Brzezińska A., Gawrycki F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, Oficyna Wydawnicza ASPRA-JR.

Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku, M. Górka (red.), Warszawa 2016, Difin.

Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, A. Podraza, P. Potakowski, K. Wiak (red.), Warszawa 2013, Difin.

Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa, H. Chałupczak, M. Pietraś, J. Misiągiewicz (red.), Zamość 2016, Wydawnictwo „Officina Simonidis".

E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni, M. Zwierżdżyński i in. (red.), Kraków 2015, Akademia Ignatianum.

Jańczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, Akademia Obrony Narodowej.

Jaźwiński J., Ważyńska-Fiok K., *Bezpieczeństwo systemów*, Warszawa 1993, Wydawnictwo Naukowe PWN.

Korzeniowski L.F., *Securitologia: nauka o bezpieczeństwie człowieka i organizacji społecznych*, Chorzów 2009, Wydawnictwo Wyższej Szkoły Bankowej WZ w Chorzowie.

Kossecki J., *Cybernetyka społeczna*, Warszawa 1981, PWN.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, Wydawnictwo Uniwersytetu Śląskiego.

Lakomy M., *Dylematy polityki cyberbezpieczeństwa Polski*, w: *Dylematy polityki bezpieczeństwa Polski na początku drugiej dekady XXI wieku*, K. Czornik, M. Lakomy (red.), Katowice 2014, Wydawnictwo Regionalnego Ośrodka Debaty Międzynarodowej, s. 425–454.

Lichocki E., *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, Difin, s. 63–80.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2015, Wydawnictwo Naukowe PWN.

Liedel K., *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, Difin, s. 45–62.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2014, Wydawnictwo Adam Marszałek.

Liedel K., *Cyberbezpieczeństwo – wyzwania przyszłości. Działania społeczności międzynarodowej*, w: *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2011, Difin, s. 437–448.

Ochrona informacji niejawnych w XXI wieku, S. Topolewski (red.), Siedlce 2016, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego.

Pączkowski T., *Słownik cyberbezpieczeństwa,* Katowice 2017, Szkoła Policji w Katowicach.

Przestępczość w XXI wieku: zapobieganie i zwalczanie: problemy technologiczno-informatyczne, E. Pływaczewski, W. Filipkowski, Z. Rau (red.), Warszawa 2015, Wolters Kluwers.

Pręgiel R., Buchwald P., *Internet w społeczeństwie informacyjnym – nowoczesne systemy informatyczne i ich bezpieczeństwo*, Dąbrowa Górnicza 2014, Wydawnictwo Wyższej Szkoły Biznesu.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014, Warszawa 2015, CERT ABW.

Singer P.W., Friedman A., *Cybersecurity and Cyberwar. What Everyone Needs to Know*, Oxford 2014, Oxford University Press.

Strnád O., *Riadenie rizík informačnej bezpečnosti*, Ostrava 2010, Amos.

Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje, J. Świątkowska (red.), Kraków 2012, Instytut Kościuszki.

Źródła internetowe

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 14 VIII 2020].

Dyrektor Huawei i były funkcjonariusz ABW zatrzymani pod zarzutem szpiegostwa, „Newsweek", 11 I 2019 r., www.newsweek.pl/polska/dyrektor-huawei-i-byly-funkcjonariusz-abw-zatrzymani-pod-zarzutem-szpiegostwa/rp8vxq5 [dostęp: 29 VI 2020].

Glossary of Key Information Security Terms, Kissel R. (red.), NISTIR 7298, rev. 2, 2013, https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [dostęp: 14 VIII 2020].

Internet Organised Crime Threat Assessment (IOCTA) 2018, Europol, Bruksela, 2018 r., www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 [dostęp: 18 II 2021].

Koncepcia kybernetickej bezpecnosti Slovenskej republiky na roky 2015–2020, Národný bezpečnostný úrad, https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf [dostęp: 22 XII 2019].

Národní strategie kybernetické bezpečnosti na období let 2015 až 2020, Národní bezpečnosti úřad, www.cybersecurity.cz/data/navratil2014.pdf [dostęp: 5 IX 2020].

Národní úřad pro kybernetickou a informační bezpečnost, www.govcert.cz/download/legislativa/containernodeid719/20120209strategieprooblastkbnbu.pdf [dostęp: 9 III 2020].

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [dostęp: 29 IX 2018].

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010 r., www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 17 X 2020].

Snow B., *What Would a World Without Internet Look Like? A thought experiment*, „The Atlantic", 5 IV 2016 r., www.theatlantic.com/technology/archive/2016/04/a-world-without-internet/476907/ [dostęp: 18 II 2021].

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017 r., www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09 [dostęp: 11 VI 2019].

Abstrakt

W artykule podjęto problematykę cyberbezpieczeństwa w Grupie Wyszehradzkiej. Mimo że w nauce pojawia się wiele terminów dotyczących bezpieczeństwa informacyjnego, jednak w ostatnich latach w dokumentach strategicznych dominuje kategoria pojęciowa „cyberbezpieczeństwo". W *Strategii Bezpieczeństwa Cybernetycznego Unii Europejskiej* z 7 marca 2013 r. stwierdza się, że bezpieczeństwo cybernetyczne odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą

jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci oraz tę infrastrukturę uszkodzić. Państwa Grupy Wyszehradzkiej wypracowały swoje własne strategie cyberbezpieczeństwa na podstawie światowych wzorców w tej dziedzinie. W tych dokumentach deklarują wprawdzie gotowość współpracy międzynarodowej, także środkowoeuropejskiej, jednak widać, że każde z nich ma ambicje odgrywania roli środkowoeuropejskiego lidera.

Słowa kluczowe: cyberbezpieczeństwo, strategie cyberbezpieczeństwa, Grupa Wyszehradzka, bezpieczeństwo teleinformatyczne, bezpieczeństwo informacyjne.

Cybersecurity in the Visegrad Group – concepts and strategies

Abstract

The article discusses the issues of cybersecurity in the Visegrad Group. There is a wide spectrum of information security terminology, but the conceptual category of cybersecurity has dominated strategic documents in recent years. The European Union Cyber Security Strategy of 7, March 2013, claims that cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. The Visegrad Group countries have developed their own cybersecurity strategies based on global models in this field. However, in these strategic documents they declare readiness for broad international cooperation, including Central European, it can be seen that each of them strives to play the role of a leader in Central Europe.

Keywords: cybersecurity, cybersecurity strategies, the Visegrad Group, ICT security, information security.

RAFAŁ WĄDOŁOWSKI
ORCID: 0000-0003-0601-1213

DOI: 10.4467/20801335PBW.21.006.13563

Ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane regulacje karne i administracyjne

W związku z brakiem piśmiennictwa poświęconego prawodawstwu, które dotyczyłoby ochrony informacji niejawnych w Federacji Rosyjskiej (dalej: FR), należy uznać za niezbędne chociażby ogólne omówienie systemu ochrony tajemnic państwowych w Rosji. Przedstawienie instytucji prawnych naszego wschodniego sąsiada jest też pretekstem do próby przeprowadzenia analizy porównawczej rozwoju systemu ochrony tajemnic publicznoprawnych w Rzeczpospolitej Polskiej (dalej: RP). Należy nadmienić, że w Polsce odrodzonej w 1918 r. kodeks karny był początkowo tożsamy z kodeksem rosyjskim, co było spowodowane przyjęciem tzw. kodeksu Nikołaja Tagancewa z 1903 r. Po II wojnie światowej kilkudziesięcioletnie pozostawanie Polski w strefie wpływów politycznych Związku Radzieckiego przyczyniło się do unifikacji formalnie odrębnych systemów prawnych. Dotyczyło to szczególnie sfery tajemnicy odnoszącej się do potencjalnych działań militarnych w ramach ówczesnego Układu Warszawskiego oraz podtrzymywania socjalistycznego ustroju państwa. Zmiany polityczne w RP po 1990 r. były podstawą ewoluowania systemu prawnego w kierunku demokratycznego państwa prawa, czego wyrazem było przyjęcie Konstytucji RP w 1997 r.[1] Wstąpienie Polski do NATO (1999 r.) i do Unii Europejskiej (2004 r.) determinowało dostosowanie systemu ochrony informacji niejawnych do standardów obowiązujących w państwach członkowskich tych organizacji, z jednoczesnym uwzględnieniem konstytucyjnego prawa obywateli do informacji publicznej. Tak określona tematyka badawcza implikuje hipotezę, że aktualne systemy ochrony tajemnicy państwowej w Rosji oraz informacji niejawnych w Polsce wykazują istotne różnice.

---

[1] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.* (DzU z 1997 r. nr 78 poz. 483).

Ograniczenie konstytucyjnego prawa do informacji w Federacji Rosyjskiej

W aktach prawnych ustanawiających system ochrony tajemnic w FR informacje niejawne o najwyższej ważności ze względu na bezpieczeństwo państwa określa się terminem tajemnica państwowa (ros. *государственная тайна*, pis. fon. gosudarstwiennaja tajna). System ochrony tajemnicy państwowej w Rosji, podobnie jak system ochrony informacji niejawnych w Polsce, jest oparty na dwóch filarach: karnoprawnym i administracyjnym. Rosyjskie tajemnice państwowe są informacjami klauzulowanymi, a ich odpowiednikiem w polskim prawodawstwie są informacje chronione na podstawie ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych[2]. Na potrzeby niniejszego opracowania będą to pojęcia synonimiczne.

W Rosji najważniejszym aktem ustanawiającym obywatelskie prawo do informacji oraz określającym sposób jego ograniczania jest Konstytucja FR z 1993 r.[3] Prawo do poszukiwania, uzyskiwania, przekazywania, wytwarzania, rozpowszechniania i dostępu do informacji zostało określone w rozdziale drugim tego aktu prawnego pt. *Prawa i wolności człowieka i obywatela*, w art. 29 ust. 4[4]. W drugim zdaniu wymienionego przepisu zaznaczono, że informacje stanowiące tajemnicę państwową wskazuje prawo federalne. Aktualnie jest to ustawa o tajemnicy państwowej z 21 lipca 1993 r.[5], której postanowienia zostały sprecyzowane w wykazie informacji stanowiących tajemnicę państwową, wprowadzonym dekretem Prezydenta FR z 30 listopada 1995 r.[6] Zatem ograniczenie prawa do informacji jest możliwe w FR, podobnie

---

[2] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (t.j.: DzU z 2019 r. poz. 742).

[3] *Конституция Российской Федерации от 12 декабря 1993 г.*, принятая всенародным голосованием 12 декабря 1993 года, вступила в силу в день её официального опубликования в газете „Российская газета" от 25.12.1993 № 237 (*Konstytucja Federacji Rosyjskiej z 12 grudnia 1993 r.*, przyjęta w głosowaniu całego narodu w dniu 12 grudnia 1993 r., obowiązuje od 25 grudnia 1993 r., z dniem jej oficjalnego opublikowania w gazecie „Gazeta Rosyjska" nr 237 – tłum. aut. **Wszystkie tłumaczenia w artykule pochodzą od autora** – przyp. red.); A. Bosiacki, H. Izdebski, *Konstytucjonalizm rosyjski. Historia i współczesność*, Kraków 2013, s. 271 i nast.

[4] *Конституция Российской Федерации*…, статья 29.4.: „Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом" (*Konstytucja Federacji Rosyjskiej*…, art. 29.4.: „Każdy ma prawo do swobodnego poszukiwania, uzyskiwania, przekazywania, tworzenia i rozpowszechniania informacji w dowolny, zgodny z prawem, sposób. Wykaz informacji stanowiących tajemnicę państwową określa ustawa federalna").

[5] *Закон Российской Федерации от 21 июля 1993 г., № 5485, „О государственной тайне"*, с изменениями, Законодательство Российской Федерации, Сборник основных федеральных законов РФ (*Ustawa FR „O tajemnicy państwowej" z 21 lipca 1993 r. nr 5485-1*, ze zmianami, Prawodawstwo Federacji Rosyjskiej, Zbiór podstawowych ustaw federalnych), http://fzrf.su/zakon/o-gosudarstvennoj-tajne-n-5485-1/ [dostęp: 30 VII 2020].

[6] *Указ Президента РФ от 30 ноября 1995 г., № 1203, „Об утверждении перечня сведений, отнесенных к государственной тайне"* (*Dekret Prezydenta FR z 30 listopada 1995 r. nr 1203*

jak w RP, wyłącznie w trybie powszechnie obowiązującej ustawy. Rosyjskim aktem uszczegóławiającym korzystanie z konstytucyjnego prawa do informacji o działalności administracji publicznej jest federalna ustawa o zapewnieniu dostępu do informacji o działalności organów państwowych i samorządów terytorialnych z 9 lutego 2009 r.[7] Wschodni ustawodawca ustanowił w niej prawa wnioskodawcy oraz obowiązki danego organu, a ponadto w art. 5 określił rodzaje informacji wyłączone z udostępniania, w tym na rzecz ochrony tajemnicy państwowej[8]. Warto dodać, że procedurę uzyskiwania informacji o działalności sądów FR objęto odrębną regulacją ustawową[9]. Konstytucja FR gwarantuje wolność masowej informacji (mass mediów) i jednocześnie zakazuje cenzury[10]. W polskim porządku prawnym obywatele mają możliwość uzyskiwania (żądania) informacji o działalności organów władzy na podstawie art. 61 ust. 1 Konstytucji RP. Jednocześnie w art. 61 ust. 3 prawodawca stanowi, że to prawo może być ograniczone w trybie ustawy między innymi z uwagi na bezpieczeństwo państwa[11]. Procedurę korzystania z prawa do informacji określono w ustawie o dostępie do informacji publicznej[12]. Należy zaznaczyć, że w art. 5 ograniczono jej stosowanie między innymi w odniesieniu do informacji niejawnych. Podstawy utajniania informacji dotyczących obszarów wskazanych w Konstytucji, w tym bezpieczeństwa, zostały uszczegółowione w art. 5 ust. 1 i 2 ustawy o ochronie informacji niejawnych.

Na marginesie tych rozważań trzeba się odnieść do historycznych przemian rosyjskiego ustroju prawnego. Wprowadzenie w 1993 r. nowej Konstytucji FR

„*O zatwierdzeniu wykazu informacji stanowiących tajemnicę państwową*"), http://base.garant.ru/10105548/ [dostęp: 19 I 2021].

7 *Федеральный закон от 9 февраля 2009 г., № 8-ФЗ, „Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления"* (*Ustawa federalna z 9 lutego 2009 r. nr 8-FZ „O zapewnieniu dostępu do informacji o działalności organów państwowych i samorządów terytorialnych*").

8 Tamże, статья 5.1.: „Доступ к информации о деятельности государственных органов и органов местного самоуправления ограничивается в случаях, если указанная информация отнесена в установленном федеральным законом порядке к сведениям, составляющим государственную или иную охраняемую законом тайну" (tamże, art. 5.1.: „Dostęp do informacji o działalności organów państwowych i jednostek samorządu terytorialnego jest ograniczony w przypadkach, gdy te informacje zostaną zaklasyfikowane w sposób określony przez prawo federalne jako informacje stanowiące tajemnicę państwową lub inną tajemnicę ustawowo chronioną").

9 *Федеральный закон от 22 декабря 2008 г., № 262-ФЗ, „Об обеспечении доступа к информации о деятельности судов в Российской Федерации"* (*Ustawa federalna z 22 XII 2008 r. nr 262-FZ „O zapewnieniu dostępu do informacji o działalności sądów w Federacji Rosyjskiej*").

10 *Конституция Российской Федерации…*, статья 29.5.: „Гарантируется свобода массовой информации. Цензура запрещается" (*Konstytucja Federacji Rosyjskiej…*, art. 29.5.: „Gwarantuje się wolność środków masowego przekazu. Cenzura jest zabroniona").

11 *Konstytucja Rzeczypospolitej Polskiej…*, art. 61 ust. 3: „Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określoną w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa".

12 *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej* (t.j.: DzU z 2020 r. poz. 2176).

nie spowodowało natychmiastowych zmian w praktyce orzeczniczej sądów oraz normowania ochrony tajemnicy państwowej przez władzę wykonawczą. Podstawowym orzeczeniem Sądu Konstytucyjnego FR w sprawie ponoszenia odpowiedzialności karnej za ujawnienie tajemnicy państwowej jest uchwała z 20 grudnia 1995 r. ze skargi obywatela Władimira Smirnowa. Sąd w uzasadnieniu jednoznacznie wskazał, że ponoszenie odpowiedzialności karnej w związku z ujawnieniem tajemnicy państwowej jest możliwe jedynie wówczas, gdy wykaz informacji stanowiących tajemnicę państwową, o którym mówił art. 29 ust. 4 Konstytucji FR, jest opublikowany w oficjalnej, jawnej i ogólnie dostępnej ustawie federalnej. Sąd wskazał, że wyrok nie może być oparty na nieopublikowanym akcie normatywnym, co wynika z art. 15 ust. 3 Konstytucji FR[13]. Ten wyrok wpłynął na zmianę dotychczasowej praktyki rosyjskich władz, która polegała na sporządzaniu wykazów informacji stanowiących tajemnicę państwową w aktach niepodlegających publikacji. Przed 1995 r. obywatele FR nie mieli zatem wiedzy o rodzajach informacji objętych ochroną państwa, co utrudniało udowodnienie sprawstwa ujawnienia tajemnicy w kontekście przepisów karnych. Pierwszym aktem opublikowanym, w którym został zawarty wykaz informacji stanowiących tajemnicę państwową, był dekret Prezydenta FR z 30 listopada 1995 r.[14] (w Polsce pierwszym opublikowanym aktem prawnym precyzującym, jakie informacje stanowią tajemnicę państwową, była ustawa z 1982 r.[15]). Profesor Aleksandr Borisow (były sędzia Sądu Konstytucyjnego FR i czołowy przedstawiciel rosyjskiej jurysprudencji) zauważa, że prawo do uzyskiwania i rozpowszechniania informacji z uwagi na zachowanie ładu społecznego jest ograniczane nawet w dojrzałych demokracjach[16]. Przywołany autor

---

[13] *Постановление Конституционного Суда РФ от 20 декабря 1995 г., № 17-П, по делу о проверке конституционности ряда положений пункта „а" статьи 64 Уголовного кодекса РСФСР в связи с жалобой гражданина В.А. Смирнова* (*Uchwała Sądu Konstytucyjnego Federacji Rosyjskiej z 20 grudnia 1995 r. nr 17-P w sprawie konstytucyjnej kontroli zakresu przepisu ustępu „a" artykułu 64 Kodeksu karnego FR w związku ze skargą obywatela W.A. Smirnowa*), http://legalacts.ru/doc/postanovlenie-konstitutsionnogo-suda-rf-ot-20121995-n/ [dostęp: 30 VII 2020]; *Конституция Российской Федерации…*, статья 15.3.: „Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения" (*Konstytucja Federacji Rosyjskiej…*, art. 15.3: „Ustawy podlegają oficjalnej publikacji. Ustawy nieopublikowane nie są stosowane. Wszelkie normatywne akty prawne dotyczące praw, wolności i obowiązków człowieka i obywatela nie są stosowane, jeżeli nie zostały oficjalnie podane do publicznej wiadomości").

[14] *Указ Президента РФ от 30 ноября 1995 г., № 1203, „Об утверждении перечня сведений…* (*Dekret Prezydenta FR z 30 listopada 1995 r. nr 1203 „O zatwierdzeniu wykazu informacji…*)

[15] *Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej* (DzU z 1982 r. nr 40 poz. 271, ze zm.). Ustawodawca w art. 6 zobligował administrację rządową do sporządzenia szczegółowych wykazów informacji objętych ochroną w zależności od charakteru danej instytucji i ogłoszenia ich w dziennikach urzędowych, z wyjątkiem informacji dotyczących obronności, Sił Zbrojnych i bezpieczeństwa państwa.

[16] А.Б. Борисов, *Комментарий к конституции Российской Федерации (постатейный): с комментариями Конституционного суда РФ*, Москва 2013, s. 56 (A.B. Borisow, *Komentarz do Konstytucji Federacji Rosyjskiej…*, Moskwa 2013).

podsumowuje, że rozpowszechnianie tajemnicy państwowej i innych tajemnic chronionych prawem w celu zachęcania do popełniania przestępstw oraz wzniecania konfliktów nacjonalistycznych, rasowych i religijnych jest zakazane w większości krajów. Jednocześnie podkreśla, że zgodnie z obowiązującym prawem wykaz tajemnic państwowych ograniczających wolność słowa może być rozszerzany w czasie wprowadzania stanów nadzwyczajnych lub stanu wojennego[17]. Podobne konsekwencje w odniesieniu do ograniczenia praw i swobód obywatelskich w Polsce są przewidziane w przypadku wprowadzenia stanu wyjątkowego i wojennego[18].

W Rosji istnieją trzy tryby sądowego dochodzenia przez stronę naruszonych praw dotyczących dostępu do informacji: przed sądem cywilnym, administracyjnym lub karnym[19].

Prawo osoby poszkodowanej bezprawną odmową dostępu do informacji albo umyślnym udzieleniem nieprawdziwych informacji do wystąpienia z powództwem cywilnym do sądu i żądania zadośćuczynienia za szkody powstałe z tego tytułu ustanawia art. 23 ust. 2 ustawy o zapewnieniu dostępu do informacji o działalności organów państwowych i jednostek samorządu terytorialnego[20]. Zasady odpowiedzialności urzędników za naruszenie prawa do informacji zostały określone w art. 25 tej ustawy. Urzędnik winny takiego naruszenia może odpowiadać dyscyplinarnie, administracyjnie[21], cywilnie lub karnie[22]. Należy dodać, że wnoszący o udzielenie

---

[17] Tamże, s. 57.

[18] Zob. szerzej: np. *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (t.j.: DzU z 2017 r. poz. 1932), art. 13 i art. 24 ust. 1 pkt 7.

[19] *Юридический энциклопедический словарь*, А.В. Малько (red.), Москва 2017, s. 397 (*Prawniczy słownik encyklopedyczny*, A.W. Malko (red.), Moskwa 2017).

[20] *Федеральный закон от 9 февраля 2009 г., № 8-ФЗ, „Об обеспечении доступа к информации о деятельности государственных органов…*, статья 23.2. „Если в результате неправомерного отказа в доступе к информации о деятельности государственных органов и органов местного самоуправления, либо несвоевременного ее предоставления, либо предоставления заведомо недостоверной или не соответствующей содержанию запроса информации пользователю информацией были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством Российской Федерации." (*Ustawa federalna z 9 lutego 2009 r. nr 8-FZ „O zapewnieniu dostępu do informacji o działalności organów państwowych…*", art. 23.2. „Jeżeli w wyniku bezprawnej odmowy dostępu do informacji o działalności organów państwowych i jednostek samorządu terytorialnego, ich nieterminowego podania lub podania umyślnie nieprawdziwych informacji lub informacji niezgodnych z treścią żądania, wyrządzono wnioskodawcy szkody, szkody te podlegają naprawieniu zgodnie z prawem cywilnym Federacji Rosyjskiej").

[21] Odpowiedzialność administracyjna urzędnika jest egzekwowana na podstawie przepisów federalnego kodeksu o wykroczeniach administracyjnych. Zob. *Федеральный закон от 30 декабря 2001 г., № 195-ФЗ, „Кодекс Российской Федерации об административных правонарушениях"* (*Ustawa federalna z 30 grudnia 2001 r. nr 195-FZ „Kodeks Federacji Rosyjskiej o wykroczeniach administracyjnych*").

[22] *Федеральный закон от 9 февраля 2009 г., № 8-ФЗ, „Об обеспечении доступа к информации о деятельности государственных органов…*, статья 25.: „Должностные

informacji w toku postępowania administracyjnego (również przed uzyskaniem rozstrzygnięcia) może złożyć skargę na czynności organu do Prokuratury Federalnej FR, która na podstawie art. 24 ust. 3 ustawy przywołanej na wstępie sprawuje urzędowy nadzór nad jej stosowaniem[23]. Szczegółowe uprawnienia prokuratury w odniesieniu do ochrony praw i wolności człowieka i obywatela, a więc również konstytucyjnego prawa do informacji, określono w artykułach 26–29 ustawy o prokuraturze FR[24]. W przypadku uzasadnionej skargi prokurator jest zobowiązany do ścigania urzędników, którzy złamali prawo, a na etapie sporu przed sądem administracyjnym może włączyć się do postępowania po stronie żądającego informacji, o czym stanowi art. 218 ust. 4 i art. 39 ust. 7 ustawy *Kodeks postępowania przed sądami administracyjnymi Federacji Rosyjskiej*[25].

Egzekwowanie prawa do informacji na szczeblu kolejnych instancji organów państwowych i samorządowych oraz przed sądem administracyjnym jest realizowane na podstawie art. 23 ust. 1[26] w związku z art. 8 ust. 4 tej ustawy. Wnoszenie odwołania od odmowy udzielenia informacji do organów drugiego stopnia odbywa się zgodnie

лица государственных органов и органов местного самоуправления, государственные и муниципальные служащие, виновные в нарушении права на доступ к информации о деятельности государственных органов и органов местного самоуправления, несут дисциплинарную, административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации" (*Ustawa federalna z 9 lutego 2009 r. nr 8-FZ „O zapewnieniu dostępu do informacji o działalności organów państwowych…"*, art. 25: „Urzędnicy organów państwowych i samorządowych, pracownicy państwowi i samorządowi winni naruszenia prawa dostępu do informacji o działalności organów państwowych i samorządowych ponoszą odpowiedzialność dyscyplinarną, administracyjną, cywilną i karną zgodnie z ustawodawstwem Federacji Rosyjskiej").

[23] Tamże, статья 24.3.: „Надзор за исполнением государственными органами, органами местного самоуправления, их должностными лицами настоящего Федерального закона осуществляют органы прокуратуры Российской Федерации в порядке, установленном Федеральным законом" «О прокуратуре Российской Федерации»" (tamże, art. 24.3.: „Nadzór nad wykonywaniem niniejszej Ustawy Federalnej przez organy państwowe, organy samorządu lokalnego i ich funkcjonariuszy sprawują organy Prokuratury Federacji Rosyjskiej w sposób określony w ustawie federalnej «O prokuraturze Federacji Rosyjskiej»").

[24] *Федеральный закон от 17 января 1992 г., № 2202-1, „О прокуратуре Российской Федерации"* (*Ustawa federalna z 17 stycznia 1992 r. nr 2202-1 „O prokuraturze Federacji Rosyjskiej"*).

[25] *Федеральный закон от 8 марта 2015, № 21-ФЗ, „Кодекс административного судопроизводства Российской Федерации"* (*Ustawa federalna z 8 marca 2015 r. nr 21-FZ „Kodeks postępowania przed sądami administracyjnymi Federacji Rosyjskiej"*).

[26] *Федеральный закон от 9 февраля 2009 г., № 8-ФЗ…*, статья 23.1. „Решения и действия (бездействие) государственных органов и органов местного самоуправления, их должностных лиц, нарушающие право на доступ к информации о деятельности государственных органов и органов местного самоуправления, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд" (*Ustawa federalna z 9 lutego 2009 r. nr 8-FZ…*, art. 23.1.: „Decyzje i działania (bezczynność) organów państwowych i samorządowych, ich urzędników, naruszające prawo dostępu do informacji o działalności organów państwowych i samorządu terytorialnego, mogą być zaskarżane do organów nadrzędnych lub wyższego urzędnika albo do sądu").

z ogólną procedurą określoną w ustawie federalnej o wnoszeniu odwołań[27], skargę do sądu administracyjnego wnosi się natomiast zgodnie z postanowieniami kodeksu postępowania przed sądami administracyjnymi[28].

Z powyższych rozważań wynika, że rosyjskie i polskie regulacje konstytucyjne w głównych postanowieniach są zbieżne: ustanawiają obywatelskie prawo do uzyskiwania informacji oraz do ich rozpowszechniania i jednocześnie wprowadzają przesłanki, które ograniczają obowiązek organów państwa w zakresie udzielania informacji obywatelom. Uszczegółowieniem norm konstytucyjnych są powszechnie obowiązujące ustawy, w których prawodawca sprecyzował sposób egzekwowania prawa do informacji oraz kategorie informacji niepodlegające udostępnieniu.

Karnoprawna ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane odniesienia do prawa polskiego

W celu wymuszenia przestrzegania przepisów o ochronie tajemnicy państwowej (informacji niejawnych) w RP ustanowiono odpowiednie instytucje prawa karnego, które wprowadzają sankcje karne za naruszenie bezpieczeństwa tajemnic. Rosyjskie prawodawstwo karne zalicza przestępstwa dotyczące tajemnicy państwowej do kategorii przestępstw skierowanych przeciwko bezpieczeństwu państwa. Polskie ustawodawstwo odeszło od tego rodzaju systematyki po wprowadzeniu kodeksu karnego z 1969 r., w którym przestępstwo przeciwko tajemnicy państwowej przyporządkowano do rozdziału XXXIV pt.: *Przestępstwa naruszenia tajemnicy państwowej i służbowej*. Należy wskazać, że aktualny kodeks karny RP z 1997 r.[29] zalicza przepisy karne sankcjonujące ujawnienie lub wykorzystanie informacji niejawnych do rozdziału XXXIII pt. *Przestępstwa przeciwko ochronie informacji*[30]. Kodeks karny FR (ros. *уголовный кодекс*, pis. fon. ugołownyj kodieks) w części szczególnej, w rozdziale X pt.:

---

[27] *Федеральный закон от 2 мая 2006 г., № 59-ФЗ, „О порядке рассмотрения обращений граждан Российской Федерации" (Ustawa federalna z 2 maja 2006 nr 59-FZ „O procedurze rozpatrywania odwołań obywateli Federacji Rosyjskiej*).

[28] *Федеральный закон „Кодекс административного судопроизводства…*

[29] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

[30] W związku z włączeniem przepisów karnych dotyczących przestępczego ujawnienia lub wykorzystania informacji niejawnych do rozdziału XXXIII pt. *Przestępstwa przeciwko ochronie informacji* powstało wiele opinii odnoszących się do normotwórczego charakteru tego tytułu i jego wpływu na wykładnię przepisów w nim zgrupowanych. Zob. szerzej: W. Wróbel, *Prawnokarna ochrona tajemnicy państwowej*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, s. 124 i nast.; M. Leciak, *Karnoprawna ochrona informacji niejawnych*, Toruń 2012, s. 125; W. Wróbel, *Pojęcie „dobra prawnego" w wykładni przepisów prawa karnego*, w: *Aktualne problemy prawa karnego. Księga pamiątkowa z okazji jubileuszu 70. urodzin profesora Andrzeja J. Szwarca*, Ł. Pohl (red.), Poznań 2009, s. 628–629; Uchwała Sądu Najwyższego z 26 IX 2002 r., I KZP 25/02, wskazująca między innymi na niekonsekwencję prawodawcy w grupowaniu przepisów karnych w rozdziały według kryterium dobra chronionego.

Przestępstwa przeciwko władzy państwowej, w podrozdziale 29 zatytułowanym *Przestępstwa przeciwko podstawom porządku konstytucyjnego i bezpieczeństwa państwa*, zawiera trzy jednostki redakcyjne: art. 283, art. 283[1] (z cyfrą „1") oraz art. 284[31]. Należy podkreślić, że kodeks w uchwalonej wersji nie zawierał art. 283[1], który został dodany nowelą numer 190-FZ z 12 listopada 2012 r.

Rozpowszechnianie tajemnicy państwowej jest spenalizowane w art. 283 kk FR[32]. Podmiot przestępstwa został tu określony jako indywidualny. Jest nim osoba, której powierzono określone tajemnice, lub osoba, która zapoznała się z tymi tajemnicami w związku z pełnieniem obowiązków służbowych, pracą albo nauką, a także w innych okolicznościach prawnie określonych przepisami Federacji Rosyjskiej. W rosyjskiej literaturze przedmiotu zwraca się uwagę na to, że nie tylko osoby mające legalny dostęp do tajemnicy państwowej stanowią potencjalny podmiot przestępstwa polegającego na jej ujawnieniu. Autorzy wskazują, że niektórzy pracownicy mogą mieć pośrednią styczność z tajemnicą w ramach wykonywanych obowiązków (np. pracownicy ochrony, kurierzy, kierowcy oraz personel pomocniczy w instytucjach przetwarzających tajemnice)[33].

Przedmiotem ochrony są informacje stanowiące tajemnicę państwową. Zarówno rosyjski kodeks karny, jak i polski - z 1997 r. (art. 265 i art. 266), nie zawierają definicji informacji, o których stanowią. Rosyjskie pojęcie „tajemnica państwowa" zostało określone w odrębnej ustawie, o czym będzie mowa w części artykułu dotyczącej rosyjskiego prawa administracyjnego, normującego zarządzanie tajemnicami. Przepisy karnego

---

[31] *Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями*, Законодательство Российской Федерации, Сборник основных федеральных законов РФ (*Kodeks karny Federacji Rosyjskiej z 13 czerwca 1996 r. nr 63-FZ, ze zmianami*, Prawodawstwo Federacji Rosyjskiej, Zbiór podstawowych ustaw federalnych FR); https://fzrf.su/kodeks/uk/ [dostęp: 9 II 2021].

[32] Tamże, статья 283.1.: „Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, если эти сведения стали достоянием других лиц, при отсутствии признаков преступлений, предусмотренных статьями 275 и 276 настоящего Кодекса - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового" (tamże, art. 283.1.: „Rozpowszechnianie informacji stanowiących tajemnicę państwową przez osobę, której je powierzono lub stały się jej znane w związku z pełnieniem obowiązków służbowych, pracą, nauką lub w innych przypadkach, przewidzianych ustawodawstwem Federacji Rosyjskiej, jeżeli te informacje stały się znane innym osobom, przy braku znamion przestępstw przewidzianych w artykułach 275 i 276 niniejszego kodeksu – skazuje się (zagrożone jest) karą aresztu na okres od czterech do sześciu miesięcy albo na karę pozbawienia wolności na okres do czterech lat z pozbawieniem prawa do zajmowania określonych stanowisk lub zajmowania się określoną działalnością na okres do trzech lat, lub bez tego" (tj. bez zastosowania dodatkowych środków karnych).

[33] Zob. szerzej: В.М. Лебедев, *Уголовный кодекс Российской Федерации с научно-практическим комментарием*, Варшава 1997, s. 543 i nast. (W.M. Lebiediew, *Kodeks karny Federacji Rosyjskiej z naukowo-praktycznymi komentarzami*, Warszawa 1997, s. 543 i nast.).

prawa materialnego w Rosji, podobnie jak i w Polsce, są w tej części blankietowe[34]. To oznacza konieczność poszukiwania adekwatnych definicji terminów użytych do ich konstrukcji w innych powszechnie obowiązujących aktach prawnych.

W rosyjskim prawodawstwie strona przedmiotowa (czynność sprawcza) polega na „rozpowszechnianiu" tajemnicy państwowej, czyli czasownikowej formie dokonanej. Przestępstwo jest znamienne skutkiem (jest przestępstwem materialnym) w postaci intelektualnego zapoznania się z ujawnionymi treściami przez inną osobę. Istota rozpowszechnienia, w polskim prawodawstwie określana jako ujawnienie, zawiera się w udostępnieniu danej tajemnicy innej osobie. W rosyjskim piśmiennictwie zwraca się uwagę na sposób rozpowszechniania, przyjmując, że każda bezprawna forma zastosowana przez sprawcę, która skutkuje ujawnieniem tajemnicy wobec innej osoby, wypełnia to znamię. Ponadto osoba nieuprawniona jest charakteryzowana jako osoba nieposiadająca legalnego dostępu do tajemnicy państwowej, a także jako osoba, która ma dostęp do tajemnicy państwowej, ale zapoznaje się z informacją niepowiązaną z zajmowanym stanowiskiem czy pełnioną funkcją[35]. Rosyjski ustawodawca w treści przepisu wprowadza zastrzeżenie, że za rozpowszechnianie tajemnicy sprawca ponosi odpowiedzialność przewidzianą w tym przepisie, o ile swoim czynem nie wypełnił znamion przestępstwa szpiegostwa albo zdrady stanu. Wymienione przestępstwa różnią się od rozpowszechniania tajemnicy zamiarem, znamiona zdrady lub szpiegostwa bowiem zostają spełnione jedynie wówczas, gdy sprawca jest świadomy, że przekazuje tajemnice obcemu państwu, organizacji międzynarodowej albo obcej organizacji lub ich przedstawicielstwom w celu wykorzystania tych tajemnic przeciwko bezpieczeństwu FR.

Omawiane przestępstwo można popełnić tylko umyślnie, w zamiarze bezpośrednim (ros. *непосредственный* – bezpośredni) lub pośrednim (ros. *косвенный* - pośredni), który w polskim piśmiennictwie jest nazywany „ewentualnym". Rosyjska doktryna prawa karnego przewiduje możliwość sprawstwa również przez zaniechanie - jako przykład podaje się urzędnika, który pozostawia niezabezpieczone tajne

---

[34] Igor Andrejew definiuje, że przepisy blankietowe to przepisy, które nie zawierają pełnego opisu czynu zabronionego. Dodatkowo zauważa, że ustawodawca w ich treści nie odsyła do innego przepisu kodeksu lub innego konkretnego aktu, lecz „(…) powołuje się tylko na nieokreślone ustawy, rozporządzenia lub inne akty normatywne, na których podstawie należy ustalić, na czym polega dany czyn zabroniony" (I. Andrejew, *Polskie prawo karne w zarysie*, Warszawa 1989, s. 76). Uwagi o problemach w rekonstrukcji normy karnej, wynikających z przepisów blankietowych, czyni również Ryszard Dębski. Jako przykład ekstremalny przywołuje konieczność zastosowania w toku tego procesu reguł nieprawnokarnych, które są formułowane nieco inaczej niż opisy czynów zabronionych. Wskazuje, że trudności w recepcji tych przepisów wynikają przede wszystkim z ich nieprecyzyjnej konstrukcji – braku jednoznaczności, która jest wymagana w prawie karnym. Autor dostrzega dodatkowe problemy interpretacyjne wynikające z zastosowania przez ustawodawcę „blankietu ogólnego", który należy wypełnić, tj. odszukać i zastosować znamiona ustanowione w wielu innych aktach. Podsumowuje, że czyni to przepis karny mało czytelnym i może naruszać funkcję gwarancyjną, która polega na „przewidywalności" reakcji karnej na zachowanie opisane prawem karnym (R. Dębski, *Pozaustawowe znamiona przestępstwa*, Łódź 1995, s. 118).

[35] В.М. Лебедев, *Уголовный кодекс Российской Федерации*…, s. 542.

dokumenty[36]. Istotną różnicą między art. 283 kk FR i art. 265 § 1 kk RP jest podmiotowy zakres zakazu karnego: w regulacji rosyjskiej podmiotem przestępstwa mogą być osoby mające szczególne uprawnienia (podmiot indywidualny), a w polskiej - każdy (podmiot powszechny). Polski przepis penalizuje ponadto nie tylko ujawnienie, lecz także nieuprawnione wykorzystanie tajemnic.

Rodzajów kar przyjętych przez rosyjskiego prawodawcę jest więcej niż przyjętych przez polskiego prawodawcę. Czyn polegający na rozpowszechnianiu tajemnicy państwowej w typie podstawowym jest zagrożony karą aresztu na okres od czterech do sześciu miesięcy albo karę pozbawienia wolności do czterech lat, z możliwością orzeczenia pozbawienia prawa do zajmowania określonych stanowisk albo zajmowania się określoną działalnością na okres do trzech lat. Warto zauważyć, że zastosowanie przez sąd RP środków karnych we wskazanej postaci na podstawie art. 41 kk RP nie jest wykluczone, orzeczenie kary aresztu jest jednak niemożliwe.

W rosyjskim prawie karnym zaostrzenie odpowiedzialności za bezprawne rozpowszechnianie tajemnic następuje wówczas, gdy czyn zaistniał z powodu nieostrożności i wywołał ciężkie następstwa[37]. Polskim odpowiednikiem tej formy winy jest nieumyślność (art. 9 ust. 2 kk z 1997 r.[38]). W Federacji Rosyjskiej rozróżnia się rodzaje nieostrożności w postaci lekkomyślności albo niedbalstwa (art. 26 ust. 1 kk FR), podobnie jak rozróżniał to polski kodeks karny z 1969 r. W przypadku wywołania ciężkich następstw spowodowanych powyższymi zaniedbaniami ustawodawca zwiększa okres kary izolacyjnej przez podwyższenie jej dolnego i górnego wymiaru, odpowiednio od trzech do siedmiu lat. Przepis wprowadza dodatkowo obowiązkowe orzeczenie zakazu zajmowania określonych stanowisk lub prowadzenia określonej działalności na okres do trzech lat. Zwiększone sankcjonowanie nieostrożności powodującej ciężkie następstwa czynu może zaskakiwać. Należy jednak uwzględnić, że kodeks karny FR w art. 27[39] przewiduje

---

[36] А.Б. Борисов, *Комментарий к уголовному кодексу*…, s. 681 i nast. (A.B. Borisow, *Komentarz do kodeksu karnego*…, s. 681 i nast.).

[37] *Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями*…, статья 283.2.: „То же деяние, повлекшее по неосторожности тяжкие последствия – наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет" (*Kodeks karny Federacji Rosyjskiej*…, art. 283.2.: „Za ten czyn, który z powodu nieostrożności spowodował ciężkie następstwa – skazuje się na karę pozbawienia wolności na okres od trzech do siedmiu lat z pozbawieniem prawa do zajmowania określonych stanowisk lub zajmowania się określoną działalnością na okres do trzech lat").

[38] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*…

[39] *Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями*…, статья 27.: „Если в результате совершения умышленного преступления причиняются тяжкие последствия, которые по закону влекут более строгое наказание и которые не охватывались умыслом лица, уголовная ответственность за такие последствия наступает только в случае, если лицо предвидело возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывало на их предотвращение, или в случае, если лицо не предвидело, но должно было и могло предвидеть возможность наступления этих последствий. В целом такое преступление признается совершенным умышленно" (*Kodeks karny Federacji*

odpowiedzialność za popełnienie czynu z podwójnym zawinieniem, tj. winą umyślną i nieumyślną (ros. *неосторожность* - nieostrożność). Zaostrzona odpowiedzialność jest spowodowana kwalifikowaniem czynu ze względu na jego następstwa. Jest to forma winy mieszanej, stanowiąca odpowiednik opisany w art. 9 § 3 polskiego kodeksu karnego z 1997 r. Zgodnie z art. 15 ust. 3 i 4 kk FR przestępstwo z art. 283 ust. 1 jest zaliczane do średnio ciężkich, a z ust. 2 do ciężkich, co ma wpływ na sądowy wymiar kary. Sąd może wziąć pod uwagę faktyczne okoliczności czynu i spowodowany przez niego stopień publicznego niebezpieczeństwa (czego odpowiednikiem w RP jest społeczna szkodliwość czynu) i orzec wymiar kary przewidziany dla przestępstw tylko o jeden stopień lżejszych. Na marginesie należy zauważyć, że w stosunku do art. 283, art. 283^1 i 284 organem właściwym do prowadzenia postępowania przygotowawczego jest Federalna Służba Bezpieczeństwa (dalej: FSB)[40].

Kolejnym przestępstwem zagrażającym bezpieczeństwu FR jest bezprawne uzyskanie informacji stanowiących tajemnicę państwową (art. 283^1 kk FR[41]). Karnoprawnym zakazem został objęty czyn umyślny polegający na nielegalnym wejściu w posiadanie tajemnicy państwowej w wyniku: kradzieży, oszustwa, szantażu, zmuszenia, groźby użycia przemocy lub w inny bezprawny sposób. Normodawca określił podmiot przestępstwa jako powszechny – przepis nie stanowi o osobowym ograniczeniu sprawstwa. Przedmiot ochrony jest tożsamy z przyjętym w art. 283.

Strona przedmiotowa czynu zabronionego jest rozbudowana, sprawca zmierzający do uzyskania informacji nie wypełnia znamion, jeśli stosuje środki prawnie dopuszczalne. Jeżeli osiągnięcie celu następuje w wyniku zastosowania sposobów zabronionych, chociażby jednego z wyżej wymienionych, wówczas zostaje naruszona norma

---

Rosyjskiej…, art. 27.: „Jeżeli wskutek popełnienia przestępstwa umyślnego dojdzie do poważnych następstw, które zgodnie z prawem pociągają za sobą surowszą karę i które nie były objęte zamiarem osoby, odpowiedzialność karna za takie następstwa powstaje tylko w przypadku, gdy dana osoba przewidywała możliwość ich wystąpienia, ale bez dostatecznych podstaw lekkomyślnie sądziła, że im zapobiegnie albo w przypadku, gdy dana osoba nie przewidywała, ale powinna i mogła przewidzieć możliwość wystąpienia takich następstw. Takie przestępstwo uznaje się za popełnione umyślnie").

[40] О.О. Скоробогатова, С.А. Перчаткина, *Уголовный кодекс Российской Федерации с комментариями*, Москва 2012, s. 234 (O.O. Skorobogatowa, S.A. Pierczatkina, *Kodeks karny Federacji Rosyjskiej z komentarzami*, Moskwa 2012).

[41] *Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями*…, статья 283^1.1.: „Получение сведений, составляющих государственную тайну, путем похищения, обмана, шантажа, принуждения, угрозы применения насилия либо иным незаконным способом (при отсутствии признаков преступлений, предусмотренных статьями 275 и 276 настоящего Кодекса) – наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до четырех лет" (*Kodeks karny Federacji Rosyjskiej*…, art. 283^1.1.: „Za uzyskanie informacji stanowiących tajemnicę państwową drogą kradzieży, oszustwa, szantażu, zmuszenia, groźby użycia przemocy lub innym bezprawnym sposobem (przy braku znamion przestępstw przewidzianych w artykułach 275 i 276 niniejszego kodeksu) – skazuje się na karę grzywny w wysokości od dwustu tysięcy do pięciuset tysięcy rubli lub w wysokości wynagrodzenia za pracę, lub innego dochodu skazanego, za okres od jednego roku do trzech lat albo na karę pozbawienia wolności na okres do czterech lat").

zakazu karnego. Jak trafnie zauważa Jurij Pudowoczkin, przy ocenie bezprawności uzyskania tajemnicy państwowej należy opierać się na przepisach materialnych prawa karnego oraz regulacjach ustawy z 21 lipca 1993 r. o tajemnicy państwowej[42]. Rosyjski prawodawca warunkuje odpowiedzialność karną z art. 283[1] kk FR brakiem wypełnienia znamion przestępstw z art. 275 (zdrada) i art. 272 kk FR (szpiegostwo). Zagrożenie karą jest przemienne, sąd może orzec karę pozbawienia wolności na okres do czterech lat albo grzywnę w wysokości od 200 tys. do 500 tys. rubli, z możliwością oznaczenia jej wysokości krotnością wynagrodzenia za pracę lub innego dochodu za okres od jednego roku do trzech lat.

W ustępie drugim omawianego przepisu sklasyfikowano przestępstwo według sposobu jego popełnienia lub jego określonego skutku[43]. Ustawodawca podwyższa górną granicę odpowiedzialności karnej z czterech do ośmiu lat pozbawienia wolności, jeżeli czyn został popełniony: przez grupę osób, z użyciem przemocy, z wykorzystaniem specjalnych środków technicznych i innych środków przeznaczonych do niejawnego uzyskiwania informacji, spowodował ciężkie następstwa, był związany z rozpowszechnianiem tajemnicy państwowej albo z przekazaniem nośników tajemnicy państwowej poza granice FR. Zagrożenie karą zmienia stopień przestępstwa ze średniego na ciężkie.

Na uwagę zasługuje generalna norma zakazu ustanowiona art. 283[1] ust. 1, sankcjonowaniu karnemu podlega bowiem uzyskanie informacji stanowiących tajemnicę państwową, nawet bez ich wykorzystania lub ujawnienia. Podstawowym skutkiem jest więc uzyskanie niejawnych informacji, typ kwalifikowany tego przestępstwa natomiast jest determinowany jego określonym rezultatem, np. ciężkimi następstwami godzącymi w bezpieczeństwo państwa albo sposobem sprawstwa. Odwołując się do historii, należy stwierdzić, że w przeszłości w polskim prawodawstwie istniały podobne

---

[42] Ю.Е. Пудовочкин, *Преступления против государственной власти*, в: *Комментарий к Уголовному кодексу Российской Федерации*, t. 2, А.В. Бриллиантов (red.), Москва 2017, s. 376 (E. Pudowoczkin, *Przestępstwa przeciwko władzy państwowej*, w: *Komentarz do Kodeksu karnego Federacji Rosyjskiej*, t. 2, A.W. Briliantow (red.), Moskwa 2017).

[43] *Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями*…, статья 283[1].2.: „То же деяние, если оно:
а) совершено группой лиц;
б) совершено с применением насилия;
в) повлекло наступление тяжких последствий;
г) совершено с использованием специальных и иных технических средств предназначенных для негласного получения информации;
д) сопряжено с распространением сведений, составляющих государственную тайну, либо с перемещением носителей таких сведений за пределы Российской Федерации – наказывается лишением свободы на срок от трех до восьми лет" (*Kodeks karny Federacji Rosyjskiej*…, art. 283[1].2.: „Za ten czyn, jeżeli: a) został on popełniony przez grupę osób, b) został popełniony z użyciem przemocy, w) spowodował ciężkie następstwa, g) został popełniony z wykorzystaniem specjalnych i innych środków technicznych przeznaczonych do niejawnego uzyskania informacji, d) był związany z rozpowszechnieniem informacji stanowiących tajemnicę państwową lub z przekazaniem nośników takich informacji poza granice Federacji Rosyjskiej – skazuje się na karę pozbawienia wolności na okres od trzech do ośmiu lat").

przepisy[44]. Penalizacji bezprawnego uzyskiwania (gromadzenia) tajemnicy państwowej zaprzestano wraz z wprowadzeniem kodeksu karnego z 1969 r. Aktualnie tego rodzaju czyn może skutkować odpowiedzialnością z art. 267 § 1 kk, który sankcjonuje nielegalne uzyskanie informacji[45].

Ostatnim przepisem wprowadzającym karnoprawną ochronę tajemnic Federacji Rosyjskiej jest art. 284 kk FR[46]. Kryminalizuje on utratę dokumentów stanowiących tajemnicę państwową albo przedmiotów chronionych taką tajemnicą w wyniku naruszenia zasad tej ochrony przez legalnego dysponenta. Podmiot przestępstwa został określony indywidualnie – jest nim osoba uprawniona do dostępu do tajemnicy państwowej i będąca w posiadaniu danych tajemnic zgodnie z uprawnieniami. Borisow wyszczególnia rodzajowy przedmiot ochrony, który określa jako właściwe funkcjonowanie władz państwowych, oraz indywidualny przedmiot ochrony, którym jest bezpieczeństwo państwa[47].

Strona podmiotowa jest złożona, tj. umyślno-nieumyślna. W odniesieniu do naruszenia przepisów określających zasady ochrony utraconych nośników sprawca działa w zamiarze bezpośrednim lub ewentualnym (przyjmuje się, że osoba mająca legalny dostęp do informacji niejawnych ma odpowiednią wiedzę w zakresie zasad ochrony

---

[44] *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciw Państwu* (DzU z 1928 r. nr 18 poz. 160), art. 5; *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu Państwa* (DzU z 1934 r. nr 94 poz. 851), art. 15; *Dekret z dnia 16 listopada 1945 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa* (DzU z 1945 r. nr 53 poz. 300), art. 8; *Dekret z dnia 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa* (DzU z 1946 r. nr 30 poz. 192), art. 7; *Dekret z dnia 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej* (DzU z 1949 r. nr 55 poz. 437), art. 3 i 4.

[45] B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości*, Warszawa 2000, s. 428; A. Marek, *Prawo karne*, Warszawa 2016, s. 688; M. Leciak, *Karnoprawna ochrona informacji*…, s. 253.

[46] *Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями*…, статья 284: „Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, ‑ наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового" (*Kodeks karny Federacji Rosyjskiej*…, art. 284.: „Za naruszenie ustanowionych zasad obchodzenia się z dokumentami zawierającymi tajemnicę państwową, jak i z przedmiotami, o których informacje stanowią tajemnicę państwową, przez osobę mającą dostęp do tajemnicy państwowej, jeżeli z powodu nieostrożności spowodowało to ich utratę i ciężkie następstwa – skazuje się na karę ograniczenia wolności na okres do trzech lat albo na karę aresztu na okres od czterech do sześciu miesięcy, albo na karę pozbawienia wolności na okres do trzech lat z pozbawieniem prawa do zajmowania określonych stanowisk lub prowadzenia określonej działalności na okres do trzech lat lub bez tego" (tj. bez zastosowania środków karnych).

[47] Zob. szerzej: А.Б. Борисов, *Комментарий к уголовному кодексу*…, s. 683 i nast. (A.B. Borisow, *Komentarz do kodeksu karnego*…, s. 683 i nast.).

tych informacji i umyślnie od nich odstępuje). Nieumyślność (ros. *неосторожность* – nieostrożność) jest związana z lekkomyślnym przekonaniem, że naruszenie przepisów nie spowoduje utraty nośników informacji i ciężkich następstw. Skutkiem czynu zabronionego jest utrata dokumentów, które są nośnikami tajemnicy państwowej, albo przedmiotów, z którymi taka tajemnica jest związana. Warunkiem odpowiedzialności jest spowodowanie ciężkich następstw godzących w bezpieczeństwo FR. Pojęcie ciężkie następstwa nie jest zdefiniowane w rosyjskim prawodawstwie. Według Borisowa zaliczenie skutków do ciężkich zawsze pozostaje w gestii sądu, który rozważa szczególnie utratę tajemnicy na rzecz obcych wywiadów oraz szkodę materialną w dużych rozmiarach. Dla wypełnienia znamion czynu jest konieczne zaistnienie związku przyczynowo-skutkowego. Utrata informacji stanowiących tajemnicę państwową, zawartych w dokumentach, albo przedmiotów, z którymi tajemnica jest związana, musi wynikać z naruszenia konkretnych przepisów dotyczących sposobu ochrony utraconych nośników tajemnicy, które należy traktować jako przedmiot wykonawczy tego przestępstwa.

Rosyjski kodeks karny przewiduje następujące rodzaje kar za przestępstwo utraty tajemnicy państwowej: ograniczenie wolności na okres do trzech lat, areszt na okres od czterech do sześciu miesięcy, pozbawienie wolności na okres do trzech lat z fakultatywnym orzeczeniem zakazu zajmowania określonych stanowisk lub prowadzenia określonej działalności na okres do trzech lat.

Przepisy wprowadzające odpowiedzialność karną za utratę dokumentu lub innego przedmiotu stanowiącego tajemnicę państwową, a także za naruszenie zarządzeń określających ich ochronę, obowiązywały w Polsce do dnia wprowadzenia kodeksu karnego z 1997 r. Był to art. 262 i art. 263 kk z 1969 r.[48] W aktualnym stanie prawnym utrata niejawnych dokumentów lub materiałów oraz naruszenie zasad ochrony nie są penalizowane w art. 265 kk lub 266 kk, o ile nie doprowadziły do ujawnienia albo wykorzystania informacji wskazanych w ich treści[49]. Możliwa jest oczywiście odpowiedzialność karna z powyższych artykułów nawet bez przestępnego dokonania czynu, przy uwzględnieniu formy stadialnej, tj. usiłowania[50], oraz niesprawczych postaci zjawiskowych[51] (podżegania i pomocnictwa). Skomplikowanym stanem faktycznym, powodującym złożoną kwalifikację prawną czynu, mogłoby być zaniechanie obowiązków przez funkcjonariusza, który na mocy art. 2 kk jest gwarantem nienastąpienia skutku. W wyniku niedopełnienia obowiązków funkcjonariusz publiczny może bowiem spowodować zniszczenie materiału niejawnego lub uniemożliwić odtworzenie informacji niejawnych w akredytowanym systemie informatycznym (przeznaczonym

---

[48] B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji*…, s. 443.

[49] M. Leciak, *Tajemnica państwowa i jej ochrona*, Toruń 2009, s. 219.

[50] Tenże, *Karnoprawna ochrona informacji*…, s. 228.

[51] Zob. szerzej: B.J. Stefańska, *Formy popełnienia przestępstwa*, w: *Kodeks karny. Komentarz*, R. Stefański (red.), Warszawa 2015, s. 219 i nast.; K. Buchała, A. Zoll, *Kodeks karny. Część ogólna*, Kraków 1998, s. 84–88.

do przetwarzania tajemnic). Wówczas, w ocenie autora artykułu, kumulatywna kwalifikacja czynu będzie obejmowała opcjonalnie popełnienie przestępstwa z art. 231 kk w zbiegu z art. 268 kk (268a kk) w związku z art. 2 kk[52] (przy założeniu, że nie dochodzi do ujawnienia lub wykorzystania informacji niejawnych)[53].

Analiza aktualnych przepisów karnych Federacji Rosyjskiej oraz Rzeczpospolitej Polskiej prowadzi do wniosku, że mimo początkowej jedności norm zakazu karnego w obu krajach system prawnokarnej ochrony informacji niejawnych (tajemnic) obowiązujący w Polsce jest mniej represyjny niż obowiązujący w Rosji. Na szczególną uwagę zasługuje art. 283[1] kk FR, który nie ma odpowiednika w polskim prawie karnym. Nie sprzyja to prewencji kryminalnej i zwalczaniu przestępstw groźnych dla bezpieczeństwa państwa. Niskie zagrożenie karą za popełnienie przestępstwa z art. 267 kk RP nie jest adekwatne do zagrożeń wynikających z nielegalnego uzyskiwania informacji ściśle tajnych czy tajnych, bez względu na ich późniejsze przeznaczenie przez sprawcę. Należy zatem postulować objęcie w przyszłości tego społecznie groźnego zachowania zakazem karnomaterialnym.

Istotne elementy pozakodeksowego systemu ochrony tajemnic w Rosji

Zarówno rosyjskie, jak i polskie przepisy karne penalizujące czyny, które naruszają bezpieczeństwo tajemnic, mają charakter blankietowy. Zdekodowanie norm zakazu karnego w celu ustalenia wypełniania znamion przestępstw może nastąpić wyłącznie dzięki zastosowaniu pojęć prawa federalnego, tj. ustawy o tajemnicy państwowej FR (ros. *закон о государственной тайне*, pis. fon. zakon o gosudarstwiennoj tajnie)[54]. W preambule do tej ustawy prawodawca stanowi, że reguluje ona stosunki, które powstają w związku

---

[52] Podjęte rozważania przekraczają ramy niniejszego artykułu, warto jednak dodać, że nie każde zaniechanie (niedopełnienie obowiązków), w którego wyniku następuje dokonanie przestępstwa skutkowego, np. zniszczenie materiału objętego tajemnicą, wypełnia znamiona przestępstwa. Jak trafnie zauważa Łukasz Pohl, „Nie każde niewykonane działanie jest działaniem zaniechanym" (Ł. Pohl, *Zasady odpowiedzialności karnej*…, s. 52). Zazwyczaj należy rozważyć trzy istotne aspekty: czy gwarant nienastąpienia skutku miał intelektualne możliwości oceny danej sytuacji, w której nie zapobiegł skutkowi, czy okoliczności występujące w miejscu i czasie, w których był zobowiązany podjąć działanie, spowodowały, że zaniechał tego działania i wreszcie, czy niemożność działania była spowodowana wcześniejszym wytworzeniem przez gwaranta takich przeszkód, które spowodowały zaniechanie z jego strony. Rozważenie tych kwestii wymaga zbadania dwóch aspektów: aspekt pierwszy – czy zaniechanie miało charakter wolicjonalny, aspekt drugi – czy wynikało ono z przyczyn niezależnych od sprawcy zaniechania albo przeszkód, których mimo podjęcia aktywności nie pokonał, co w rezultacie doprowadziło do nastąpienia skutku. Jak słusznie zauważa cytowany autor, nikt nie ma obowiązku czynienia rzeczy niemożliwych (łac. *impossibilium nulla obligatio est* - niemożliwe unicestwia obowiązek).

[53] B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji*…, s. 619 i nast.; S. Hoc, *Karnoprawna ochrona informacji*, Opole 2009, s. 103 i nast.

[54] *Закон Российской Федерации от 21 июля 1993 г., №5485-1, „О государственной тайне"* (*Ustawa Federacji Rosyjskiej z 21 lipca 1993 r. nr 5485-1 „O tajemnicy państwowej"*).

z klasyfikacją informacji jako tajemnicy państwowej, utajnianiem i odtajnianiem informacji oraz ochroną informacji w celu zapewnienia bezpieczeństwa FR.

W artykule pierwszym wymienionej ustawy określono zakres jej stosowania według właściwości terytorialnej (obowiązuje na terytorium FR i poza jej granicami) oraz kompetencji podmiotowej. Adresatami ustawy są urzędnicy oraz obywatele, którzy przyjęli na siebie obowiązek przestrzegania jej postanowień albo co do których ten obowiązek wynika z ich statusu. Akt odnosi się dodatkowo do osób prawnych (instytucji), abstrakcyjnie zdefiniowanych jako: władze publiczne, samorząd terytorialny, przedsiębiorstwa, instytucje i organizacje – niezależnie od ich formy organizacyjnej oraz prawnej i stosunków własnościowych. Określenie właściwości podmiotowej przez rodzajowe wyliczenie osób i instytucji pozwala na stwierdzenie, że ustawa, o której mowa, nie ma zasięgu powszechnego, co jest zbieżne z odpowiednią regulacją RP (podmioty, do których jest adresowana *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, zostały wyliczone w jej art. 1 ust 2).

Ważną wskazówką dotyczącą rozszerzenia obowiązywania ustawy o tajemnicy państwowej FR jest klauzula ustanowiona w art. 3, w którym rosyjski prawodawca nakazuje jej stosowanie odpowiednio do ustawy o bezpieczeństwie Federacji Rosyjskiej[55] oraz innych ustaw, których przepisy dotyczą tajemnicy państwowej.

Definicje legalne pojęć użytych w ustawie zawiera art. 2. Z punktu widzenia odpowiedzialności karnej najistotniejsza jest definicja pojęcia „tajemnica państwowa". Przez to pojęcie rozumie się informacje chronione przez państwo, dotyczące jego działań: wojskowych, międzynarodowych, gospodarczych, wywiadowczych, kontrwywiadowczych i operacyjno-rozpoznawczych. Rozpowszechnianie tych informacji może zaszkodzić bezpieczeństwu FR. Z tego wynika, że o uznaniu informacji z wymienionych dziedzin za tajemnicę przesądza kryterium groźby wystąpienia szkody. Zastosowana materialnoprawna konstrukcja definicji jest co do zasady zbieżna z polskim rozumieniem informacji niejawnych. Rosyjski prawodawca ustanowił wykaz informacji, które stanowią tajemnicę państwową, w art. 5 ustawy o tajemnicy państwowej i podzielił je według zagadnień wskazanych w przywołanej definicji.

Uzupełnieniem definicji pojęcia „tajemnica państwowa" i wykazu informacji stanowiących tego rodzaju tajemnicę, zawartego w art. 5 wymienionej ustawy, jest sporządzany przez Prezydenta FR spis dziedzin, z których informacje (z uwagi na ich charakter) stanowią tajemnicę państwową, oraz rejestr organów uprawnionych do zarządzania nimi. Od 1995 r. wykazy są publikowane łącznie w formie dekretu (ros. *указ Президента РФ*, pis. fon. ukaz Priezidienta RF)[56] i okresowo uzupełniane. Ostatnie zmiany wprowadzono 8 czerwca 2020 r. Aktualny dekret jest bardzo rozbudowany,

---

[55] *Федеральный закон от 28 декабря 2010, № 390-ФЗ, „О безопасности"* (*Ustawa federalna z 28 grudnia 2010 r. nr 390-FZ „O bezpieczeństwie"*).

[56] *Указ Президента РФ от 30 ноября 1995 г., № 1203, „Об утверждении перечня сведений…* (*Dekret Prezydenta FR z 30 listopada 1995 r. nr 1203 „O zatwierdzeniu wykazu informacji…*).

wymienia m.in. następujące dziedziny i jednocześnie organy uprawnione do zarządzania informacjami, które funkcjonalnie są z nimi związane:

1) wojskowość – informacje dotyczące głównie: planów strategicznych, uzbrojenia, mobilizacji, gotowości i liczebności armii, użycia Sił Zbrojnych FR, operacji antyterrorystycznych, broni atomowej, programów naukowo-badawczych, łączności i częstotliwości radiowych, działań w kosmosie, międzynarodowej polityki w dziedzinie bezpieczeństwa (łącznie 28 szczegółowych obszarów); organy powiązane to: Ministerstwo Spraw Wewnętrznych, Ministerstwo Obrony FR, Ministerstwo Obrony Cywilnej, Federalna Agencja Rządowej Łączności i Informacji, Służba Graniczna Federalnej Służby Bezpieczeństwa FR, Rosatom[57], Roskosmos[58] i inne;
2) ekonomia, nauka i technologie (łącznie 40 szczegółowych dziedzin); organy powiązane to głównie ministerstwa: Obrony, Spraw Wewnętrznych, Rozwoju Cyfryzacji i Łączności oraz Komunikacji Masowej, Spraw Zagranicznych, Spraw Nadzwyczajnych, Transportu i in.;
3) polityka zagraniczna i gospodarka – informacje dotyczące głównie: strategii prowadzenia przez Rosję polityki zagranicznej między innymi w zakresie handlu paliwami, minerałami (metalami szlachetnymi) i bronią, umów dotyczących zbrojnego wsparcia innych państw, gospodarki finansowej (monetarnej), wywiadu, kontrwywiadu i czynności operacyjno-rozpoznawczych, sposobu ochrony i stanu tajemnic, kryptografii, finansowania wywiadu i kontrwywiadu, zwalczania obcych wywiadów i współpracy z nimi, danych personalnych własnej agentury i jej uplasowania w organach innych państw lub w zagranicznych grupach przestępczych, danych dotyczących rzeczywistego stanu i organizacji obrony oraz innych zagadnień (łącznie 45 rozbudowanych dziedzin); organy powiązane to: Służba Wywiadu Zagranicznego, Federalna Służba Kontroli Technicznej i Transportu, Ministerstwo Spraw Wewnętrznych, Ministerstwo Obrony FR, Ministerstwo Obrony Cywilnej, Federalna Agencja Rządowej Łączności i Informacji, Służba Graniczna Federalnej Służby Bezpieczeństwa FR, Federalna Służba Bezpieczeństwa, Służba Bezpieczeństwa Prezydenta FR, Główny Zarząd Bezpieczeństwa Ministerstwa Spraw Zagranicznych, Główny Zarząd ds. Operacji Specjalnych Prezydenta Rosji i inne.

Należy nadmienić, że dziedziny wymienione w dekrecie odpowiadają dziedzinom wskazanym w definicji tajemnicy państwowej, każda z nich jednak jest uszczegółowiona przez określenie kolejnych zagadnień tematycznych, którymi się zajmuje. W wyniku sprecyzowania dziedzin i podmiotów uprawnionych do zarządzania danego rodzaju informacjami istnieje możliwość dookreślenia odesłania zawartego w art. 29 ust. 4

[57] Rosyjska Państwowa Korporacja Energii Atomowej „Rosatom", https://rosatom.ru/about/ [dostęp: 30 VII 2020].

[58] Rosyjska Państwowa Korporacja Rozwoju Technologii Kosmicznych „Roskosmos", https://www.roscosmos.ru/25919/ [dostęp: 30 VII 2020].

Konstytucji FR oraz w art. 5 ustawy o tajemnicy państwowej. Warto zasygnalizować, że polskie prawodawstwo odeszło od konstruowania wykazów informacji stanowiących określoną tajemnicę wraz z wprowadzeniem do obrotu prawnego ustawy o ochronie informacji niejawnych z 2010 r.

Interesującym rozwiązaniem legislacyjnym zastosowanym w rosyjskiej ustawie jest określenie obowiązków i uprawnień najważniejszych organów państwa w zakresie ochrony, administrowania i oddziaływania na system prawny z uwagi na bezpieczeństwo tajemnic (art. 4). Organami zobowiązanymi są m.in. Prezydent FR (szczególnie do wydawania dekretów wykonawczych) oraz organy władzy sądowniczej, które rozpatrują sprawy karne, cywilne i administracyjne dotyczące naruszeń tajemnicy oraz mają zapewnić przestrzeganie tajemnicy we własnych strukturach.

Istotną regulacją, o której stanowi rosyjska ustawa, zbieżną w dużym zakresie z przepisami polskimi, jest nakaz klauzulowania informacji. Kryterium klasyfikacyjne tajemnicy wprowadza art. 8, wskazujący, że stopień klauzuli (poziom ochrony) powinien być adekwatny do rozmiaru szkody, jaką może ponieść FR w związku z rozpowszechnieniem (upublicznieniem) danej informacji. Należy zauważyć, że przepis stanowi o klauzulowaniu nośników informacji (a więc formy zmaterializowanej), a nie samej informacji, jak ma to miejsce w ustawie polskiej. Wspomniany przepis wprowadza trzy stopnie ochrony tajemnicy informacji, do których są przypisane klauzule tajności (ros. *грифы*, pis. fon. grify): *Особой важности* (pol. „O szczególnym znaczeniu"), *Совершенно секретно* (pol. „Ściśle tajne") i *Секретно* (pol. „Tajne"). Jednocześnie ustawodawca deleguje obowiązek uszczegółowienia zasad klasyfikowania informacji do danego stopnia tajności, tj. klauzuli, rządowi FR. Wprowadza również zakaz stosowania wymienionych klauzul do oznaczania informacji, które nie stanowią tajemnicy państwowej.

Warto nadmienić, że na podstawie umowy między rządem Rzeczpospolitej Polskiej a rządem Federacji Rosyjskiej o wzajemnej ochronie informacji strony zobowiązały się do wzajemnej ochrony informacji niejawnych wymienianych w wyniku współpracy politycznej, gospodarczej, naukowo-technicznej i innej[59]. Rządy określiły wzajemne przyporządkowanie stosowanych klauzul w celu zapewnienia otrzymywanym informacjom odpowiedniej ochrony.

Lp.	Klauzula stosowana w RP	Klauzula stosowana w FR
1.	Ściśle tajne	Совершенно секретно
2.	Tajne	Секретно
3.	Poufne	Секретно
4.	Zastrzeżone	Для служебного пользования (pol. Do użytku służbowego)

[59] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacji Rosyjskiej o wzajemnej ochronie informacji z dnia 8 lutego 2008 r.* (DzU z 2008 r. nr 217 poz. 1384).

Na uwagę zasługuje przyporządkowanie polskich informacji poufnych i tajnych do rosyjskiej klauzuli „Секретно" oraz polskiej klauzuli „Zastrzeżone" do statusu rosyjskich informacji oznaczanych klauzulą „Для служебного пользования" („Do użytku służbowego"). W Polsce to ostatnie oznaczenie było stosowane przed wprowadzeniem ustawy o ochronie informacji niejawnych z 1999 r.

Ważnym faktem wynikającym z uzyskania przez daną osobę uprawnień dostępu do rosyjskiej tajemnicy państwowej jest wyrażenie przez nią zgody na ograniczenie jej wolności i praw obywatelskich. W art. 21 rosyjskiej ustawy o tajemnicy państwowej ustanowiono m.in. następujące ograniczenia i obowiązki:

1) złożenie pisemnego zobowiązania do nierozpowszechniania powierzonych informacji stanowiących tajemnicę państwową;
2) złożenie pisemnej zgody na przeprowadzenie procedury sprawdzającej przez organy państwowe według przepisów obowiązujących te podmioty;
3) wyrażenie zgody na częściowe, czasowe ograniczenie prawa: wyjazdu poza granicę państwa na uzgodniony okres, nienaruszalności życia prywatnego w związku z procedurą sprawdzającą i inne;
4) zapoznanie się z normami ustawodawstwa o tajemnicy państwowej, przewidującymi odpowiedzialność za ich naruszenie.

Warto wskazać, że jedynie deklaracja (pkt 2) i czynność (pkt 4) mają swoje odzwierciedlenie w przepisach polskiej ustawy o ochronie informacji niejawnych (podobne ograniczenia swobód wprowadzało *Zarządzenie nr 60/83 Ministra Spraw Wewnętrznych z dnia 29 czerwca 1983 roku w sprawie szczegółowych zasad i sposobu postępowania z wiadomościami stanowiącymi tajemnicę państwową i służbową*[60]).

Szczegółowym aktem, w którym określono procedurę i zakres czynności związanych z przeprowadzeniem postępowania sprawdzającego osób przez FSB, jest instrukcja dotycząca dopuszczenia urzędników i innych obywateli FR do tajemnicy państwowej. Została ona wprowadzona uchwałą rządu Federacji Rosyjskiej z 6 lutego 2010 r.[61] Instrukcja zawiera szczegółowe regulacje, które usystematyzowano w sześciu działach:

1) *Postanowienia ogólne*;
2) *Procedura formalnego uzyskania dostępu do tajemnicy państwowej*;
3) *Odstępstwa w procedurze uzyskania dostępu do tajemnicy państwowej dla osób pracujących u kilku pracodawców*;

---

[60] Archiwum Instytutu Pamięci Narodowej w Warszawie, Ministerstwo Spraw Wewnętrznych w Warszawie (1944) 1954–1990 (tytuł zbioru dokumentów – przyp. red.), sygn. IPN BU 01451/18, *Zarządzenie Ministra Spraw Wewnętrznych nr 60/83 z dnia 29 czerwca 1983 roku w sprawie szczegółowych zasad i sposobu postępowania z wiadomościami stanowiącymi tajemnicę państwową i służbową*, Warszawa 1983, (niepublikowane).

[61] *Постановление Правительства РФ от 6 февраля 2010 г., №° 63, „Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне* (*Uchwała Rządu Federacji Rosyjskiej z 6 lutego 2010 r. nr 63 „O zatwierdzeniu instrukcji o procedurze dopuszczenia urzędników państwowych i obywateli Federacji Rosyjskiej do tajemnicy państwowej"*).

4) *Odstępstwa w procedurze uzyskania dostępu do tajemnicy państwowej dla kierowników i członków organizacji samorządowych*[62];
5) *Powtórne uzyskanie dostępu do tajemnicy państwowej*;
6) *Procedura uzyskania dostępu do informacji stanowiących tajemnicę państwową przez obywateli delegowanych do innych pracodawców*.

W końcowej części instrukcji zamieszczono wzory formularzy ewidencyjnych przeznaczonych do: zaliczania stanowisk do określonego poziomu dostępu do tajemnicy; wnioskowania do FSB o przeprowadzenie postępowania sprawdzającego oraz późniejszej rejestracji osób, które uzyskały dostęp do tajemnicy; dokonywania zmian wynikających z utraty dostępu lub zmiany miejsca zatrudnienia oraz wzór ankiety personalnej.

Z postanowień zawartych w instrukcji wynika, że wykaz stanowisk związanych z dostępem do tajemnicy opracowuje szef komórki do spraw ochrony tajemnicy (ros. *руководитель режимно-секретного подразделения*) w porozumieniu ze swoim przełożonym, tj. kierownikiem danej instytucji. Następnie wykaz, o którym mowa, jest przesyłany w dwóch egzemplarzach do zatwierdzenia właściwej jednostce FSB. Po ewentualnym zatwierdzeniu jeden egzemplarz odsyła się do wytwórcy dokumentu. Wykaz jest aktualizowany co najmniej raz na pięć lat.

Wyróżnia się trzy poziomy dostępu do tajemnic: „szczególnego znaczenia", „ściśle tajnych" i „tajnych". Do poziomu informacji o klauzuli „Do użytku służbowego" nie przeprowadza się sprawdzeń ani odrębnej rejestracji, są one dostępne z uwagi na zajmowane stanowisko. Zainteresowany pracownik wypełnia ankietę, w której wskazuje ukończone szkoły, poprzednich pracodawców, miejsca zamieszkania i krewnych (powyżej 14 roku życia). Ponadto informuje o wyjazdach zagranicznych i podaje dane personalne osób, z którymi utrzymuje kontakty, a które wyjeżdżały poza FR lub są cudzoziemcami. Ankietę weryfikuje i podpisuje kierownik komórki do spraw kadrowych oraz kierownik komórki do spraw ochrony tajemnicy. Sprawdzeń danej osoby dokonuje się na wniosek kierownika komórki ochrony tajemnicy, skierowany do rejonowej jednostki FSB, która informuje o pozytywnym lub negatywnym wyniku sprawdzeń i nadaje indywidualny numer przyznanych uprawnień. Jeżeli kierownik jednostki organizacyjnej nie wyda decyzji o udostępnieniu osobie sprawdzonej informacji stanowiących tajemnicę państwową w okresie sześciu miesięcy, to procedurę sprawdzenia dokonanego przez FSB należy powtórzyć. Warto dodać, że objęcie dostępem do określonego poziomu tajemnicy nie ma charakteru uniwersalnego, jest ważne wyłącznie w instytucji (pracodawcy), która nadała uprawnienia. Na gruncie prawa polskiego poświadczenia bezpieczeństwa wydane przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego obowiązują we wszystkich innych podmiotach, wydane przez inne służby zaś

[62] W Federacji Rosyjskiej ustawowo powołano osoby prawne samoregulacyjne, które w dużym uproszczeniu zrzeszają producentów z danej branży w celu wspólnego podejmowania działań non profit (niekomercyjnych). Stanowi o tym rosyjska ustawa: *Закон № 315-ФЗ от 1 декабря 2007 г. „О саморегулируемых организациях"* (*Ustawa nr 315-FZ z 1 grudnia 2007 r. „O samorządowych organizacjach zawodowych"*).

są ważne tylko w ich strukturach (art. 29 ust. 5 ustawy o ochronie informacji niejawnych). Jeżeli pracownik nie zmienia miejsca zatrudnienia, to powtórnego sprawdzenia (ros. *оформление*, tutaj w znaczeniu: 'rejestracja', 'opracowanie') się nie dokonuje. Jeżeli natomiast pracownik zmienił pracodawcę, to – o ile nie wystąpiły przesłanki do cofnięcia przyznanego dostępu – powtórne sprawdzenie przeprowadza się po 10 latach w odniesieniu do tajemnic ściśle tajnych i po 15 – dla pozostałych. W instrukcji podano powody powtórnego sprawdzenia predyspozycji pracownika do ochrony powierzonych mu tajemnic. Jest to między innymi: zawarcie związku małżeńskiego (jeżeli małżonek również ma dostęp do tego typu informacji, sprawdzenia się nie przeprowadza), wyjazd za granicę na okres powyżej sześciu miesięcy, zatrudnienie w komórce do spraw ochrony tajemnicy państwowej albo zatrudnienie osoby, która wcześniej miała dostęp do określonych informacji na mocy prawa w związku ze sprawowaną funkcją (sędziowie, deputowani do Dumy Państwowej, członkowie Rady Federacji, adwokaci i obrońcy w sprawach karnych, w których wykorzystywano materiały chronione klauzulami).

Przesłanki, które wpływają na odmowę dostępu do informacji klauzulowanych lub na cofnięcie już przyznanych uprawnień, to:

1) całkowite lub częściowe ubezwłasnowolnienie;
2) oskarżenie o przestępstwo karne przeciwko władzy państwowej popełnione umyślnie lub z nieostrożności albo skazanie za to przestępstwo, a także niewykonanie nałożonej kary za tego rodzaju przestępstwa;
3) przeciwwskazania medyczne w zakresie dostępu do tajemnicy państwowej[63];
4) pobyt sprawdzanego lub osób wymienionych w złożonej przez niego ankiecie za granicą (powyżej sześciu miesięcy) albo złożenie przez sprawdzanego lub osoby wymienione przez niego w ankiecie wniosku o zgodę na pobyt w innych krajach;
5) ustalenie w wyniku prowadzonych czynności sprawdzających okoliczności stwarzających zagrożenie bezpieczeństwa FR;
6) uchylanie się osoby sprawdzanej od współpracy w czynnościach weryfikacyjnych lub podanie fałszywych danych w ankiecie personalnej.

---

[63] Osoba, która ubiega się o dostęp do tajemnicy, jest zobowiązana przedstawić zaświadczenie o braku medycznych (psychicznych) przeciwwskazań do pracy z informacjami stanowiącymi tajemnicę państwową, wydawane na podstawie zarządzenia Ministerstwa Zdrowia i Rozwoju Społecznego FR, w: *Приказ Министерства здравоохранения и социального развития РФ от 26 августа 2011 г., № 989н, „Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну* (*Zarządzenie Ministerstwa Zdrowia i Rozwoju Społecznego FR z 26 sierpnia 2011 r.*, nr 989n, „*O zatwierdzeniu wykazu przeciwwskazań lekarskich do pracy z wykorzystaniem informacji stanowiących tajemnicę państwową, trybu uzyskiwania i formy zaświadczenia o braku przeciwwskazań lekarskich do pracy z informacjami stanowiącymi tajemnicę państwową*").

Jednostka FSB informuje kierownika danej instytucji o rezultacie sprawdzeń. Kierownik instytucji na tej podstawie podejmuje decyzję o udostępnieniu albo odmowie udostępnienia tajemnicy. Jeżeli decyzja jest negatywna, to osoba zainteresowana udostępnieniem informacji ma prawo wnieść skargę do organu wyższego stopnia w strukturach administracji publicznej albo wyższego przełożonego w pozostałych instytucjach, a następnie do sądu.

Warto nadmienić, że polska ustawa o ochronie informacji niejawnych z 2010 r. w odniesieniu do zdrowia psychicznego i uzależnień osób sprawdzanych uprawnia organ prowadzący poszerzone postępowanie sprawdzające do zobowiązania osoby sprawdzanej, aby poddała się odpowiednim badaniom i przedstawiła ich wyniki (art. 26 ust. 6 ustawy o ochronie informacji niejawnych). Ponadto w postępowaniu odwoławczym przed Wojewódzkim Sądem Administracyjnym sąd może, z urzędu lub na wniosek osoby sprawdzanej, skorzystać z uprawnień ustanowionych powyższym przepisem. W przypadku braku okoliczności wskazujących na istnienie schorzeń psychicznych lub uzależnień organ prowadzący postępowanie, co do zasady, przyjmuje na podstawie oświadczenia złożonego w ankiecie bezpieczeństwa, że dana osoba jest zdrowa. Rosyjskie regulacje nakazują złożenie zaświadczenia o braku przeciwwskazań zdrowotnych do pracy z informacjami stanowiącymi tajemnicę państwową w każdym przypadku wraz z wypełnioną ankietą.

Należy zasygnalizować, że instytucją prawną, która nie występuje w polskim prawodawstwie, są procentowe dodatki finansowe do uposażenia dla pracowników komórek ochrony tajemnicy oraz innych struktur – w zależności od poziomu dostępu do tajemnicy, ustanowione w art. 21 rosyjskiej ustawy o tajemnicy państwowej.

W przypadku podjęcia przez pracownika równoległej pracy w innym podmiocie na stanowisku z dostępem do tajemnicy państwowej pracodawca wydaje duplikat decyzji o dopuszczeniu go do określonego poziomu tajemnicy. Jednocześnie przesyła do rejonowej jednostki FSB kartę ewidencyjną z informacją o przekazaniu uprawnień do innego pracodawcy oraz informuje drugiego pracodawcę o jednostce FSB, która przeprowadziła czynności sprawdzające, i podaje numer oraz datę wydania tych uprawnień.

Gdy kierownik danej instytucji otrzyma od FSB informacje dotyczące okoliczności, które mogą stanowić podstawę cofnięcia określonemu pracownikowi dostępu do tajemnicy państwowej, podejmuje decyzję w tej sprawie. Jeżeli postanawia utrzymać dotychczasowe uprawnienia w zakresie dostępu do tego rodzaju tajemnicy w kierowanym przez niego podmiocie, pisemnie informuje jednostkę FSB o powodach uzasadniających to utrzymanie wbrew informacji organu bezpieczeństwa.

W związku z istotną rolą FSB w reglamentacji publicznoprawnych tajemnic FR należy odnieść się do zadań tej formacji[64]. Uprawnienia i obowiązki jej żołnierzy oraz pracowników są bardzo szerokie i wynikają z uniwersalnego charakteru służby. Zakres oddziaływania FSB na system bezpieczeństwa państwa jest nieporównywalny

[64] *Федеральный закон от 3 апреля 1995 г., № 40-ФЗ, „О Федеральной службе безопасности"… (Ustawa federalna z 3 kwietnia 1995 r. nr 40-FZ „O Federalnej Służbie Bezpieczeństwa"…).*

z zakresem oddziaływania jakiejkolwiek ze służb polskich. Ustawowe zadania tej formacji obejmują: walkę z terroryzmem i przestępczością, ochronę granicy państwowej, a przede wszystkim – prowadzenie wojskowego i cywilnego kontrwywiadu oraz wywiadu we współpracy ze Służbą Wywiadu Zagranicznego FR (ros. Служба Внешней Разведки - СВР, pis. fon. Służba Wniesznej Razwiedki - SWR; przed 1991 r. – Zarząd I KGB ZSRR. Dalej będzie stosowany skrót najbardziej rozpoznawalny w Polsce: SWR)[65]. Ważnym zadaniem SWR z punktu widzenia bezpieczeństwa informacji jest prowadzenie rozpoznania osób, które uzyskały dostęp do tajemnicy państwowej FR i przebywają poza granicami tego kraju (art. 11 ustawy o SWR). W odniesieniu do FSB natomiast należy zaznaczyć, że jednym z aspektów działalności kontrwywiadowczej tej służby jest ochrona tajemnicy państwowej (art. 9 pkt w oraz art. 12 pkt k ustawy o FSB). Powyższe zadanie jest realizowane przez:

1) partycypację w opracowywaniu i wdrażaniu środków ochrony informacji stanowiących tajemnicę państwową;
2) sprawowanie kontroli nad zapewnianiem bezpieczeństwa informacji stanowiących tajemnicę państwową w organach państwowych, formacjach wojskowych, przedsiębiorstwach, instytucjach i organizacjach, niezależnie od formy własności;
3) przeprowadzanie, według ustalonej procedury, działań związanych z udostępnianiem informacji stanowiących tajemnicę państwową.

Dodatkowo zadania FSB i sposób ich realizacji, m.in. w odniesieniu do ochrony tajemnicy państwowej, zostały uszczegółowione w pkt 9 ppkt 12 dekretu Prezydenta FR z 2003 r. w sprawie zadań FSB[66]. Zgodnie z tym aktem służba przeprowadza czynności w zakresie udzielania obywatelom i osobom prawnym dostępu do tajemnicy państwowej.

Ważną instrukcją kształtującą system ochrony tajemnicy państwowej w FR jest instrukcja o zabezpieczaniu zachowania tej tajemnicy. W związku z tym, że wydano ją z klauzulą „Do użytku służbowego", nie została ona opublikowana[67]. Merytoryczne zbadanie i omówienie metod i środków stosowanych przez FSB w celu ochrony tajemnicy państwowej napotyka poważne trudności ze względu na ustawowy obowiązek chronienia tego rodzaju informacji, a w rezultacie - objęcie ich tajemnicą.

Niniejszy artykuł nie wyczerpuje przedmiotu rozważań, może jednak stanowić podstawę wstępnych wniosków, a także asumpt do dalszych badań.

---

[65] *Федеральный закон от 10 января 1996 г., № 5-ФЗ, „О внешней разведке" (Ustawa federalna z 10 stycznia 1996 r. nr 5-FZ „O wywiadzie zagranicznym"*).

[66] *Указ Президента РФ от 11 августа 2003 г., № 960, „Вопросы Федеральной службы безопасности Российской Федерации" (Dekret Prezydenta FR z 11 sierpnia 2003 r. nr 960 „Zadania Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej"*).

[67] *Постановление Правительства Российской Федерации от 5 января 2004 г., № 3-1, „Об утверждении Инструкции по обеспечению режима секретности в Российской Федерации"* (*Uchwała z dnia 5 stycznia 2004 r. Rządu Federacji Rosyjskiej nr 3-1 „O zatwierdzeniu Instrukcji o zabezpieczeniu zachowania tajemnicy w Federacji Rosyjskiej"*).

Podsumowanie

Należy stwierdzić, że polski system ochrony najistotniejszych tajemnic publicznoprawnych ustanowiono aktami prawa administracyjnego z uwzględnieniem dziedzin określonych w art. 61 ust. 3 Konstytucji RP. Naruszenie ich poufności, które może zagrozić interesowi państwa, jest sankcjonowane prawem karnym. Podobne konstrukcje prawne przyjęto w prawodawstwie Federacji Rosyjskiej. Uregulowanie systemu ochrony tajemnic państwowych, w tym zasad weryfikacji osób aktami prawa administracyjnego, a także blankietowy charakter przepisów karnego prawa materialnego FR, pozwalają na identyfikację podobnych elementów w polskim systemie ochrony informacji niejawnych. Wyraźne podobieństwa regulacji zachodzą w odniesieniu do przepisów uchylonego polskiego kodeksu karnego z 1969 r. oraz ustawy o ochronie informacji niejawnych z 1999 r. Aktualne prawodawstwo RP wprowadza uniwersalne kryteria klasyfikowania informacji i obejmowania ich ochroną państwa. Zrezygnowano ze sporządzania wykazów informacji, którym należy nadać klauzulę. Pozwala to na zidentyfikowanie różnic w systemie ochrony informacji niejawnych (tajemnic państwowych) Polski i Rosji, a ponieważ nie są one diametralne, przyjęta na wstępie hipoteza robocza zostaje obalona.

Bibliografia

Andrejew I., *Polskie prawo karne w zarysie*, Warszawa 1989, Państwowe Wydawnictwo Naukowe.

Bosiacki A., Izdebski H., *Konstytucjonalizm rosyjski. Historia i współczesność*, Kraków 2013, Wydawnictwo ARCANA.

Dębski R., *Pozaustawowe znamiona przestępstwa*, Łódź 1995, Wydawnictwo Uniwersytetu Łódzkiego.

Hoc S., *Karnoprawna ochrona informacji*, Opole 2009, Wydawnictwo Uniwersytetu Opolskiego.

Kunicka-Michalska B., *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości*, Warszawa 2000, C.H. Beck.

Leciak M., *Karnoprawna ochrona informacji niejawnych*, Toruń 2012, TNOiK.

Leciak M., *Tajemnica państwowa i jej ochrona*, Toruń 2009, TNOiK.

Marek A., *Prawo karne*, Warszawa 2016, C.H. Beck.

Pohl Ł., *Zasady odpowiedzialności karnej*, w: *Kodeks karny. Komentarz*, R. Stefański (red.), Warszawa 2015, C.H. Beck.

Literatura rosyjska

Борисов А.Б., *Комментарий к конституции Российской Федерации (постатейный): с комментариями Конституционного суда РФ*, Москва 2013, Книжный мир.

Борисов А.Б., *Комментарий к Уголовному кодексу Российской Федерации (постатейный) с постатейными материалами и практическими разъяснениями официальных органов*, wyd. 7, Москва 2014, Книжный мир.

Лебедев В.М., *Уголовный кодекс Российской Федерации с научно-практическими комментариями*, Варшава 1997, Бюро по демократическим институтам и правам человека.

Пудовочкин Ю.Е., *Преступления против государственной власти*, в: *Комментарий к Уголовному кодексу Российской Федерации*, t. 2, А.В. Бриллиантов (red.), Москва 2017, Проспект.

Скоробогатова О.О., Перчаткина С.А., *Уголовный кодекс Российской Федерации с комментариями*, Москва 2012, Эксмо.

Юридический энциклопедический словарь, А.В. Малько (red.), wyd. 2, Москва 2017, Проспект.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacji Rosyjskiej o wzajemnej ochronie informacji z dnia 8 lutego 2008 r. (DzU z 2008 r. nr 217 poz. 1384).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j.: DzU z 2019 r. poz. 742).

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

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j.: DzU z 2020 r. poz. 2176).

Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (DzU z 1982 r. nr 40 poz. 271, ze zm.).

Rozporządzenie Prezydenta Rzeczypospolitej z dnia 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu Państwa (DzU z 1934 r. nr 94 poz. 851).

Rozporządzenie Prezydenta Rzeczypospolitej z dnia 16 lutego 1928 r. o karach za szpiegostwo i niektóre inne przestępstwa przeciw Państwu (DzU z 1928 r. nr 18 poz. 160).

Dekret z dnia 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej (DzU z 1949 r. nr 55 poz. 437).

Dekret z dnia 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa (DzU z 1946 r. nr 30 poz. 192).

Dekret z dnia 16 listopada 1945 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa (DzU z 1945 r. nr 53 poz. 300).

Rosyjskie akty prawne

Конституция Российской Федерации от 12 декабря 1993 г., https://rg.ru/zakon/1993/12/25_publish.html [dostęp: 8 II 2021].

Указ Президента РФ от 30 ноября 1995 г., № 1203, „Об утверждении перечня сведений, отнесенных к государственной тайне”, http://base.garant.ru/10105548/ [dostęp: 19 I 2021].

Федеральный закон от 8 марта 2015 г., № 21-ФЗ, „Кодекс административного судопроизводства Российской Федерации”, https://fzrf.su/kodeks/kas/ [dostęp: 8 II 2021].

Федеральный закон от 30 декабря 2001 г., № 195-ФЗ, „Кодекс Российской Федерации об административных правонарушениях”, https://fzrf.su/kodeks/koap/ [dostęp: 8 II 2021].

Федеральный закон о безопасности от 28 декабря 2010 г., № 390-ФЗ, „О безопасности”, https://fzrf.su/zakon/o-bezopasnosti-390-fz/ [dostęp: 8 II 2021].

Федеральный закон от 9 февраля 2009 г., № 8-ФЗ, „Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления”, http://www.consultant.ru/document/cons_doc_LAW_84602/ [dostęp: 8 II 2021].

Федеральный закон от 22 декабря 2008 г., № 262-ФЗ, „Об обеспечении доступа к информации о деятельности судов в Российской Федерации”, https://fzrf.su/zakon/dostup-k-informacii-o-deyatelnosti-sudov-262-fz/ [dostęp: 8 II 2021].

Федеральный закон от 2 мая 2006 г., № 59-ФЗ, „О порядке рассмотрения обращений граждан Российской Федерации”, http://www.consultant.ru/document/cons_doc_LAW_59999/ [dostęp: 8 II 2021].

Федеральный закон от 17 января 1992 г., № 2202-1, „О прокуратуре Российской Федерации”, https://fzrf.su/zakon/o-prokurature-2202-1/ [dostęp: 8 II 2021].

Закон Российской Федерации от 21 июля 1993 г., № 5485-1, „О государственной тайне”, с изменениями, Законодательство Российской Федерации, Сборник основных федеральных законов РФ, http://fzrf.su/zakon/o-gosudarstvennoj-tajne-n-5485-1/ [dostęp: 30 VII 2020].

Уголовный кодекс Российской Федерации от 13 июня 1996 г., № 63-ФЗ, с изменениями, Законодательство Российской Федерации, Сборник основных федеральных законов РФ, https://fzrf.su/kodeks/uk/ [dostęp: 8 II 2021].

Постановление Конституционного Суда РФ от 20 декабря 1995 г., № 17-П, по делу о проверке конституционности ряда положений пункта „а” статьи 64 Уголовного кодекса РСФСР в связи с жалобой гражданина В.А. Смирнова, http://legalacts.ru/doc/postanovlenie-konstitutsionnogo-suda-rf-ot-20121995-n/ [dostęp: 30 VII 2020].

Постановление Правительства РФ от 6 февраля 2010 г., № 63, „Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне”, http://www.consultant.ru/document/cons_doc_LAW_97474/ [dostęp: 8 II 2021].

Abstrakt

W artykule omówiono regulacje administracyjne dotyczące udostępniania informacji tajnych i ściśle tajnych oraz przedstawiono przepisy karne dotyczące ujawniania tajemnicy państwowej obowiązujące w Federacji Rosyjskiej wraz z ich interpretacją. Autor w odniesieniu do rosyjskich przepisów konstytucyjnych, administracyjnych i karnych wybiórczo przedstawia adekwatne do nich przepisy prawa polskiego. Ponadto w związku z tym, że przepisy prawa karnego nie zawierają definicji terminów użytych do ich konstrukcji, w artykule zaprezentowano przepisy administracyjne rosyjskiego systemu ochrony tajemnic publicznych, które są niezbędne do rekonstrukcji karnych norm prawnych. Na podstawie opracowania sformułowano wniosek, że w polskim ustawodawstwie brakuje odrębnego przepisu penalizującego uzyskanie informacji tajnej lub ściśle tajnej w wyniku popełnienia odrębnego czynu zabronionego. Powyższe może być podstawą do ewentualnych przyszłych zmian legislacyjnych w tym zakresie.

Należy zaznaczyć, że artykuł nie wyczerpuje tematu, a jedynie wskazuje wybrane zagadnienia związane z systemem ochrony tajemnicy państwowej w Rosji. Zainicjowana eksploracja może w przyszłości być wykorzystana do pogłębionych badań porównawczych nad zagadnieniem, o którym mowa.

Słowa kluczowe: służba specjalna, kodeks karny, ujawnienie, informacje niejawne, postępowanie sprawdzające, poświadczenie bezpieczeństwa.

The protection of State Secrets in the Russian Federation. Selected penal and administrative regulations

Abstract

The article discusses the administrative regulations regarding the disclosure of secret and top-secret information in the Russian Federation. Moreover, it presents the effective penal code provisions directed against the disclosure of state secrets in Russia and the interpretation of these provisions. The author does not limit himself only to Russian constitutional, administrative and criminal regulations but gives examples of Polish corresponding laws. Additionally, in connection with the fact that criminal law provisions often contain non-specific references to other legislation, the article presents administrative acts of the protection system of public secrets. On the basis of the formulated conclusions, it was recognised that the Polish legislation lacks an individual provision penalising the fact of obtaining secret or top-secret information as a result of committing a separate unlawful act. It can be the basis to formulate postulates de lege ferenda.

It should be noted that the article does not exhaust the topic, but only indicates selected issues of the protection system of state secrets in Russia. Initiated study can be used to carry out in-depth comparative research on this topic in the future.

Keywords: secret service, penal code, disclosure, classified information, security background investigation, security clearance.

PAWEŁ POKRZYWIŃSKI
ORCID: 0000-0002-5018-2186

DOI: 10.4467/20801335PBW.21.004.13561

Izraelskie ustawodawstwo antyterrorystyczne wobec zagrożeń XXI wieku

Państwo Izrael od czasu ogłoszenia niepodległości w 1948 r. zmaga się z różnymi zagrożeniami. Początkowo miały one charakter przede wszystkim konwencjonalny i były związane z wrogim stosunkiem państw arabskich w regionie Bliskiego Wschodu (np. wojna o niepodległość w 1948 r., wojna na wyczerpanie w latach 1967–1970, wojna Jom Kipur w 1973 r.) lub wynikały z izraelskiego poczucia zagrożenia ze strony państw ościennych (kryzys sueski w 1956 r., wojna sześciodniowa w 1967 r.). Dzięki podpisaniu traktatów pokojowych z Egiptem (1979 r.) i Jordanią (1994 r.) Izrael odsunął i zminimalizował zagrożenia konwencjonalne.

Bezpieczeństwu Izraela zagrażają również terroryzm i działalność arabskich ugrupowań paramilitarnych. Te zjawiska towarzyszyły konfliktom na Bliskim Wschodzie już od lat 50. XX w. (m.in. ataki fedainów trwające od 1948 r. do kryzysu sueskiego). Działania nieregularne oraz ataki terrorystyczne zyskiwały na znaczeniu wraz ze spadkiem zagrożeń konwencjonalnych, umacnianiem się palestyńskich dążeń do uzyskania niepodległości i radykalizacją postaw. W Izrael są wymierzone również działania nieregularne o charakterze terrorystycznym inicjowane z zewnątrz. Jako przykład można podać Liban i działający w nim Hezbollah, a także ataki na izraelskich obywateli przebywających za granicą[1]. Izrael podejmował różne kroki, które miały zapobiec działaniom nieregularnym i atakom terrorystycznym, poczynając od działań prewencyjnych i zatrzymywania podejrzanych, przez likwidowanie pojedynczych terrorystów (tzw. *targeted killing*), burzenie domów zamieszkiwanych przez terrorystów i ich rodziny, a kończąc na operacjach wojskowych (np. druga wojna libańska w 2006 r., operacja Płynny Ołów z lat 2008–2009, operacja Ochronny Brzeg w 2014 r.).

[1] Przykładem może być zamach w Burgas (Bułgaria) w 2012 r.

Pozasiłową formą walki z terroryzmem jest ustawodawstwo. Definiuje ono terminy odnoszące się do działań i organizacji terrorystycznych zgodnie z państwową racją stanu. Oprócz tego prawo wyznacza podmioty odpowiedzialne za bezpieczeństwo i walkę z tym zjawiskiem, określa ich kompetencje, a także ustala katalog sankcji i kar. Prawo tworzy przede wszystkim ramy działalności państwa i jego instytucji, jest odbiciem percepcji pewnych zjawisk i zagrożeń oraz stanowi o formach walki z działalnością terrorystyczną, akceptowanych w danym społeczeństwie. Legislacja musi ponadto uwzględniać płynność zjawiska terroryzmu oraz zmienność metod działań organizacji terrorystycznych.

Dnia 23 czerwca 2016 r. prawicowo-religijna koalicja, w której znalazły się: Likud, My Wszyscy (Kulanu), Żydowski Dom (Ha-Bajt ha-Jehudi), Szas, Zjednoczony Judaizm Tory (Jahadut ha-Tora), Nasz Dom Izrael (Israel Beitenu), przyjęła *Prawo zwalczania terroryzmu*[2]. Już na wstępie należy zaznaczyć, że izraelska prawica charakteryzuje się jastrzębim podejściem do kwestii bezpieczeństwa i stosunków międzynarodowych. Cechuje ją ponadto stawianie na odstraszanie przeciwnika, dominację siłową oraz militaryzm w działaniach podejmowanych w odpowiedzi na zagrożenia[3]. Znalazło to przełożenie podczas tworzenia projektu wspomnianego prawa w 2011 r., a prace nad nim wywoływały liczne kontrowersje. Izraelski Instytut Demokracji przestrzegał wówczas, że w tym prawie mogą się znaleźć zapisy przewidujące sankcje, a także nadające organom bezpieczeństwa przywileje, które będą niewspółmiernie duże do zagrożenia, jakie stanowi terroryzm wobec takiego państwa jak Izrael. Uznano jednocześnie, że będzie to pierwsza dopracowana i kompleksowa propozycja nowego ustawodawstwa związanego z definiowaniem i zwalczaniem działalności terrorystycznej[4].

Celem niniejszego artykułu jest przedstawienie izraelskich rozwiązań przyjętych w *Prawie zwalczania terroryzmu* oraz porównanie ich z ustawodawstwem antyterrorystycznym obowiązującym wcześniej w Państwie Izrael. Tematyka izraelskiego prawodawstwa antyterrorystycznego nie doczekała się zbyt wielu opracowań w literaturze polskojęzycznej[5]. Problematyka bezpieczeństwa została natomiast dobrze opisana w kontekście polityki zagranicznej, sytuacji geopolitycznej w regionie Bliskiego Wschodu, przemian politycznych w państwach arabskich czy zagadnień militarnych[6].

---

[2] W artykule autor będzie używał tłumaczenia nazw dokumentów z języka hebrajskiego na język polski. W oryginale nazwa brzmi następująco: 2016-חוק קבאמה לטרור, תשע"ו (wym. *chok ha-maawak be-teror, 5776–2016*).

[3] I. Peleg, *The Israeli Right*, w: *Contemporary Israel. Domestic Politics, Foreign Policy, and Security Challenges*, R.O. Freedman (red.), Boulder 2009, s. 34–37.

[4] M. Kremnicer, J. Szani, A. Foks, *Hacaat chok ha-maawak be-teror 5771–2011*, https://www.idi.org.il/articles/7757 [dostęp: 1 VI 2020].

[5] Zob. A.K. Siadkowski, *Polityka instytucjonalno-prawna Izraela wobec wewnętrznych zagrożeń bezpieczeństwa*, w: *Problemy bezpieczeństwa Bliskiego Wschodu i Północnej Afryki (MENA)*, R. Bania, R. Czulda, K. Zdulski (red.), Łódź 2016, s. 121–135.

[6] Zob. A. Pohl, *Główne determinanty polityki bezpieczeństwa Izraela na początku XXI wieku*, Poznań 2020; A. Krawczyk, *Terroryzm ugrupowań fundamentalistycznych na obszarze Izraela w drugiej*

Autor przedstawi ramy definicyjne, katalog kar, a także podmioty odpowiedzialne za bezpieczeństwo oraz ich kompetencje, wskazane w prawie z 2016 r. Zastosuje analizę instytucjonalno-prawną, pozwalającą na ukazanie i wyjaśnienie norm prawnych dotyczących wybranego zjawiska, w tym wypadku zwalczania terroryzmu. W tym rodzaju analizy wykorzystuje się m.in. teksty aktów prawnych[7]. W celu porównania izraelskiego ustawodawstwa dotyczącego terroryzmu zostanie ponadto użyta metoda porównawcza różnicy, polegająca na analizie podobnych przypadków różniących się zmiennymi[8]. Pozwoli ona stwierdzić, czy w poszczególnych aktach prawnych występowały różnice w definiowaniu terroryzmu i jego percepcji. W realizacji przyjętych założeń będzie pomocna także teoria sekurytyzacji opracowana przez Barry'ego Buzana, Ole Wævera i Jaapa de Wildego. Zakłada ona, że aktor sekurytyzujący (np. politycy, rząd, premier) uznaje, że egzystencjalne bezpieczeństwo obiektu referencyjnego (np. narodu lub państwa) zostało zagrożone i należy podjąć nadzwyczajne środki w celu likwidacji tego zagrożenia. Taki przekaz musi zostać skierowany do wybranego grona odbiorców, których należy przekonać do tego, że zagrożenie wystąpiło i należy je zneutralizować[9]. W tym wypadku nie odwołujemy się do pojęcia obiektywne zagrożenie, ponieważ bezpieczeństwo staje się konceptem konstruowanym przez aktorów. To oni decydują o tym, co zostaje włączone w obszar bezpieczeństwa, a co będzie z niego wyłączone. W związku z tym o obiektywnym zagrożeniu można mówić w momencie, kiedy zostanie ono za takie uznane i zaakceptowane[10].

Przyjęta metodologia oraz teoria przyczyniły się do postawienia następujących pytań badawczych:

1. Jakie zmiany wprowadziło *Prawo zwalczania terroryzmu* z 2016 r. w stosunku do ustawodawstwa obowiązującego wcześniej?
2. Jaki katalog przestępstw związanych z terroryzmem wprowadza to prawo w kontekście ewolucji terroryzmu?
3. Jakie podmioty w myśl tego prawa są odpowiedzialne za zapewnienie bezpieczeństwa oraz jakie kompetencje im przyznano?

Autor sformułował także hipotezy badawcze:

---

połowie XX wieku, Toruń 2007; M. Jadwiszczok, *Antyizraelskie ugrupowania terrorystyczne i ich zwalczanie*, Toruń 2010; A. Dzisiów-Szuszczykiewicz, *„Trzęsienie ziemi" w środowisku bezpieczeństwa Izraela*, „Bezpieczeństwo Narodowe" 2011, nr 3, s. 165–180; M. Szydzisz, *Polityka zagraniczna Izraela wobec aktualnych wydarzeń na Bliskim Wschodzie*, w: *Badanie polityki zagranicznej państwa: Stany Zjednoczone, Azja Wschodnia, Bliski Wschód i Ameryka Łacińska*, P. Materny i in. (red.), Warszawa 2017, s. 209–228; A. Skorek, *Bliskowschodnia strategia Izraela po arabskiej wiośnie*, „Krakowskie Studia Międzynarodowe" 2018, nr 3, s. 107–125; M. Harkot, *Odstraszanie jako element strategii bezpieczeństwa Izraela*, „Ante Portas – Studia nad Bezpieczeństwem" 2019, nr 1, s. 81–92.

7 A.J. Chodubski, *Wstęp do badań politologicznych*, Gdańsk 2004, s. 126.

8 J.R. Sielezin, *Badania źródłoznawcze w politologii. Wybrane zagadnienia metodologiczne*, Wrocław 2010, s. 16–18.

9 B. Buzan, O. Wæver, J. de Wilde, *Security. A New Framework for Analysis*, Boulder 1998, s. 36, 40.

10 B. Buzan, L. Hansen, *The Evolution of International Security Studies*, Cambridge 2009, s. 33–34.

1. W związku z tym, że izraelska prawica przyjmuje jastrzębie stanowisko w kwestiach bezpieczeństwa, to definicje zawarte w prawie będą ujęte bardzo szeroko i niejednoznacznie.
2. Izrael traktuje terroryzm jako główne zagrożenie bezpieczeństwa państwa i społeczeństwa, wobec czego nowe prawo legalizuje nadzwyczajne i kontrowersyjne środki prewencji.

W niniejszym artykule przedmiotem analizy będą wspomniane już *Prawo zwalczania terroryzmu* z 2016 r., a także obowiązujące wcześniej ustawodawstwo związane ze zjawiskiem terroryzmu: *Przepisy obronne (nadzwyczajne)*[11] z 1945 r., *Rozporządzenie zapobiegające terroryzmowi*[12] z 1948 r., *Prawo zakazu finansowania terroryzmu*[13] z 2005 r. i *Prawo karne (zatrzymany oskarżony o przestępstwo związane z bezpieczeństwem)(Przepis tymczasowy)*[14] z 2006 r.[15]

Zagrożenia bezpieczeństwa Izraela w XXI wieku

Strategia Armii Obrony Izraela opublikowana w 2015 r. definiuje współczesne zagrożenia Państwa Izrael, dzieląc je na regularne i nieregularne. Do tych pierwszych zalicza przede wszystkim zagrożenia płynące ze strony Iranu, Libanu i Syrii. Zgodnie z tym dokumentem wskazane państwa są źródłem destabilizacji w regionie Bliskiego Wschodu[16]. Analiza zapisów tej strategii pozwala stwierdzić, że głównym źródłem niebezpieczeństwa są jednak organizacje „niepaństwowe", terrorystyczne. Dokument wymienia w tym kontekście Hezbollah, Hamas, Palestyński Islamski Dżihad, tzw. Państwo Islamskie i światowy dżihad. Zwrócono uwagę, że rola, jaką odegrały one w ostatnich latach, przysłoniła niebezpieczeństwa kreowane przez regularne armie państw ościennych[17]. Marcin Szydzisz zaznacza również, że Izrael prezentuje światowy i lokalny terroryzm jako główne zagrożenie demokracji i pokoju na poziomie państwa, regionu i systemu

---

[11] Nazwa hebrajska: הגנהה תונקת (סוריח תעש), 1945 (wym. *tkanot ha-hagana (szaat cherum), 1945*).

[12] Nazwa hebrajska: רורט תעינמ תדוקפ, ח"שתה-1948 (wym. *pkudat mnijat teror 5708-1948*).

[13] Nazwa hebrajska: רורט ומימ רוסיא קוח, ה"סשתה-2005 (wym. c*hok isur mimun teror 5765-2005*).

[14] Nazwa hebrajska: ילילפה וידה רדס קוח (וחטיב תוריבעב דושחה רוצע) (העש תארוה), ו"סשתה-2006 (wym. *chok seder ha-din ha-plili (acur he-chaszud ba-awirut bitachon)(horaat szaa) 5766-2006*).

[15] Niniejszy artykuł nie ma na celu szczegółowej analizy izraelskiego prawodawstwa antyterrorystycznego ze względu na obszerny zakres materiału źródłowego. Taka analiza powinna stać się częścią szerszego opracowania naukowego. Jednocześnie czas, który upłynął od momentu uchwalenia tego prawa, pozwala na zaprezentowanie działań struktur bezpieczeństwa i reakcji na znajdujące się w nim zapisy.

[16] *Estrategijat Cahal*, Tel Awiw 2015, s. 9. Warto zaznaczyć, że w Izraelu w walkę z terroryzmem są czynnie zaangażowane różne struktury: armia (w tym wywiad wojskowy Aman), Szabak, Mosad i Policja Izraela.

[17] Tamże, s. 9, 11.

międzynarodowego[18]. Według izraelskiej lewicy oraz prawicy palestyński terroryzm utrudnia proces pokojowy. Jednak zdaniem lewicowej Partii Pracy zawarcie pokoju ma doprowadzić do zmniejszenia skali terroru. Z kolei Likud uważa, że eliminacja działalności terrorystycznej będzie stanowić punkt wyjścia do zawarcia stabilnego pokoju[19].

Jak pisze Boaz Ganor, terroryzm jest zjawiskiem zmiennym, dynamicznym, które dostosowuje się do otoczenia, ograniczeń. Organizacja terrorystyczna jest organizacją uczącą się, mającą cele, motywacje, a także sponsorów. Proces uczenia się pozwala na zmianę i dobranie taktyki działania, przez co terroryzm ewoluuje[20]. Według Ganora XXI w. przyniósł nowe wyzwania państwom, które muszą zmierzyć się z hybrydowymi organizacjami terrorystycznymi. Ten nowy typ organizacji oprócz skrzydła politycznego i zbrojnego rozwinął działalność mającą na celu „zdobycie serc i umysłów". Pod tym hasłem kryje się wiele działań związanych z propagandą w sieci i mediach, działalnością charytatywną, socjalną, edukacyjną. To sprawia, że państwo musi angażować wszystkie swoje struktury, aby w efektywny sposób walczyć z takimi organizacjami i jednocześnie zachować autorytet i pozycję[21]. Ponadto Ganor zaznacza, że wiele współczesnych organizacji terrorystycznych ma finansowe, zbrojeniowe, szkoleniowe i operacyjne wsparcie na zasadzie relacji sponsor–beneficjent[22].

Dotychczasowe izraelskie doświadczenia związane z Hamasem czy Hezbollahem pokazały, że wiele cech nowoczesnego terroryzmu ma też terroryzm na Bliskim Wschodzie. Yoram Schweitzer pisze, że struktury Hamasu i Hezbollahu oraz ich sposoby walki wykraczają poza znaną dotychczas *guerillę* i ewoluują w stronę *terrorilli*. Mają one rozwinięte organizację, dowodzenie i hierarchię, czym przypominają regularne armie i są w stanie z nimi współdziałać (np. Hezbollah w Syrii). Wyposażenie takich organizacji pochodzi z dostaw z krajów zewnętrznych. Schweitzer uważa, że sposoby walki w *terrorilli* są podobne do działań partyzanckich opartych na znajomości terenu i wsparciu lokalnej ludności (przy czym nie zawsze jest to wsparcie dobrowolne), uzupełnionych o działania o charakterze terrorystycznym. Ponadto walka tych organizacji polega na pojedynczych uderzeniach na wybrane cele czy ostrzałach rakietowych, które mają wywołać efekt psychologiczny i przyczynić się do strat[23].

Kolejnym przejawem zmian w działaniach organizacji terrorystycznych zagrażających Izraelowi są ostrzały rakietowe. Tę taktykę od 2001 r. stosuje głównie Hamas. Izraelczycy szacują, że w arsenale Hamasu znajdują się rakiety produkcji chińskiej,

---

[18] M. Szydzisz, *Sekurytyzacja jako narzędzie polityki zagranicznej Izraela w świetle teorii regionalnych kompleksów bezpieczeństwa*, Warszawa 2019, s. 96–98.

[19] Tamże, s. 226–228.

[20] B. Ganor, *Global Alert. The Rationality of Modern Islamist Terrorism and the Challenge to the Liberal Democratic World*, New York 2015, s. 1.

[21] Tamże, s. 2–3.

[22] Tamże, s. 64–68.

[23] Y. Schweitzer, *Defning the Victor in the Fight against an Army of "Terrorilla"*, w: *The Lessons of Operation Protective Edge*, A. Kurz, S. Brom (red.), Tel Aviv 2014, s. 22–23.

syryjskiej, irańskiej, radzieckiej oraz własnej. Tego rodzaju ostrzały nie powodują poważnych zniszczeń i dużej liczby ofiar, m.in. dzięki systemowi Iron Dome[24], ich zadaniem jest raczej wywarcie efektu psychologicznego. Od 2008 r. Hamas podejmował wysiłki na rzecz zwiększenia możliwości wystrzeliwania rakiet, zwłaszcza z gęsto zaludnionych obszarów, jak również magazynowania amunicji i wyrzutni[25].

Kolejnym elementem zagrażającym Izraelowi są podziemne tunele wykorzystywane przez Hezbollah oraz organizacje palestyńskie. Znajdują się one pod granicą libańsko-izraelską, między Strefą Gazy i Izraelem oraz między Egiptem i Strefą Gazy. W dwóch pierwszych przypadkach są to tzw. tunele ofensywne, służą głównie do infiltracji terytorium Izraela i przeprowadzania ataków. Tunele wykorzystuje się również do przerzutu osób, przemytu broni lub jej magazynowania[26]. To zjawisko zaczęło się nasilać od 2006 r. jako odpowiedź na rozwój izraelskich naziemnych systemów obserwacji i wykrywania. W 2013 r. Armia Obrony Izraela ogłosiła walkę z podziemnymi tunelami. Na przełomie lat 2018 i 2019 przeprowadzono operację Północna Tarcza, której celem było zniszczenie tuneli Hezbollahu pod granicą libańsko-izraelską[27].

Czynnikiem, który może wpłynąć na mobilizację członków organizacji terrorystycznych, a proces rekrutacji do tych ugrupowań uczynić bardziej skutecznym, jest sukces działań propagandowych prowadzonych w sieci przez tzw. Państwo Islamskie. Wykorzystywało ono media społecznościowe do publikacji swoich materiałów, nawiązywania kontaktu z sympatykami i prowadzenia wojny psychologicznej[28]. Ten przykład wskazuje, że Internet może zostać skutecznie wykorzystany przez organizacje terrorystyczne w sposób jawny. W 2019 r. „The Times of Israel" informował o tym, że Twitter zablokował konta związane z Hamasem, Hezbollahem, Al-Manar (libańska stacja telewizyjna należąca do Hezbollahu) i Quds News Network. Przedstawiciele internetowego serwisu społecznościowego podali, że zawieszone konta propagowały działalność terrorystyczną[29]. Na zwiększające się zagrożenie atakami w cyberprzestrzeni na izraelską infrastrukturę krytyczną i cywilną wskazuje się w przypadku

---

[24] System Iron Dome oblicza trajektorię i kierunek pocisku. Jednocześnie jest uruchamiany alarm przeciwrakietowy w rejonach będących celem ostrzału, a mieszkańcy muszą udać się do schronów. Zob. Y.S. Shapir, *Rocket Warfare in Operation Protective Edge*, w: *The Lessons*…, s. 43, 45.

[25] G. Siboni, *Operations Cast Lead, Pillar of Defense, and Protective Edge:* A *Comparative Review*, w: *The Lessons*…, s. 30–31.

[26] Y.S. Shapir, G. Perel, *Subterranean Warfare: A New-Old Challenge*, w: *The Lessons*…, s. 51.

[27] L. Morris, R. Eglash, *Israel announces operation to destroy Hezbollah tunnels under its northern border*, „The Washington Post", 4 XII 2018 r., https://www.washingtonpost.com/world/middle_east/israel-announces-operation-to-destroy-hezbollah-tunnels-in-its-territory/2018/12/04/f9e74058-f7cb-11e8-8642-c9718a256cbd_story.html [dostęp: 5 VI 2020].

[28] M.G. Bartoszewicz, *Siła czy przesilenie? Działalność i znaczenie Państwa Islamskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 46–48.

[29] A. Rasgon, *Twitter suspends Hamas- and Hezbollah-affiliated handles*, „The Times of Israel", 3 XI 2019 r., https://www.timesofisrael.com/twitter-suspends-hamas-and-hezbollah-affiliated-handles/ [dostęp: 5 VI 2020].

kręgów powiązanych z Iranem[30]. Sieć przyczyniła się także do mobilizacji młodych Palestyńczyków w latach 2015–2016 podczas tzw. intifady noży (ang. *Stabbing Intifada* lub *Knife Intifada*). Charakteryzowała się ona atakami na izraelskich żołnierzy, policjantów i cywili przeprowadzanymi z użyciem noży, nożyczek, maczet oraz innych ostrych przedmiotów, łatwych do schowania pod ubraniem. Ataki były fotografowane lub utrwalane za pomocą telefonów i publikowane w mediach społecznościowych[31]. Te działania spotkały się z poparciem ze strony Hamasu, który uznał je za nową formę walki z Izraelczykami[32]. To wskazuje, że działalność organizacji terrorystycznych lub tzw. samotnych wilków dostosowuje się do rzeczywistości i polega na omijaniu środków kontroli i ochrony przyjętych w Izraelu. Rozwijane są formy ataku z bliska i na odległość, aby móc korzystać z elementu zaskoczenia i potęgować efekt psychologiczny.

Izraelskie ustawodawstwo antyterrorystyczne przed 2016 rokiem

W Izraelu obowiązuje system prawa powszechnego. W rezultacie w państwowym ustawodawstwie funkcjonują przepisy oraz elementy porządku prawnego z czasów Imperium Osmańskiego lub brytyjskiego Mandatu Palestyny. Te standardy obowiązują także w kwestiach bezpieczeństwa. Ministerstwo Sprawiedliwości Izraela podaje, że do 2016 r. najważniejszymi aktami prawnymi, które dotyczyły zwalczania terroryzmu, były wspomniane już: *Przepisy obronne (nadzwyczajne)* z 1945 r., *Rozporządzenie zapobiegające terroryzmowi* z 1948 r., *Prawo zakazu finansowania terroryzmu* z 2005 r. i *Prawo karne (zatrzymany oskarżony o przestępstwo związane z bezpieczeństwem)(Przepis tymczasowy)* z 2006 r.[33]

W 1945 r. władze Mandatu Palestyny wprowadziły *Przepisy obronne (nadzwyczajne)*, które wraz z powstaniem Państwa Izrael stały się częścią jego systemu prawnego. Zawarte w nich zapisy umożliwiały sądzenie cywilów przez sądy wojskowe, izolację określonych obszarów, wprowadzały instytucję przeszukania i konfiskaty oraz godzinę policyjną. Omawiane przepisy zezwalały na wyburzenie domu, którego właściciele wspierali działalność

[30] D. Siman-Tov, Sh. Even, *A New Level in the Cyber War between Israel and Iran*, https://www.inss.org.il/publication/iran-israel-cyber-war/?fbclid=IwAR1QmAUyquwbm3GTJ6eJn39VaJg8USIlOJdMoyyThFbjL9uVkouJy3zwjuI [dostęp: 7 VI 2020].

[31] P. Leurent, *Palestinian 'knife intifada' reflects a generation's despair*, France 24, 6 V 2016 r., https://www.france24.com/en/20160506-reporter-israel-knife-intifada-palestinian-territories-violence [dostęp: 5 VI 2020].

[32] B. Lynfield, *Gaza shootings: Hamas pledge new intifada as ‚day of rage' sees Israeli soldiers kill six Palestinian protesters*, „The Independent", 9 X 2015 r., https://www.independent.co.uk/news/world/middle-east/gaza-shootings-hamas-pledge-new-intifada-as-day-of-rage-sees-israeli-soldiers-kill--six-palestinian-a6688586.html [dostęp: 5 VI 2020].

[33] *2016 – chok ha-maawak be-teror, 5776-2016, kawej gdila*, https://www.gov.il/he/Departments/publications/reports/roots_2016_2 [dostęp: 7 VI 2020].

terrorystyczną lub brali w niej udział[34]. Współcześnie te praktyki są stosowane na obszarze Zachodniego Brzegu, a wyburzanie domów ma stanowić środek odwetowy i zniechęcający do wspierania terroryzmu lub przynależności do organizacji terrorystycznych.

Rozporządzenie zapobiegające terroryzmowi zostało uchwalone w okresie, kiedy Izrael zmagał się z atakami armii arabskich państw ościennych i różnych palestyńskich grup zbrojnych oraz z podziemnymi prawicowymi organizacjami paramilitarnymi, takimi jak Lechi i Irgun[35]. Wówczas organizację terrorystyczną zdefiniowano jako (…) *grupę ludzi stosujących niemoralne działania mogące doprowadzić do śmierci człowieka lub do jego zranienia, lub grożących takimi niemoralnymi działaniami*[36]. Z kolei członkiem organizacji terrorystycznej była (…) *osoba, która uważała się za członka takiej organizacji, brała udział w działaniach tej organizacji, rozpowszechniała informacje na korzyść tej organizacji, jej działań i celów, zbierała fundusze lub przedmioty w celu wsparcia organizacji, lub wsparcia jej działań*[37]. Osoby będące w ścisłym dowództwie organizacji terrorystycznej podlegały karze do 10 lat pozbawienia wolności, biorący udział w działaniach organizacji podlegali karze pozbawienia wolności do lat 5, a wspierający organizację przez propagandę, zbiórkę pieniędzy lub innych rzeczy – karze pozbawienia wolności do lat 3 lub karze grzywny w wysokości 1000 funtów palestyńskich, lub obu wymienionym karom jednocześnie[38]. Było to pierwsze izraelskie prawo penalizujące terroryzm, ale, jak pisze Daphne Barak-Erez, stosowano je głównie wobec organizacji palestyńskich[39].

W 2005 r. w Izraelu uchwalono *Prawo zakazu finansowania terroryzmu*. Wprowadzało ono pojęcia: organizacja terrorystyczna i uznana organizacja terrorystyczna. Różnica między nimi polegała na tym, że ta druga to organizacja uznana za terrorystyczną przez rząd Izraela, komitet ministrów ds. bezpieczeństwa narodowego lub ministra obrony. Natomiast organizacja terrorystyczna to (…) *organizacja, która działa w celu przeprowadzenia aktu terrorystycznego, lub umożliwia albo nawołuje do przeprowadzenia tego aktu, bez znaczenia, czy członkowie organizacji się znają, czy ilość członków jest stała lub zmienna, czy organizacja działa zgodnie z prawem lub w legalnych celach*[40]. Zatem omawiane prawo uzależniało uznanie danej organizacji za terrorystyczną od decyzji organów rządowych lub od „aktu terrorystycznego". Za taki prawo uznawało czyn będący

---

[34] *The Defence (Emergency) Regulations, 1945*, http://nolegalfrontiers.org/military-orders/mil029ed2.html?lang=en#PART_I_-_INTRODUCTORY [dostęp: 5 VI 2020].

[35] D. Barak-Erez, *Israel's anti-terrorism law: past, present and future*, w: *Global Anti-Terrorism Law and Policy*, V.V. Ramraj i in. (red.), Cambridge 2012, s. 589.

[36] *Pkudat mnijat teror 5708–1948*, https://fs.knesset.gov.il/0/law/0_lsr_312695.PDF [dostęp: 5 VI 2020].

[37] Tamże.

[38] Tamże.

[39] D. Barak-Erez, *Israel's anti-terrorism*…, s. 599.

[40] *Chok isur mimun teror 5765–2005*, https://fs.knesset.gov.il/16/law/16_lsr_299751.pdf [dostęp: 6 VI 2020].

przestępstwem, który został lub miał być popełniony w celu wywarcia wpływu na sprawy polityczne, ideologiczne lub religijne przez wywołanie strachu, paniki, nacisku na rząd krajowy lub zagraniczny, zagrożenie życia i mienia, spowodowanie śmierci, zakłócenie działania infrastruktury krytycznej, systemów lub usług[41]. *Prawo zakazu finansowania terroryzmu* w rozdziale trzecim penalizowało finansowanie działalności terrorystycznej, nawoływanie do finansowania działalności, udział w zbieraniu funduszy i nagradzanie za dokonanie aktu terrorystycznego[42]. Gilad Noam pisze, że głównym zarzutem wobec tego prawa jest objęcie postępowaniem administracyjnym lub karnym wyłącznie podmiotów zagranicznych. Wiąże się to z ograniczonymi możliwościami konfiskaty majątku oskarżonych osób lub organizacji. Natomiast wobec podmiotów mających związek z Izraelem mogą być podjęte stanowcze i natychmiastowe działania na podstawie *Przepisów obronnych (nadzwyczajnych)*[43]. Wskazane prawo utrwalało więc stanowisko, że palestyński terroryzm jest wewnętrzną sprawą Izraela. W związku z tym walka z nim powinna się odbywać według przepisów izraelskich, a nie międzynarodowych.

Ostatnim analizowanym aktem prawnym jest *Prawo karne (zatrzymany oskarżony o przestępstwo związane z bezpieczeństwem)(Przepis tymczasowy)* z 2006 r., które wprowadziło do ustawodawstwa kategorię przestępstwa związanego z bezpieczeństwem. Definiowano je jako (…) *przestępstwo popełnione w okolicznościach mogących stanowić zagrożenie dla bezpieczeństwa państwa, również powiązanych z terroryzmem*[44]. W przypadku osób oskarżonych o popełnienie przestępstwa związanego z bezpieczeństwem wskazane prawo wydłuża dozwolony okres przetrzymywania ich w areszcie tymczasowym oraz w areszcie przed wydaniem wyroku (nawet do 96 godzin). Ponadto przepisy zezwalają na przeprowadzenie wielu czynności bez obecności zatrzymanego lub oskarżonego[45].

Prawo zwalczania terroryzmu z 2016 r. wobec współczesnych wyzwań dotyczących zachowania bezpieczeństwa

Dnia 23 czerwca 2016 r. Kneset przyjął *Prawo zwalczania terroryzmu*, o którym na stronie Ministerstwa Sprawiedliwości Izraela napisano, że jest najbardziej kompleksowe. Jest ono sumą doświadczeń zebranych z wcześniejszych przepisów, a jego uchwalenie zniosło obowiązywanie praw opisanych powyżej[46]. Prawo, o którym mowa,

---

41 Tamże.

42 Tamże.

43 G. Noam, *Hitmodedut ha-miszpatit bi-Israel im tofaat mimun ha-teror*, Jeruszalaim 2009, s. 69–70.

44 *Chok seder ha-din ha-plili (acur he-chaszud ba-awirut bitachon)(horaat szaa) 5766–2006*, https://fs.knesset.gov.il/17/law/17_lsr_300016.pdf [dostęp: 6 VI 2020].

45 Tamże.

46 *2016 – chok ha-maawak be-teror, 5776-2016, kawej gdila*, https://www.gov.il/he/Departments/publications/reports/roots_2016_2 [dostęp: 7 VI 2020].

jeszcze przed przyjęciem stało się źródłem wielu kontrowersji związanych z prawami człowieka i kompetencjami różnych organów[47].

Już w pierwszym artykule zaznaczono, że celem prawa jest zapobieganie powstawaniu, funkcjonowaniu i działaniu organizacji terrorystycznych, a także zapobieganie działalności terrorystycznej. We wstępie wskazano także, że przepisy respektują prawo humanitarne przy jednoczesnym uwzględnieniu interesów strategicznych Izraela i niebezpieczeństw, jakie niesie terroryzm dla obywateli kraju i instytucji tego państwa[48].

Prawo zwalczania terroryzmu w artykule drugim podaje aż trzy definicje pojęcia organizacja terrorystyczna. Jest nią:

1. Grupa ludzi o charakterze ciągłym i zorganizowanym, która dokonuje aktów terrorystycznych lub działa w celu ich przeprowadzenia, włączając w to wspomnianą organizację, która zajmuje się szkoleniem i przygotowywaniem do przeprowadzenia aktu, lub działa z użyciem broni, lub handluje bronią w celu przeprowadzenia aktu (…);
2. Grupa ludzi o charakterze ciągłym i zorganizowanym, która działa w sposób bezpośredni lub pośredni w celu wspomożenia organizacji z paragrafu (1), lub w celu promowania działań wspomnianej organizacji, włączając w to finansowanie w sposób znaczny lub ciągły działań tej organizacji, lub będąca w związku z tą organizacją (…);
3. Organizacja uznana za terrorystyczną poza granicami Państwa Izrael (…)[49].

Powyższe wskazuje, że nowe spojrzenie na to, czym jest organizacja terrorystyczna, wykracza poza samą działalność terrorystyczną, koncentrując się również na organizacjach udzielających wsparcia lub propagujących działania terrorystyczne. Może to jednak prowadzić do nadużyć ze strony służb bezpieczeństwa.

Nowe prawo rozszerzyło także definicję pojęcia członek organizacji terrorystycznej. Jest nim nie tylko członek takiej organizacji czy osoba, która w jakikolwiek sposób bierze udział w działalności organizacji terrorystycznej lub działa jako przedstawiciel albo wysłannik tej organizacji, lecz także ten, kto wyraził chęć przystąpienia do organizacji terrorystycznej, kto jest postrzegany jako przedstawiciel tej organizacji[50].

Akt terrorystyczny uznaje się za taki, jeśli stanowi przestępstwo lub groźbę popełnienia takiego przestępstwa, a także jeżeli:

– został popełniony z pobudek politycznych, religijnych, nacjonalistycznych lub ideologicznych;

---

47 J. Lis, *Bikurat al. chok ha-teror: kimat bilti efszari lehitgonen mifnejo*, „Ha-Arec", 7 VI 2013 r., https://www.haaretz.co.il/news/politics/1.2040313 [dostęp: 7 VI 2020].

48 *Chok ha-maawak be-teror, 5776–2016*, https://fs.knesset.gov.il/20/law/20_lsr_343902.pdf [dostęp: 9 VI 2020].

49 Tamże.

50 Tamże.

– miał na celu wywołanie strachu i paniki lub jego intencją był nacisk na krajowy lub zagraniczny rząd, instytucję rządową lub instytucję międzynarodową w celu zmuszenia do jakiejś decyzji albo wstrzymania się od jej podjęcia;
– jego przeprowadzenie lub możliwość jego przeprowadzenia wywołały lub stanowiły poważne zagrożenie jednego z elementów, takich jak: ludzkie życie, wolność, własność, bezpieczeństwo, obiekty religijne i kultu religijnego, infrastruktura krytyczna, strategiczne systemy i usługi, środowisko i państwowa gospodarka[51].

Ponadto za akt terrorystyczny prawo uznaje przestępstwo popełnione z użyciem broni lub broni białej, skutkujące lub mogące skutkować poważnymi obrażeniami ciała, nawet jeśli nie było one popełnione z pobudek religijnych, nacjonalistycznych, politycznych lub ideologicznych. Za akt terrorystyczny uznaje się także atak na duży obszar lub skupisko ludzi przeprowadzony z użyciem broni biologicznej, chemicznej, radioaktywnej lub substancji szkodliwej, również bez wyżej wymienionych pobudek[52]. Omawiane prawo wprowadziło pojęcie własność organizacji terrorystycznej, przez którą rozumie się własność będącą w posiadaniu, pod kontrolą lub kuratelą takiej organizacji, a także wszystko, co służy do przeprowadzania aktów terroru, oraz własność, której pozyskanie zostało sfinansowane przez inny podmiot, lub własność, która była darowizną[53]. Warstwa definicyjna aktu wskazuje na szerokie ujęcie pojęć: „organizacja terrorystyczna", „akt terrorystyczny", a nawet „członek organizacji terrorystycznej".

Kolejna istotna część tego prawa dotyczy organów odpowiedzialnych za bezpieczeństwo i uznania organizacji za terrorystyczną lub osoby za terrorystę. Zgodnie z przepisami do służb bezpieczeństwa zalicza się: Szabak, Mosad, Armię Obrony Izraela oraz Policję Izraela[54]. Minister obrony uznaje organizację za terrorystyczną na wniosek szefa Szabaku lub innej służby bezpieczeństwa wymienionej w prawie. Co więcej, w wyjątkowej sytuacji, na prośbę ministra obrony, taką decyzję może podjąć premier lub komitet ministrów. Prawo zakłada ponadto stworzenie Komitetu Doradczego powoływanego przez ministra sprawiedliwości. Zadaniem komitetu będzie okresowa weryfikacja istniejącego stanu rzeczy lub wychwycenie nowych okoliczności i faktów wpływających na uznanie organizacji za terrorystyczną. Nowe ustawodawstwo zakłada, że jeżeli inne państwo, Organizacja Narodów Zjednoczonych lub jakakolwiek struktura wyspecjalizowana w dziedzinie bezpieczeństwa (np. Rada Bezpieczeństwa ONZ) określą jakąś organizację za terrorystyczną, a osobę za terrorystę lub też zaprzestaną je ze takie uważać, to minister obrony może zasięgnąć opinii ministra spraw zagranicznych w celu podjęcia wymaganej decyzji[55]. Specjalne uprawnienia w związku ze zwalczaniem aktywności terrorystycznej ma komendant dystryktu[56]

[51] Tamże.

[52] Tamże.

[53] Tamże.

[54] Tamże.

[55] Tamże.

[56] Dystrykt jest w Izraelu główną jednostką administracyjną podziału terytorium. W całym państwie

Policji Izraela. Jeżeli istnieją uzasadnione przesłanki, że na podlegającym mu obszarze działalność prowadzą organizacje terrorystyczne lub dochodzi do spotkań, demonstracji czy też wspierania tego rodzaju działalności, to ma on prawo wydać zarządzenie o zwalczaniu takiej aktywności z podaniem wymaganego na to czasu. Podobne kompetencje przysługują komendantom dystryktu w przypadku miejsc wykorzystywanych do prowadzenia zakazanej działalności. Mogą oni wyłączyć takie miejsce z użytku na okres nie dłuższy niż trzy miesiące, z możliwością przedłużenia do sześciu miesięcy[57]. W 2018 r. Kneset uchwalił poprawkę nr 3 do *Prawa zwalczania terroryzmu*, która nadaje Policji Izraela specjalne uprawnienie. Pozwala ono komendantom na wydanie zakazu przemarszu pogrzebowego i przeprowadzenia pogrzebu, jeżeli istnieje przesłanka, że w ich trakcie może dojść do naruszenia porządku, zasad bezpieczeństwa, agitacji na rzecz organizacji terrorystycznej czy uszkodzenia ciała lub mienia. Ponadto komendanci mogą wstrzymać wydanie ciała o 10 dni, do momentu, kiedy zostaną spełnione warunki bezpieczeństwa wymagane przez prawo[58]. Policja jest uprawniona do zatrzymania podejrzanego na 48 godzin przed rozprawą sądową. Służby bezpieczeństwa mogą wystąpić do ministra obrony z prośbą o administracyjne zajęcie majątku nie tylko organizacji terrorystycznej lub terrorysty, lecz także grupy nieuznanej za terrorystyczną, której działalność może wspierać organizacje przestępcze lub te, które są w posiadaniu majątku organizacji przestępczych. Jeżeli osoba uznana za terrorystę będzie wjeżdżać do Izraela, to służby mają prawo zająć jej majątek już w dniu przekroczenia granicy. Z kolei Szabak uzyskał uprawnienie do inwigilacji cyfrowej każdej osoby podejrzanej o terroryzm[59].

Prawo zwalczania terroryzmu wprowadziło także obszerny katalog przestępstw związanych z działalnością terrorystyczną lub jej wspieraniem. Wymienione są w nim m.in.:

- dowództwo nad organizacją terrorystyczną lub znajdowanie się w jej organach zarządzających – kara 15 lat pozbawienia wolności;
- członkostwo w organizacji – 5 lat;
- rekrutacja do organizacji, działanie w jej imieniu lub intencja takiego działania – 7 lat;
- zapewnianie usług, dóbr organizacji lub jej wspieranie – 5 lat;
- utożsamianie się z organizacją (m.in. używanie jej symboliki, wyrażanie sympatii, udostępnianie pieśni) – 3 lata;
- bezpośrednie nawoływanie do popełnienia aktu terrorystycznego – 5 lat;
- świadome lub nieświadome ułatwianie przeprowadzenia aktu terrorystycznego – 5 lat;
- grożenie przeprowadzeniem aktu terrorystycznego – 7 lat;

---

jest ich siedem (włączając w to Judeę i Samarię, czyli Zachodni Brzeg).

[57] *Chok ha-maawak be-teror, 5776–2016…*

[58] *Chok ha-maawak be-teror (tikun mispar 3), 5778–2018*, https://fs.knesset.gov.il/20/law/20_lsr_491925.pdf [dostęp: 18 VI 2020].

[59] *Chok ha-maawak be-teror, 5776–2016…*

– przygotowywanie do przeprowadzenia aktu terrorystycznego – 15 lat;
– przeprowadzanie szkoleń i instruktaży na potrzeby działalności terrorystycznej – 9 lat;
– branie udziału w szkoleniach i instruktażach – 7 lat;
– posiadanie, sprzedaż, handel, wytwarzanie, naprawa, import, eksport, transport broni w celu wsparcia organizacji lub przeprowadzenia ataku – 20 lat, a zrobienie tego samego w przypadku broni biologicznej, chemicznej, radioaktywnej – 25 lat;
– przeprowadzenie ataku terrorystycznego, w tym ataku z użyciem broni chemicznej, biologicznej lub radioaktywnej – kara dożywotniego pozbawienia wolności[60].

Ponadto zakazuje się przeprowadzania jakichkolwiek transakcji na rzecz organizacji terrorystycznych, w ich imieniu, w celu udzielenia im wsparcia finansowego, wsparcia ich działalności lub w celu wynagradzania za działalność terrorystyczną[61].

Podsumowanie

Z powyższej analizy wynika, że izraelskie prawo dotyczące zwalczania terroryzmu i zapewniania bezpieczeństwa stanowi sumę doświadczeń z przeszłości. Wyraża ono stanowisko, zgodnie z którym to rząd ma pełne prawo do decydowania, w jaki sposób definiuje zagrożenia i z nimi walczy. Rozwój metod stosowanych przez organizacje terrorystyczne doprowadził Izrael do rozbudowy i aktualizacji ustawodawstwa mającego przeciwdziałać temu zjawisku. Przeprowadzona analiza wskazuje na intencję jak najszerszego zdefiniowania zjawisk związanych z terroryzmem i działalnością wymierzoną w państwo, jego instytucje i obywateli. W tym miejscu należy zaznaczyć, że Państwo Izrael stara się przeciwdziałać terroryzmowi, korzystając z rozbudowanych i kontrowersyjnych środków w podobny sposób, w jaki władze mandatowe zwalczały żydowskie podziemie przed 1948 r. Jednocześnie argument zapewnienia bezpieczeństwa wewnętrznego jest dla Izraela głównym czynnikiem legitymizującym działania przedstawione powyżej.

W percepcji izraelskiej zjawisko terroryzmu jest ujmowane szeroko – nie tylko jako prowadzenie działalności terrorystycznej, lecz także jako udzielanie organizacji wsparcia z zewnątrz, utożsamianie się z nią lub propagowanie jej działalności. Można to uznać za przeciwdziałanie zagrożeniom XXI w. związanym z aktywnością terrorystyczną w sieci, udostępnianiem materiałów propagandowych, rekrutowaniem lub nawoływaniem do przystąpienia do takich organizacji. Takie pojmowanie zagrożeń wynika również ze sceptycznego stosunku izraelskiej prawicy do działań organizacji pozarządowych, które skupiają się na monitorowaniu przestrzegania praw człowieka lub udzielają pomocy finansowej Palestyńczykom. Muszą one m.in. ujawniać swoje źródła zagranicznego finansowania,

[60] Tamże.

[61] Tamże.

co jest krytykowane przez Unię Europejską[62]. Duży zakres pojęcia „terroryzm" w myśl teorii sekurytyzacji pozwala władzy na swobodne definiowanie zagrożeń bezpieczeństwa państwa, jego instytucji oraz obywateli. Obszerny zbiór zagrożeń umożliwia z kolei służbom odpowiedzialnym za bezpieczeństwo tworzenie rozbudowanego katalogu narzędzi służących do walki z nimi, co może prowadzić do nadużywania kompetencji tych służb.

Na podstawie nowego ustawodawstwa za przestępstwo o charakterze terrorystycznym można uznać kopanie tuneli wykorzystywanych przez Hamas lub Hezbollah czy też wspomniane ataki przy użyciu noży. Oba te działania były prezentowane jako istotne zagrożenia porządku i bezpieczeństwa[63]. Największe kontrowersje związane z tym prawem wzbudza możliwość uznania dowolnej organizacji (charytatywnej, pozarządowej) za wspierającą terroryzm, jeżeli między nią a działalnością terrorystyczną istnieje pośredni związek lub kontakt. W trakcie uchwalania prawa, o którym mowa, zwracano uwagę, że takie zapisy mogą prowadzić do łamania prawa międzynarodowego lub praw człowieka[64]. Za budzące wątpliwości z punktu widzenia wolności religijnej można uznać również zapisy dotyczące możliwości opóźnienia wydania ciała rodzinie w momencie, kiedy służby bezpieczeństwa uznają, że pogrzeb może przerodzić się w wiec poparcia dla organizacji terrorystycznej lub z użyciem jej symboliki. Przy częstych napięciach w stosunkach izraelsko-palestyńskich te przepisy mogą być wykorzystywane jako środek prewencyjny, dochodzi jednak do nadużywania uprawnień. Już rok po przegłosowaniu wspomnianego prawa Sąd Najwyższy Izraela orzekł, że służby bezpieczeństwa notorycznie wykorzystywały nowe zapisy umożliwiające przetrzymywanie ciał, co miało być niezgodne z prawem. Nakazano władzom wydanie wszystkich ciał w ciągu sześciu miesięcy oraz rozpoczęcie prac nad zmianami zapisów dotyczących tych zagadnień[65].

Warto także zwrócić uwagę na to, że zbieranie pieniędzy i wypłacanie zapomóg rodzinom męczenników i więźniów jest uznawane za przestępstwo[66]. Na początku 2020 r. weszły w życie zarządzenia Armii Obrony Izraela wprowadzające zapisy *Prawa zwalczania terroryzmu* na Zachodnim Brzegu. W związku z tym banki, które miały

---

[62] *EU criticises Israel law forcing NGOs to reveal foreign funding*, BBC, 12 VI 2016 r., https://www.bbc.com/news/world-middle-east-36775032 [dostęp: 22 VI 2020]; *Israeli government targets foreign government funding of NGOs*, Reuters, 27 XII 2015 r., https://www.reuters.com/article/us-israel-palestinians-ngo/israeli-government-targets-foreign-government-funding-of-ngos-idUSKBN0UA0EE20151227 [dostęp: 22 VI 2020].

[63] Intifada noży przyczyniła się do zwiększenia zabezpieczeń w Izraelu. Zamontowano m.in. wykrywacze metali przy wejściu na obszar przy Ścianie Płaczu, co doprowadziło do sporów izraelsko-palestyńskich i wśród samych Izraelczyków. Broń biała jest łatwiejsza do ukrycia, a jej nabycie nie wymaga korzystania z sieci powiązań i dużych nakładów finansowych.

[64] Z. Kam, *„Maane model 2016": chok ha-maawak be-teror uszar ba-Kneset*, „Makor Riszon", 15 VI 2016 r., https://www.makorrishon.co.il/nrg/online/1/ART2/788/479.html [dostęp: 22 VI 2020].

[65] J.A. Gross, *High Court: Israel can't keep holding terrorists' bodies without a law*, „The Times of Israel", 14 XII 2017 r., https://www.timesofisrael.com/high-court-israel-cant-keep-holding-terrorists-bodies-without-a-law/ [dostęp: 22 VI 2020].

[66] Hamas oraz władze Autonomii Palestyńskiej wypłacają specjalne świadczenia rodzinom, których członkowie zginęli jako męczennicy lub odbywają w więzieniu karę pozbawienia wolności.

swoje oddziały na tym obszarze, poprosiły rodziny otrzymujące świadczenia od Hamasu lub Autonomii Palestyńskiej, aby w celu utrzymania możliwości dalszego korzystania z takich funduszy zamknęły swoje konta bankowe i przeniosły je do innych banków[67]. Na podstawie nowego prawa doszło również do zatrzymań pojedynczych osób, które miały dokonywać przelewów dla rodzin osób przebywających w izraelskich więzieniach[68].

Powyższa analiza pozwala stwierdzić, że zapisy o międzynarodowym terroryzmie i jego zwalczaniu mają uwiarygadniać potrzebę zapewnienia szerokich i kontrowersyjnych kompetencji służbom odpowiedzialnym za bezpieczeństwo. Wynika z nich również, że walka z palestyńskim terroryzmem została uznana za wewnętrzną sprawę Izraela. Pisze o tym Szydzisz, który podkreśla wagę terroryzmu w kreowaniu izraelskiej polityki bezpieczeństwa, dopuszczającej stosowanie środków nadzwyczajnych w walce z nim[69]. Te wnioski znajdują odzwierciedlenie w izraelskich badaniach opinii publicznej, w których Izraelczycy wyrażają poparcie dla stosowania radykalnych środków walki z terroryzmem oraz postrzegają terroryzm (pod postacią działalności Hamasu i Hezbollahu) jako główne zagrożenie państwa[70]. W 2016 r. 46,8 proc. Izraelczyków uważało, że Palestyńczyk przeprowadzający atak terrorystyczny powinien zostać zabity na miejscu. Z kolei 44,4 proc. Izraelczyków wyraziło obawę, że oni sami lub członkowie ich rodzin każdego dnia mogą stać się ofiarami ataku. Wśród badanych 49 proc. zaakceptowałoby w walce z terroryzmem środki łamiące prawa człowieka lub je ignorujące[71]. Stwarza to stan rzeczy, w którym instytucje rządowe, mimo sprzeciwu międzynarodowego, mogą korzystać z nastrojów społecznych w celu implementacji kompleksowego ustawodawstwa, przyznającego państwu szerokie kompetencje i narzędzia walki z terroryzmem. Sytuacja, w której obywatele będący obiektem referencyjnym postrzegają terroryzm w ten sam sposób, ułatwia politykom przekonanie odbiorców komunikatów do zaakceptowania nowych środków nadzwyczajnych.

---

67 *No pay to slay? Fearing Israel law, Palestinian bank blocks terrorists' accounts*, „The Times of Israel", 7 V 2020 r., https://www.timesofisrael.com/palestinian-banks-said-to-block-terror-convicts-accounts-due-to-new-israeli-law/ [dostęp: 22 VI 2020].

68 *6 East Jerusalemites arrested for violating anti-terrorism laws*, „The Times of Israel", 15 V 2019 r., https://www.timesofisrael.com/6-east-jerusalemites-arrested-for-violating-anti-terrorism-laws/ [dostęp: 22 VI 2020].

69 M. Szydzisz, *Sekurytyzacja jak narzędzie…*, s. 249–251.

70 *Israeli Public Opinion Polls: Opinions On Fighting with Hamas*, https://www.jewishvirtuallibrary.org/israeli-opinions-on-fighting-with-hamas [dostęp: 22 VI 2020]; *Israeli Public Opinion Polls: Opinion on War with Hezbollah*, https://www.jewishvirtuallibrary.org/israeli-opinion-on-the-war-with-hezbollah [dostęp: 22 VI 2020].

71 *Israeli Public Opinion Polls: Opinion Toward Terrorism (2008 - 2016)*, https://www.jewishvirtuallibrary.org/israeli-opinion-toward-terrorism-2008-2010 [dostęp: 22 VI 2020].

Bibliografia

Barak-Erez D., *Israel's anti-terrorism law: past, present and future*, w: *Global Anti-Terrorism Law and Policy*, V.V. Ramraj i in. (red.), Cambridge 2012, Cambridge University Press.

Bartoszewicz M.G., *Siła czy przesilenie? Działalność i znaczenie Państwa Islamskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 39–65.

Buzan B., Hansen L., *The Evolution of International Security Studies*, Cambridge 2009, Cambridge University Press.

Buzan B., Wæver O., de Wilde J., *Security. A New Framework for Analysis*, Boulder 1998, Lynne Reiner Publishers.

Chodubski A.J., *Wstęp do badań politologicznych*, Gdańsk 2004, Wydawnictwo Uniwersytetu Gdańskiego.

Estrategijat Cahal, Tel Awiw 2015.

Ganor B., *Global Alert. The Rationality of Modern Islamist Terrorism and the Challenge to the Liberal Democratic World*, New York 2015, Columbia University Press.

Noam G., *Hitmodedut ha-miszpatit bi-Israel im tofaat mimun ha-teror*, Jeruszalaim 2009, Ha-merkaz le-bitachon we-demokratija.

Peleg I., *The Israeli Right*, w: *Contemporary Israel. Domestic Politics, Foreign Policy, and Security Challenges*, R.O. Freedman (red.), Boulder 2009, Routledge.

Schweitzer Y., *Defning the Victor in the Fight against an Army of "Terrorilla"*, w: *The Lessons of Operation Protective Edge*, A. Kurz, S. Brom (red.), Tel Aviv 2014, Institute for National Security Studies.

Shapir Y.S., *Rocket Warfare in Operation Protective Edge*, w: *The Lessons of Operation Protective Edge*, A. Kurz, S. Brom (red.), Tel Aviv 2014, Institute for National Security Studies.

Shapir Y.S., Perel G., *Subterranean Warfare: A New-Old Challenge*, w: *The Lessons of Operation Protective Edge*, A. Kurz, S. Brom (red.), Tel Aviv 2014, Institute for National Security Studies.

Siboni G., *Operations Cast Lead, Pillar of Defense, and Protective Edge: A Comparative Review*, w: *The Lessons of Operation Protective Edge*, A. Kurz, S. Brom (red.), Tel Aviv 2014, Institute for National Security Studies.

Sielezin J.R., *Badania źródłoznawcze w politologii. Wybrane zagadnienia metodologiczne*, Wrocław 2010, Wydawnictwo Uniwersytetu Wrocławskiego.

Szydzisz M., *Sekurytyzacja jako narzędzie polityki zagranicznej Izraela w świetle teorii regionalnych kompleksów bezpieczeństwa*, Warszawa 2019, Wydawnictwo Uniwersytetu Warszawskiego.

Źródła internetowe

EU criticises Israel law forcing NGOs to reveal foreign funding, BBC, 12 VI 2016 r., https://www.bbc.com/news/world-middle-east-36775032 [dostęp: 22 VI 2020].

Gross J.A., *High Court: Israel can't keep holding terrorists' bodies without a law*, „The Times of Israel", 14 XII 2017 r., https://www.timesofisrael.com/high-court-israel-cant-keep-holding-terrorists-bodies-without-a-law/ [dostęp: 22 VI 2020].

Israeli government targets foreign government funding of NGOs, Reuters, 27 XII 2015 r., https://www.reuters.com/article/us-israel-palestinians-ngo/israeli-government-targets-foreign--government-funding-of-ngos-idUSKBN0UA0EE20151227 [dostęp: 22 VI 2020].

Israeli Public Opinion Polls: Opinions on Fighting with Hamas, https://www.jewishvirtuallibrary.org/israeli-opinions-on-fighting-with-hamas [dostęp: 22 VI 2020].

Israeli Public Opinion Polls: Opinion on War with Hezbollah, https://www.jewishvirtuallibrary.org/israeli-opinion-on-the-war-with-hezbollah [dostęp: 22 VI 2020].

Israeli Public Opinion Polls: Opinion Toward Terrorism (2008 - 2016), https://www.jewishvirtuallibrary.org/israeli-opinion-toward-terrorism-2008-2010 [dostęp: 22 VI 2020].

Kam Z., *„Maane model 2016": chok ha-maawak be-teror uszar ba-Kneset*, „Makor Riszon", 15 VI 2016 r., https://www.makorrishon.co.il/nrg/online/1/ART2/788/479.html [dostęp: 22 VI 2020].

Kremnicer M., Szani J., Foks A., *Hacaat chok ha-maawak be-teror 5771–2011*, https://www.idi.org.il/articles/7757 [dostęp: 1 VI 2020].

Leurent P., *Palestinian 'knife intifada' reflects a generation's despair*, France 24, 6 V 2016 r., https://www.france24.com/en/20160506-reporter-israel-knife-intifada-palestinian-territories-violence [dostęp: 5 VI 2020].

Lis J., *Bikurat al. chok ha-teror: kimat bilti efszari lehitgonen mifnejo*, „Ha-Arec", 7 VI 2013 r., https://www.haaretz.co.il/news/politics/1.2040313 [dostęp: 7 VI 2020].

Lynfield B., *Gaza shootings: Hamas pledge new intifada as ‚day of rage' sees Israeli soldiers kill six Palestinian protesters*, „The Independent", 9 X 2015 r., https://www.independent.co.uk/news/world/middle-east/gaza-shootings-hamas-pledge-new-intifada-as-day-of-rage-sees-israeli-soldiers-kill-six-palestinian-a6688586.html [dostęp: 5 VI 2020].

Morris L., Eglash R., *Israel announces operation to destroy Hezbollah tunnels under its northern border*, „The Washington Post", 4 XII 2018 r., https://www.washingtonpost.com/world/middle_east/israel-announces-operation-to-destroy-hezbollah-tunnels-in-its-territory/2018/12/04/f9e74058-f7cb-11e8-8642-c9718a256cbd_story.html [dostęp: 5 VI 2020].

No pay to slay? Fearing Israel law, Palestinian bank blocks terrorists' accounts, „The Times of Israel", 7 V 2020 r., https://www.timesofisrael.com/palestinian-banks-said-to-block-terror-convicts-accounts-due-to-new-israeli-law/ [dostęp: 22 VI 2020].

Rasgon A., *Twitter suspends Hamas- and Hezbollah-affiliated handles*, „The Times of Israel", 3 XI 2019 r., https://www.timesofisrael.com/twitter-suspends-hamas-and-hezbollah-affiliated--handles/ [dostęp: 5 VI 2020].

Siman-Tov D., Even Sh., *A New Level in the Cyber War between Israel and Iran*, https://www.inss.org.il/publication/iran-israel-cyber-war/?fbclid=IwAR1QmAUyquwbm3GTJ6eJn39VaJg8USIlOJdMoyyThFbjL9uVkouJy3zwj [dostęp: 7 VI 2020].

2016 – chok ha-maawak be-teror, 5776-2016, kawej gdila, https://www.gov.il/he/Departments/publications/reports/roots_2016_2 [dostęp: 7 VI 2020].

Akty prawne

Chok ha-maawak be-teror, 5776–2016, https://fs.knesset.gov.il/20/law/20_lsr_343902.pdf [dostęp: 9 VI 2020].

Chok ha-maawak be-teror (tikun mispar 3), 5778–2018, https://fs.knesset.gov.il/20/law/20_lsr_491925.pdf [dostęp: 1 VI 2020].

Chok seder ha-din ha-plili (acur he-chaszud ba-awirut bitachon)(horaat szaa) 5766–2006, https://fs.knesset.gov.il/17/law/17_lsr_300016.pdf [dostęp: 6 VI 2020].

Pkudat mnijat teror 5708–1948, https://fs.knesset.gov.il/0/law/0_lsr_312695.PDF [dostęp: 5 VI 2020].

The Defence (Emergency) Regulations, 1945, http://nolegalfrontiers.org/military-orders/mil029ed2.html?lang=en#PART_I_-_INTRODUCTORY [dostęp: 5 VI 2020].

Abstrakt

Artykuł ma na celu przedstawienie założeń *Prawa zwalczania terroryzmu* uchwalonego w 2016 r. w Izraelu w zakresie definiowania i, zwalczania terroryzmu oraz sankcjonowania przestępstw z nim związanych. Autor ukazuje izraelską percepcję tych zagrożeń uwidaczniającą się w nowym ustawodawstwie. Zostanie ona zestawiona z przepisami obowiązującymi wcześniej, aby pokazać, jak zmieniało się postrzeganie tych zagadnień przez rządzących i jakie zmiany wprowadziło nowe prawo. W tym celu autor zastosuje metodę instytucjonalno-prawną i metodę porównawczą różnicy, a także skorzysta z teorii sekurytyzacji. Przeprowadzona analiza pozwoli mu na stwierdzenie, że z perspektywy rządzących terroryzm jest nadal uważany za główne zagrożenie Państwa Izrael. Prawo z 2016 r. wprowadziło możliwość zastosowania wielu środków

nadzwyczajnych w ramach przeciwdziałania temu zjawisku. To pokazuje, że partie, które je uchwaliły, mają jastrzębie spojrzenie na kwestie związane z walką z terroryzmem.

Słowa kluczowe: Izrael, antyterroryzm, polityka bezpieczeństwa Izraela, ustawodawstwo antyterrorystyczne Izraela, konflikt izraelsko-palestyński.

Israeli counter-terrorist legislation against the threats of the 21st century

Abstract

The aim of the article is to present objectives of the Israeli Counter-Terrorism Law passed in 2016. The author examines the way of defining and combating terrorism, and the penalty measures related to criminal activity linked with it. Thus, the author shows the Israeli authorities' perception of threat connected with terrorism. The previous counter-terrorist law is compared with the new one to demonstrate the modification of the vision of security. The article seeks to answer the question what changes and views have been implemented by the new law. To achieve those aims the author used the comparison method and an analysis of the law and the securitization theory. It allowed to state that terrorism is still regarded by Israeli politicians as the main threat for the State of Israel and its citizens. The amended law allowed for the use of many emergency measures. Overall, it exhibits a hawkish stance towards combating terrorism of parties which amended the law.

Keywords: Israel, counter-terrorism, the Israeli security policy, the Israeli counter-terrorism legislation, the Israeli-Palestinian conflict.

PAWEŁ GACEK
ORCID: 0000-0001-6365-3146

DOI: 10.4467/20801335PBW.21.005.13562

Zakaz członkostwa w partii politycznej funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu oraz uczestnictwa w działalności tej partii lub na jej rzecz

Zagadnienia wstępne. Szczególny charakter służby publicznej

Służba publiczna ma charakter selekcyjny. To oznacza, że nie każdy, kto się ubiega o przyjęcie do niej, musi zostać przyjęty. Wszystkie formacje zmilitaryzowane (paramilitarne) odrębnie określają wymogi, których spełnienie umożliwia nawiązanie więzi prawnej z kandydatem do służby, tj. stosunku służbowego[1]. Również w art. 44 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[2] (dalej: ustawa o ABW oraz AW) enumeratywnie zostały wskazane cechy, jakimi powinna legitymować się osoba fizyczna zgłaszająca gotowość podjęcia służby w tych formacjach[3]. Jedną z nich jest warunek wymieniony w art. 44 pkt 5 ustawy o ABW oraz AW[4]. Kandydat do służby musi być gotowy do poddania się szczególnego rodzaju

---

[1] Szerzej na temat stosunku służbowego zob. T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy*, w: *System prawa administracyjnego*, t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2011; P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych i żołnierzy zawodowych jako sprawa administracyjna*, Warszawa 2012; M. Wieczorek, *Charakter prawny stosunków służbowych funkcjonariuszy służb mundurowych*, Toruń 2017; także: P. Gacek, *Nawiązanie stosunku służbowego z funkcjonariuszem Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Charakter prawny mianowania – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 98 i nast., i przywołana tam literatura.

[2] Tekst jednolity: DzU z 2020 r. poz. 27, ze zm.

[3] Szerzej na ten temat zob. P. Gacek, *Wymogi formalne niezbędne do pełnienia służby w Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 56 i nast.

[4] Zgodnie z tym przepisem służbę w ABW albo AW może pełnić osoba mająca wykształcenie co najmniej średnie lub średnie branżowe i określone kwalifikacje zawodowe oraz zdolność fizyczną

reżimowi obowiązującemu w tego typu formacjach. Musi zatem mieć świadomość, że służba publiczna wiąże się ze szczególnymi i specyficznymi ograniczeniami nieznanymi innym grupom zawodowym, których podstawą zatrudnienia jest stosunek pracy. Służba nie jest bowiem zwykłą pracą najemną. Nie stanowi więc stosunku pracy. Stosunek służbowy jest usytuowany w sferze prawa administracyjnego. Jego kształt jest *stricte* administracyjnoprawny, z czego wynika, że jego ramy w sposób jednostronny i władczy określa organ administracyjny. Nie oznacza to jednak możliwości uregulowania go w sposób dowolny, gdyż poszczególne elementy kształtujące ten stosunek wynikają wprost z konkretnych przepisów pragmatyki służbowej. Podmiot zatrudniający (o którym mowa w art. 50 ust. 1 ustawy o ABW oraz AW, tj. Szef ABW lub Szef AW) nie może więc arbitralnie określić warunków służby funkcjonariusza, z którym nawiązuje stosunek służbowy. Kandydat do służby nie uczestniczy z kolei w kształtowaniu powstałej z nim więzi prawnej. Może przyjąć w całości zaproponowane warunki lub je odrzucić. Nie może ich negocjować, ponieważ stosunek służbowy nie jest stosunkiem obligacyjnym, którego kształt jest określany w drodze zgodnych oświadczeń woli stron tego stosunku. Nawiązanie stosunku służbowego musi poprzedzać dobrowolne zgłoszenie się osoby fizycznej (kandydata) do służby. Jak słusznie zauważa Przemysław Szustakiewicz, do służby w ABW lub AW (a także do innych formacji zmilitaryzowanych lub paramilitarnych) nie można zostać „wcielonym". Kandydat zgłaszający gotowość do podjęcia służby w formacji zmilitaryzowanej (paramilitarnej) jest zobligowany przede wszystkim do wykazania woli poddania się jej rygorom[5]. Dobrowolność jest podstawowym wymogiem pełnienia służby. Tym samym oświadczenie kandydata o dobrowolnym zgłoszeniu się do służby musi immanentnie łączyć się z dobrowolnym oświadczeniem, z którego wynika, że jest on gotów poddać się rygorom tej służby. Zatem musi on wykazać się aktywnością, która w ocenie podmiotu zatrudniającego będzie mogła być uznana za spełnienie tego podstawowego wymogu. Z kolei spełnienie wymogów wskazanych w art. 44 ustawy o ABW oraz AW stanowi nie tylko warunek wstępny, umożliwiający nawiązanie stosunku służbowego, lecz także jest niezbędne do jego kontynuowania przez funkcjonariuszy ABW i AW. Konieczne jest więc zaakcentowanie, że warunki, o których mowa, dotyczą zarówno kandydatów do służby, jak i czynnych funkcjonariuszy ABW i AW.

Istnieją jednak jeszcze inne uwarunkowania (obowiązki, nakazy i zakazy), które zaczynają obowiązywać w związku z nawiązaniem stosunku służbowego. Odnoszą się one wyłącznie do funkcjonariuszy ABW oraz AW i wytyczają sferę ich dozwolonego zachowania jako funkcjonariuszy publicznych i członków formacji zhierarchizowanych i zmilitaryzowanych. Nie są one badane w trakcie trwającego postępowania

---

i psychiczną do służby w formacjach uzbrojonych, wymagających szczególnej dyscypliny służbowej, której taka osoba jest gotowa się podporządkować.

[5] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis (komentarz do art. 48 ustawy o ABW oraz AW).

kwalifikacyjnego, gdyż nie dotyczą kandydatów do służby. Materializują się z kolei w momencie, gdy osoba fizyczna nabywa status funkcjonariusza. Ich przestrzeganie jest świadectwem dobrowolnego podporządkowania się, przestrzegania dyscypliny służbowej i – w szerszym aspekcie – zdolności funkcjonariusza do poddania się reżimowi wynikającemu z charakteru pełnionej służby. Dobrowolność jest podstawą stosunku służbowego.

Funkcjonariusze ABW oraz AW nie mogą m.in. podejmować określonej działalności (art. 79a ustawy o ABW oraz AW) ani zajęcia zarobkowego poza służbą bez zgody przełożonego (art. 80 ustawy o ABW oraz AW), są zobowiązani do składania oświadczeń majątkowych (art. 80a ustawy o ABW oraz AW), nie mogą być członkami partii politycznych ani uczestniczyć w działalności partii lub na jej rzecz, nie mogą się zrzeszać w związkach zawodowych, są obowiązani do poinformowania przełożonego o przynależności do stowarzyszeń krajowych, do uzyskania zezwolenia szefa właściwej Agencji lub upoważnionego przez niego przełożonego na przynależność do organizacji lub stowarzyszeń zagranicznych albo międzynarodowych (art. 81 ustawy o ABW oraz AW), a także do uzyskania zezwolenia szefa właściwej Agencji na wyjazd za granicę (art. 82 ustawy o ABW oraz AW). Te ograniczenia mają na celu zagwarantowanie ochrony dobra publicznego, a tym samym – przyznania mu prymatu przed partykularnym interesem samego funkcjonariusza[6].

Rezygnacja z poszczególnych wolności i praw musi być poprzedzona dobrowolną zgodą funkcjonariusza, który uprzednio dobrowolnie zgłosił gotowość pełnienia służby, a następnie przyjął akt mianowania inicjujący stosunek służbowy. Ustanowione zakazy wynikają z charakteru służby w formacjach, jakimi są ABW i AW. Funkcjonariusz może się nie podporządkować wymienionym ograniczeniom lub zakazom, ale takie działanie może skutkować jego odpowiedzialnością dyscyplinarną za naruszenie dyscypliny służbowej (art. 145 ust. 1 ustawy o ABW oraz AW)[7]. Może to również doprowadzić do rozwiązania z nim stosunku służbowego, szczególnie na podstawie art. 60 ust. 2 pkt 5 ustawy o ABW oraz AW[8]. Świadome i celowe naruszenie norm zawartych w przepisach powszechnie obowiązujących (zawartych w ustawie o ABW oraz AW) mogłoby świadczyć w sposób bezpośredni o braku zgody funkcjonariusza na poddanie się

---

[6] B. Opaliński, P. Szustakiewicz, *Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu*, w: *Stosunek służbowy w formacjach mundurowych*, W. Maciejko, P. Szustakiewicz (red.), Warszawa 2016, Legalis/el.

[7] Jak słusznie zauważa się w judykaturze, w ramach postępowania dyscyplinarnego rozstrzyga się o odpowiedzialności funkcjonariusza za czyny, które uchybiają godności lub regułom wykonywania zawodu. Nie muszą one jednak wyczerpywać jednocześnie znamion przestępstw lub wykroczeń (wyrok Naczelnego Sądu Administracyjnego, dalej: NSA, z 5 V 2011 r., I OSK 53/11, Legalis nr 352235).

[8] Nie można również wykluczyć, że naruszenie art. 81 ust. 1 ustawy o ABW oraz AW, będące podstawą do zainicjowania postępowania dyscyplinarnego, mogłoby skutkować wymierzeniem funkcjonariuszowi kary dyscyplinarnej wydalenia ze służby (art. 146 ust. 1 pkt 10 ustawy o ABW oraz AW). Wówczas jednak zmaterializowałaby się przesłanka do obligatoryjnego zwolnienia ze służby na podstawie art. 60 ust. 1 pkt 3 wymienionej ustawy).

szczególnemu rygorowi pełnienia służby i reżimowi panującemu w formacji zhierarchizowanej i zmilitaryzowanej. Takie zachowanie mogłoby, w ocenie jego przełożonego, być podstawą uznania, że została naruszona wartość prawnie chroniona, jaką jest „ważny interes służby". Pojęcie ważny interes służby stanowi klauzulę generalną[9], ale nie może budzić wątpliwości, że takie pojęcia, jak interes służby czy dobro służby są tożsame z pojęciem interes społeczny. Ustawodawca uzasadnił taką podstawę zwolnienia funkcjonariusza ze służby potrzebą ochrony interesu służby (interesu społecznego) jako interesu nadrzędnego w stosunku do partykularnego interesu jednostki[10]. Jak słusznie zauważa Naczelny Sąd Administracyjny w wyroku z 8 czerwca 2017 r., I OSK 656/16[11]:

> Ze służbą w Policji łączą się nie tylko liczne przywileje, ale także istotne obowiązki, a nawet pewne ograniczenia wolności osobistej. Każdy funkcjonariusz[,] decydując się na dobrowolne przystąpienie do takiej służby, musi mieć tego świadomość. Składa on rotę ślubowania i zobowiązuje się do respektowania reguł obowiązujących w macierzystej formacji, w tym do dbałości o honor, godność i dobre imię służby i do przestrzegania zasad etyki zawodowej. Osoba mianowana na stanowisko funkcjonariusza Policji w czasie wolnym od zajęć służbowych nie przestaje być policjantem. Zatem żaden funkcjonariusz Policji nie jest zwolniony z należytego zachowania się nawet w czasie wolnym od służby. Musi on zawsze postępować tak, by swą postawą umacniać autorytet i zaufanie Policji, a ponadto bezwzględnie unikać wszystkich takich sytuacji, które godziłyby w dobre imię macierzystej formacji. Powinien być on ponadto gotowym do niesienia pomocy innym osobom, które w różnych okolicznościach mogą potrzebować takiego wsparcia.

Chociaż przywołane orzeczenie dotyczy funkcjonariusza Policji, to nie ulega wątpliwości, że stanowisko w nim wyrażone można odnieść *per analogiam* do funkcjonariuszy ABW i AW. Służba w formacji zmilitaryzowanej i zhierarchizowanej obliguje bowiem do określonego sposobu postępowania, zachowania zgodnego z określonymi nakazami i zakazami, wynikającymi zarówno z przepisów prawa powszechnie obowiązującego, przepisów wewnętrznych, jak i rozkazów i poleceń przełożonych. W interesie służby (lub szerszej – w interesie społecznym) jest, aby funkcjonariusze podporządkowali się regułom panującym w organizacji mającej strukturę zhierarchizowaną.

---

[9] Nie jest to (czyli „ważny interes służby") pojęcie prawnie zdefiniowane. W orzecznictwie przyjmuje się jednak, że przy odczytywaniu treści wyrażenia „ważny interes służby" należy sięgnąć przede wszystkim do przepisów regulujących cele i zadania danej formacji (w tym przypadku orzeczenie dotyczyło funkcjonariusza Policji) oraz szczególnego statusu funkcjonariuszy w niej zatrudnionych (wyrok NSA z 4 VIII 2017 r., I OSK 1607/16, Legalis nr 1664019), podobnie w wyroku NSA z 29 I 2020 r., I OSK 3250/18, Legalis nr 2286751 oraz w wyroku NSA z 18 V 2018 r., I OSK 2439/16, Legalis nr 1837307.

[10] Wyrok NSA z 12 VII 2019 r., I OSK 710/17, Legalis nr 2194129; wyrok NSA z 23 III 2017 r., I OSK 436/16, Legalis nr 1632185.

[11] Legalis nr 1632706.

Przejawy braku zachowania dyscypliny służbowej nie tylko niekorzystnie wpływają na innych funkcjonariuszy, gdyż mogą prowadzić do rozluźnienia dyscypliny służbowej, lecz także istnieje zagrożenie, że mogą stworzyć negatywny obraz całej formacji w oczach opinii publicznej. Pragmatyka służbowa stawia funkcjonariuszom wyższe niż przeciętne wymagania w zakresie poszanowania przepisów prawa. Są oni zobowiązani nie tylko do spełniania wymogów określonych w art. 44 ustawy o ABW oraz AW[12], lecz także do postępowania zgodnie z rotą złożonego ślubowania[13]. Naruszenie obowiązków służbowych, jakim jest niestosowanie się do nakazów i zakazów wynikających z ustawy o ABW oraz AW, lub też inne zachowania niezgodne z prawem mogą być uznane za zachowania naruszające ważny interes służby, a tym samym mogą skutkować zwolnieniem funkcjonariusza ze służby.

Nie sposób jednak w ramach jednego opracowania odnieść się do wszystkich wyżej wymienionych obowiązków funkcjonariusza. Dlatego dalsze rozważania zostały skoncentrowane na jednym z nich, uregulowanym w art. 81 ust. 1 ustawy o ABW oraz AW. Zgodnie z tym artykułem funkcjonariusz ABW oraz AW nie może być członkiem partii politycznej ani uczestniczyć w działalności tej partii lub na jej rzecz[14]. *Prima facie* ten zakaz dotyczy wszelkiej aktywności funkcjonariusza, która mogłaby się wiązać z jego formalną przynależnością do partii politycznej, a także z aktywnością niemającą takiego charakteru, ale bezpośrednio wiążącą się z działalnością (funkcjonowaniem) tego typu partii. Ten problem wydaje się mieć istotne znaczenie, gdyż wytycza granicę dozwolonego zachowania funkcjonariusza. W interesie służby jest natomiast to, aby zakres jego dozwolonej aktywności był precyzyjnie wytyczony. Ważne jest więc wskazanie, jakiego działania funkcjonariusz nie może podejmować, aby nie narazić się na negatywne następstwa, które mogą być konsekwencją nieprzestrzegania zakazu ustanowionego w pragmatyce służbowej. Ten temat nie był dotychczas przedmiotem dogłębnej analizy w doktrynie i nie poświęcono mu szerszego opracowania.

Omawiana problematyka dotyczy samych funkcjonariuszy, ale przede wszystkim ich przełożonych, którzy są zobligowani zarówno do egzekwowania praw i obowiązków funkcjonariuszy wynikających ze stosunku służbowego, jak i do dbałości o utrzymanie dyscypliny służbowej przez swoich podwładnych, a tym samym – do zachowania i utrwalania modelu hierarchicznej struktury organizacyjnej formacji zmilitaryzowanej. Niniejszy artykuł stanowi próbę udzielenia odpowiedzi na pytanie dotyczące granic dozwolonego zachowania funkcjonariusza. W związku z tym konieczne jest wskazanie, jakie zachowanie (działanie lub w szerszym aspekcie – aktywność)

---

[12] Por. z wyrokiem NSA z 16 I 2020 r., I OSK 2748/18, Legalis nr 2287530, oraz z wyrokiem NSA z 16 I 2020 r., I OSK 2949/18, Legalis nr 2282018, w którym sąd wskazał, że pojęcie „ważny interes służby" należy wiązać z przymiotami stanowiącymi wymogi formalne niezbędne do pełnienia służby w Policji.

[13] Wyrok NSA z 18 V 2018 r., I OSK 2439/16…

[14] Pomimo wielu zmian w ustawie o ABW oraz AW treść art. 81 ust. 1 tej ustawy się nie zmieniła. Por. z art. 81 ust. 1 ustawy o ABW oraz AW w pierwotnym brzmieniu (DzU z 2002 r. nr 74 poz. 676, ze zm.).

funkcjonariuszy będzie naruszać dyspozycję normy prawnej zawartej w art. 81 ust. 1 ustawy o ABW oraz AW.

Nawiązanie stosunku służbowego, co już wyżej zaznaczono, immanentnie łączy się z koniecznością powstrzymania się przez funkcjonariusza przed określoną aktywnością związaną z działalnością partii politycznych, manifestowaniem poglądów politycznych, wspieraniem tych partii, działaniem na ich rzecz itp. Stąd też konieczne jest poprzedzenie rozważań stanowiących zasadniczą część tego opracowania omówieniem problematyki dotyczącej konstytucyjnie zagwarantowanej wolności zrzeszania się w partii politycznej. Funkcjonariusz, przyjmując akt mianowania inicjujący stosunek służbowy, zrzeka się części swoich praw i wolności, jakie ma ogół społeczeństwa. Musi zatem mieć świadomość, jaki zakres ma to zrzeczenie. Tylko w ten sposób podjęta przez niego decyzja może być uznana za w pełni świadomą, a tym samym może stanowić podstawę do stwierdzenia, że funkcjonariusz ma zdolność do poddania się szczególnemu reżimowi wynikającemu z charakteru służby w formacji, w której chce tę służbę pełnić.

Wolność zrzeszania się w partiach politycznych a możliwość ograniczenia tej wolności

Konstytucja Rzeczpospolitej Polskiej z 2 kwietnia 1997 r.[15] w art. 11 ust. 1 stanowi, że Rzeczpospolita Polska zapewnia wolność tworzenia i działania partii politycznych[16]. Partie zrzeszają obywateli polskich na zasadach dobrowolności i równości w celu wpływania metodami demokratycznymi na kształtowanie polityki państwa. Jak zaznacza doktryna, w zakresie przynależności do partii politycznych Konstytucja RP rozstrzyga trzy sprawy: przesądza, że członkiem partii może być tylko obywatel polski[17]; wymaga, aby członkostwo w partii było dobrowolne oraz aby było oparte na zasadach równości[18]. To oznacza, że obywatel polski nie może zostać wcielony do żadnej partii politycznej wbrew swojej wiedzy lub woli, ponieważ członkostwo w partii musi być oparte na dobrowolności i równości. Konstytucja RP bowiem zapewnia każdemu wolność zrzeszania się (art. 58 ust. 1 Konstytucji RP)[19]. Jak słusznie zaznacza się w doktrynie,

---

[15] DzU z 1997 r. nr 78 poz. 483, ze zm.

[16] Szerzej na temat pojęcia partia polityczna zob. M. Chmaj, M. Żmigrodzki, *Status prawny partii politycznych w Polsce*, Toruń 1995, s. 7 i nast.

[17] Przeciwnego zdania jest Marcin Dąbrowski, który twierdzi, że taki pogląd nie znajduje podstaw w treści przepisów ustawy zasadniczej, jest niewystarczająco uzasadniony i budzi wiele poważnych wątpliwości. Zob. tenże, *Konstytucyjny aspekt zrzeszania się cudzoziemców w partiach politycznych w Polsce*, „Przegląd Sejmowy" 2011, nr 2, s. 114.

[18] *Konstytucja RP. Tom I. Komentarz do art. 1–86*, M. Safjan, L. Bosek (red.), Warszawa 2016, (komentarz do art. 11 Konstytucji RP).

[19] Piotr Winczorek zalicza wolność zrzeszania się w partiach politycznych do wolności i praw politycznych. Odnoszą się one do udziału jednostki w życiu politycznym społeczeństwa, a tym samym

(…) *wolność zrzeszania się oznacza swobodę tworzenia przez obywateli różnego rodzaju organizacji, funkcjonujących dla realizacji wytyczonych przez nich celów*[20]. W Konstytucji RP określono jedynie ramy, w jakich ta wolność może być realizowana. Jedną z nich jest wolność zrzeszania się w partii politycznej[21].

Szczegółowe uregulowania dotyczące partii politycznych zostały zawarte w ustawie zwykłej, tj. *Ustawie z dnia 27 czerwca 1997 r. o partiach politycznych*[22] (dalej: ustawa o partiach politycznych). Przepis art. 1 ust. 1 tej ustawy definiuje partię polityczną jako dobrowolną organizację występującą pod określoną nazwą, stawiającą sobie za cel udział w życiu publicznym przez wywieranie metodami demokratycznymi wpływu na kształtowanie polityki państwa lub sprawowanie władzy publicznej[23]. Jest ona zatem formą zrzeszenia, za którego pośrednictwem społeczeństwo wyraża swoją wolę polityczną, a także - pośrednio - wpływa na kierunek i sposób sprawowania władzy publicznej[24]. Partia polityczna może korzystać z praw wynikających z ustaw dopiero po uzyskaniu wpisu do ewidencji partii politycznych (art. 1 ust. 2 ustawy o partiach politycznych). Ta regulacja wskazuje również, że członkami partii politycznej mogą być obywatele Rzeczpospolitej Polskiej, którzy ukończyli 18 lat (art. 2 ust. 1 ustawy o partiach politycznych).

Sprawy związane z członkostwem w partii politycznej zostały zastrzeżone jako materia statutowa każdej tego typu partii. Zgodnie z treścią art. 9 ust. 1 pkt 2 ustawy o partiach politycznych sposób nabywania i utraty członkostwa w partii politycznej określa statut tej partii[25]. Tym samym statut każdej partii politycznej może w sposób odmienny określać zasady, na jakich osoba może się ubiegać o bycie jej członkiem, a także sposoby pozbawienia tego prawa, tj. wykluczenia z grona osób będących członkami takiej partii. Statut partii nie może jednak naruszyć gwarancji wynikających z postanowień Konstytucji RP. Nie może więc ustanowić reguł, które nie respektowałyby zasady równości i dobrowolności w ubieganiu się o członkostwo w danej partii politycznej, a także możliwości wystąpienia z niej. Autonomia partii politycznej w zakresie określania celu, struktury, zasad działania, a zwłaszcza sposobu nabywania i utraty

---

do udziału w sprawowaniu władzy publicznej. Zob. tenże, *Prawo konstytucyjne Rzeczypospolitej Polskiej*, Warszawa 2003, s. 91; także: W. Skrzydło, *Polskie prawo konstytucyjne*, Lublin 1997, s. 188; *Prawo administracyjne*, J. Boć (red.), Wrocław 2001, s. 450.

[20] *Prawo konstytucyjne RP*, P. Sarnecki (red.), Warszawa 2011, s. 131.

[21] Szerzej na ten temat zob. J. Oniszczuk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w.*, Kraków 2004, s. 664 i nast.

[22] Tekst jednolity: DzU z 2018 r. poz. 580.

[23] Jest to podstawowy cel każdej partii politycznej (wyrok NSA z 18 XII 2014 r., I OSK 611/14, Legalis nr 1330014).

[24] *Prawo konstytucyjne RP*…, s. 132. W tym samym duchu wypowiada się Piotr Tuleja. Zob. *Prawo konstytucyjne*, P. Tuleja (red.) Warszawa 1995, s. 96.

[25] Statut partii politycznej jest uchwalany przez zgromadzenie ogólne członków partii lub zgromadzenie przedstawicieli członków partii wybranych w sposób demokratyczny (art. 9 ust. 2 ustawy o partiach politycznych).

członkostwa w niej, nie ma zatem charakteru bezwzględnego. Te granice wytycza zarówno Konstytucja RP, jak i ustawa o partiach politycznych.

Prawo do tworzenia partii politycznych i uczestnictwa w ich działalności przysługuje, co do zasady, każdemu obywatelowi RP na tych samych zasadach. Zakaz przynależności do partii politycznych musi wynikać z przepisu szczególnego o randze ustawy (art. 2 ust. 2 ustawy o partiach politycznych).

Takie ograniczenie zostało wprowadzone w art. 81 ust. 1 ustawy o ABW oraz AW. Identyczne rozwiązanie zostało przewidziane również w innych formacjach zmilitaryzowanych[26], o czym stanowią: art. 73 ust. 1 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[27], art. 40 ust. 1 *Ustawy z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego*[28], art. 139 ust. 1 *Ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa*[29] oraz art. 47 ust. 1 *Ustawy z dnia z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej*[30]. Należy również dodać, że taka sama treść jak w art. 81 ust. 1 ustawy o ABW oraz AW została zawarta także w art. 50 ust. 1 nieobowiązującej już *Ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa*[31]. Ta regulacja poprzedzała ustawę o ABW oraz AW[32].

Podobnie w art. 63 ust. 1 *Ustawy z dnia 6 kwietnia 1990 r. o Policji*[33] zawarto zapis, że policjant nie może być członkiem partii politycznej. Taka sama redakcja przepisu została zamieszczona w art. 163 *Ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej*[34], w art. 68 ust. 1 *Ustawy z dnia 12 października 1990 r. o Straży Granicznej*[35], w art. 202 ust. 1 pkt 1 *Ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej*[36] oraz w art. 57c ust. 1 *Ustawy z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej*[37]. Zgodnie z art. 106 ust. 1 pkt 1–3 *Ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych*[38] żołnierzowi zawodowemu w czasie pełnienia zawodowej służby wojskowej nie wolno: być członkiem partii politycznej, stowarzyszenia, organizacji

---

[26] Jak zaznacza M. Wieczorek, zakaz zrzeszania się w partiach politycznych jest zawarty we wszystkich pragmatykach służbowych (służb zmilitaryzowanych – przyp. aut.). Tenże, *Charakter prawny stosunków służbowych*…, s. 318.

[27] Tekst jednolity: DzU z 2019 r. poz. 1921, ze zm.

[28] Tekst jednolity: DzU z 2020 r. poz. 1221, ze zm.

[29] Tekst jednolity: DzU z 2020 r. poz. 384, ze zm.

[30] Tekst jednolity: DzU z 2019 r. poz. 1940, ze zm.

[31] Tekst jednolity: DzU z 1999 r. nr 51 poz. 526.

[32] Na podstawie art. 234 ustawy o ABW oraz AW; ustawa o Urzędzie Ochrony Państwa utraciła moc.

[33] Tekst jednolity: DzU z 2020 r. poz. 360, ze zm.

[34] Tekst jednolity: DzU z 2020 r. poz. 848, ze zm. Porównaj także z art. 64 ust. 1 nieobowiązującej *Ustawy z dnia 26 kwietnia 1996 r. o Służbie Więziennej* (t.j.: DzU z 2002 r. nr 207 poz. 1761, ze zm.).

[35] Tekst jednolity: DzU z 2020 r. poz. 305, ze zm.

[36] Tekst jednolity: DzU z 2021 r. poz. 422. Porównaj także z art. 125 pkt 1 nieobowiązującej *Ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej* (t.j.: DzU z 2016 r. poz. 1799, ze zm.).

[37] Tekst jednolity: DzU z 2020 r. poz. 1123, ze zm.

[38] Tekst jednolity: DzU z 2020 r. poz. 860, ze zm.

lub ruchu obywatelskiego stawiających sobie cele polityczne, brać udziału w zgromadzeniach o charakterze politycznym, a także prowadzić działalności politycznej[39].

Jednocześnie trzeba zaznaczyć, że ograniczenia w zakresie członkostwa funkcjonariuszy poszczególnych służb w partiach politycznych, wprowadzone w wyżej wymienionych aktach, nie naruszają istoty prawa określonego w ustawie zasadniczej i w ustawie o partiach politycznych. Jak bowiem zaznaczył Trybunał Konstytucyjny (dalej: TK) w wyroku z 10 kwietnia 2002 r. (sygn. akt K 26/00)[40], art. 2 ust. 2 ustawy o partiach politycznych oraz przepisy pozostałych pragmatyk służbowych wprowadzających zakaz członkostwa w partiach politycznych (w tym szczególnie żołnierzy zawodowych, policjantów, funkcjonariuszy Urzędu Ochrony Państwa, Straży Granicznej, Służby Więziennej, Służby Celnej) są zgodne m.in. z art. 11 ust. 1 Konstytucji RP.

Zdaniem Trybunału Konstytucyjnego:

> (…) zakaz członkostwa w partiach politycznych osób sprawujących określone funkcje w aparacie państwowym nie wynika z dążenia do ograniczenia praw obywatelskich tych kategorii osób, ale zapobiega konfliktom interesów i ról wynikających z wykonywania służby publicznej i prowadzenia działalności na rzecz określonej partii. Istotą członkostwa w partii politycznej wyraźnie formułowaną w statutach większości partii politycznych, jest obowiązek stosowania się do uchwał statutowych organów partyjnych i czynnego uczestnictwa w kształtowaniu i realizacji programu partii. Przyjęcie tego rodzaju zobowiązań nie jest obojętne z punktu widzenia obowiązków ciążących na funkcjonariuszach służb publicznych oraz pozostawaniu tych służb pod politycznym kierownictwem rządu tworzonego w oparciu o aktualną większość parlamentarną. Z punktu widzenia etyki funkcjonariusza służb publicznych niepożądana jest sytuacja, w której osoba korzystająca z prawa, przysługującego mu jako obywatelowi, narusza obowiązki wynikające z tytułu pełnienia służby publicznej. «Demokratyczne państwo prawne nie powinno być państwem partii. Przy wszystkich sprzężeniach między partiami a państwem potrzebny jest pewien dystans. Poddanie partii reżimowi prawa wywołuje ten skutek, że organy stosowania prawa, jak sądy, prokuratura czy policja, a w jakimś stopniu również i organy orzecznictwa administracyjnego, powinny być wolne od oddziaływania partii politycznych»[41].

W ocenie TK ustawodawca może ustanowić hierarchię określonych wartości i dać prymat jednym, tj. bezpieczeństwu państwowemu lub porządkowi publicznemu, przed innymi, szczególnie przed wartością, jaką jest wolność zrzeszania się, jeśli w określonych okolicznościach zachodzi kolizja pomiędzy tymi wartościami.

---

[39] Porównaj z art. 68 ust. 1 pkt 1–4 nieobowiązującej *Ustawy z dnia 30 czerwca 1970 r. o służbie wojskowej żołnierzy zawodowych* (t.j.: DzU z 1997 r. nr 10 poz. 55, ze zm.).

[40] Legalis nr 53826, OTK Seria A 2002, nr 2, poz. 18; także: DzU z 2002 nr 56 poz. 517.

[41] Przywołany w cytowanym orzeczeniu. Cyt. za: W. Sokolewicz, *Partie polityczne w polskim prawie konstytucyjnym: wczoraj, dziś, jutro*, „Studia Prawnicze" 1991, z. 4, bez paginacji.

W dalszych rozważaniach TK odniósł się *stricte* do zakazu ustanowionego dla funkcjonariuszy Policji. Wskazał, że:

> (…) zakaz członkostwa w partiach politycznych funkcjonariuszy Policji znajduje uzasadnienie zarówno w zadaniach tej służby i wynikających z nich uprawnień funkcjonariuszy, jak i z systemu organizacji Policji, opartego na zasadach dyscypliny i pełnej podległości podwładnych przełożonym. Działania w sferze zapewnienia bezpieczeństwa i porządku publicznego mogą być podejmowane i prowadzone z motywów politycznych i w szerokim zakresie wykorzystywane dla celów o takim charakterze. W ocenie TK, zwłaszcza tam, gdzie zakres powierzonych kompetencji jest na tyle szeroki, że wkracza w sferę praw i wolności innych osób, zrozumiałe jest wprowadzenie takich uregulowań, które tworzą bardziej rygorystyczne gwarancje bezstronności tych organów. Zgodnie z art. 1 ustawy o Policji (Dz.U. z 2002 r. Nr 7, poz. 58) do jej podstawowych zadań należy ochrona życia i zdrowia ludzi oraz mienia, ochrona bezpieczeństwa i porządku publicznego, wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców, kontrola przestrzegania przepisów porządkowych i administracyjnych związanych z działalnością publiczną. W granicach swych kompetencji Policja wykonuje czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe. Policja może, w zakresie koniecznym do wykonywania jej ustawowych zadań, korzystać z informacji o osobie, uzyskanych przez UOP i Straż Graniczną (art. 14 ustawy o Policji). Funkcjonariusze Policji dysponują szeregiem uprawnień, łącznie ze stosowaniem środków przymusu bezpośredniego (art. 15 i art. 16 ustawy o Policji), które w sposób bardzo istotny wkraczają w sferę praw i wolności jednostki. W związku z tym uzasadnione jest istnienie ograniczeń praw funkcjonariuszy, gwarantujących ich neutralność polityczną[42].

Jednocześnie TK zaznaczył, że zaprezentowane stanowisko należy odnieść również do funkcjonariuszy innych służb (formacji zmilitaryzowanych), które pełnią funkcje i wykonują zadania o charakterze zbliżonym do funkcji i zadań Policji. Mają one bowiem – w szerszym lub węższym zakresie – uprawnienia do stosowania instrumentów, które wkraczają bezpośrednio w sferę podstawowych praw i wolności obywatelskich, w tym do stosowania środków przymusu bezpośredniego. Zatem argumentacja odnosząca się wprost do zakazu członkostwa funkcjonariuszy Policji w partiach

[42] Por. także: „Biorąc pod uwagę art. 10, 11 oraz 14 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r., Nr 61, poz. 284) Trybunał stwierdza, że państwo może uznać za konieczne konstytucyjne zagwarantowanie politycznej neutralności sił policyjnych i wprowadzenie regulacji dotyczących ograniczeń w zakresie stowarzyszeń w dziedzinie polityki wobec funkcjonariuszy Policji. Funkcjonariusze są bowiem uprawnieni do stosowania przymusu przy regulowaniu zachowania obywateli, w niektórych krajach są uzbrojeni, a siły policyjne pozostają na służbie państwa. Społeczeństwo może więc oczekiwać, iż w swoich relacjach z Policją będzie miało do czynienia z neutralnymi politycznie funkcjonariuszami" (wyrok Europejskiego Trybunału Praw Człowieka z 20 V 1999 r., sygn. 25390/94, Legalis nr 102542).

politycznych musi być odniesiona *per analogiam* do funkcjonariuszy służb zobowiązanych do wykonywania zadań podobnych do zadań Policji i dysponujących podobnymi uprawnieniami oraz mających strukturę hierarchiczną opartą na podległości służbowej w stosunkach pomiędzy przełożonym a podwładnym i szczególnej dyscyplinie.

Stanowisko zaprezentowane przez TK pozostaje aktualne również w odniesieniu do zakazu wprowadzonego w ustawie o ABW oraz AW. Nie może budzić wątpliwości to, że szczególny charakter służby publicznej pełnionej przez funkcjonariuszy ABW i AW, zwłaszcza w świetle zadań przewidzianych dla tych formacji (wymienionych w art. 5 i art. 6 ustawy o ABW oraz AW), wymaga zagwarantowania ich politycznej neutralności. Ten zakaz ma służyć wyeliminowaniu lub znacznemu ograniczeniu jakichkolwiek wątpliwości, że działania podejmowane przez funkcjonariuszy, a tym samym przez samą formację[43], zwłaszcza w stosunku do obywateli, są inspirowane motywami lub pobudkami o charakterze politycznym[44]. Wymienione formacje, jak już wspomniano, mają bowiem szerokie uprawnienia do ingerencji w sferę praw i wolności ludzi. Społeczeństwo musi więc mieć przekonanie, że zadania realizowane przez ABW lub AW służą wypełnieniu misji tych organizacji. Tym samym wymienione formacje muszą się cieszyć pełnym zaufaniem społecznym. Ma to szczególne znaczenie w kontekście jawności ich działań. Ludzie nie mają (i w bardzo wielu przypadkach nie będą mieli) wiedzy o zakresie i celu poszczególnych zadań realizowanych przez te formacje. Muszą wobec tego mieć przekonanie, że determinantą do ich podjęcia jest wyłącznie zamiar wykonania przez ABW lub AW zadań określonych w ustawie kompetencyjnej oraz że te zadania nie są uzasadnione polityczną wolą konkretnej grupy reprezentującej określony pogląd polityczny lub wolą partii politycznej.I mimo że nie wynika to wprost ze stanowiska TK, gdyż oceniał on zgodność

---

[43] Jak słusznie zaznacza TK (wyrok TK z 15 IX 1999 r., K 11/99, OTK 1999 r., nr 6, poz. 116, Legalis nr 45366): „(…) pojęcie funkcjonariusza pozostaje zawsze w nierozerwalnym związku z instytucją, bądź strukturą[,] w ramach której i na rzecz której funkcjonariusz działa. Z jednostki organizacyjnej czy też organu, z którym jest związany, funkcjonariusz czerpie upoważnienie i umocowanie do podejmowanych przez siebie działań. Można w związku z tym mówić o swoistej identyfikacji tychże działań z celami organizacji[,] na rzecz której działa. Poszczególne działania funkcjonariusza pozostające w związku z wykonywaną przez niego funkcją wywierają skutki dla jednostki organizacyjnej[,] z którą jest związany. Działalność samej jednostki organizacyjnej jest w praktyce uzewnętrzniana przez jej organy i funkcjonariuszy. Funkcjonariusz zatem zapewnia organizacji (organowi) możliwość działania poprzez realizację właściwych dla niej zadań merytorycznych. Status funkcjonariusza jest ściśle związany z realizowaniem merytorycznych zadań jednostki organizacyjnej (organu), a przez to podstawowych ich celów".

[44] M. Wieczorek, *Charakter prawny stosunków służbowych*…, s. 31; także: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Straży Granicznej. Komentarz*, Warszawa 2019, Legalis (komentarz do art. 68 ustawy o Straży Granicznej). Analogiczne uzasadnienie prezentuje Adam Zdunek w odniesieniu do funkcjonariuszy Krajowej Administracji Skarbowej. Twierdzi on, że „(…) te zakazy uzasadnione są specyfiką pełnienia służby w Służbie Celno-Skarbowej i koniecznością zagwarantowania niezależności funkcjonariusza". Zob. *Ustawa o Krajowej Administracji Skarbowej. Komentarz*, L. Bielecki, A. Gorgol (red.), Warszawa 2018, Legalis (komentarz do art. 202 ustawy o Krajowej Administracji Skarbowej); także: „Regulacja ta ma na celu zapewnienie gwarancji bezstronnego wykonywania przez policjantów powierzonych im zadań służbowych". Zob. Ł. Czebotar i in., *Ustawa o Policji. Komentarz*, Warszawa 2015, s. 482.

przepisów pragmatyk służbowych dotyczących zakazu przynależności funkcjonariuszy służb zmilitaryzowanych (zwłaszcza funkcjonariuszy Policji) do partii politycznych z Konstytucją RP, to niewątpliwie z treści cytowanych fragmentów orzeczenia można wywieść uzasadnienie wprowadzenia tego rodzaju ograniczeń w stosunku do funkcjonariuszy publicznych. Funkcjonariusze publiczni bowiem mają przede wszystkim realizować zadania wyznaczone formacji, w której pełnią służbę. Informacja o formalnej lub nieformalnej przynależności funkcjonariusza danej służby do określonej partii politycznej może wpływać na zdolność do realizacji przez niego zadań, a tym samym – na efektywność realizacji zadań służby. Ograniczenia wprowadzone dla funkcjonariuszy są zatem, jak słusznie zaznacza TK, gwarancją neutralności politycznej i bezstronności tych organów.

Istota zakazu wynikającego z art. 81 ust. 1 ustawy o ABW oraz AW

Jak już wcześniej wspomniano, z treści art. 81 ust. 1 ustawy o ABW oraz AW wynika, że funkcjonariusz ABW lub AW nie może być członkiem partii politycznej ani uczestniczyć w działalności tej partii lub na jej rzecz. To oznacza, że tym przepisem ustanowiono dwa odrębne zakazy. Pierwszy z nich to zakaz członkostwa w partii politycznej[45]. Odnosi się on do partii politycznych legalnie działających w polskim porządku prawnym. Nie można bowiem odnieść go do nieformalnych organizacji, które nie spełniają kryteriów wskazanych przez przepisy ustawy o partiach politycznych[46], a także do organizacji, których działalność jest zakazana przez przepisy prawa. Zakaz ten należy *stricte* odnieść do partii politycznej spełniającej kryteria, o których mowa w art. 1 ust. 1 ustawy o partiach politycznych. Przy założeniu, że ustawodawca jest racjonalny, jeśli posłużyłby się pojęciem partia polityczna w innym znaczeniu niż w ustawie o partiach politycznych, wskazałby to *expressis verbis* w konkretnym przepisie pragmatyki służbowej. Skoro nie zawarł takiego zastrzeżenia, to konieczne jest ustalenie zakresu znaczeniowego tego pojęcia na podstawie aktu prawnego, który taką definicję zawiera, tj. ustawy o partiach politycznych. Przeciwne stanowisko prowadziłoby do wniosku, że system prawa nie jest spójny.

Należy podkreślić, że zakaz członkostwa w partii politycznej ma charakter bezwzględny[47]. Tym samym od chwili zainicjowania z osobą fizyczną stosunku służbowego

---

[45] Jest to formalny zakaz bycia członkiem partii politycznej. Zob. B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*… (komentarz do art. 81 ustawy o ABW oraz AW).

[46] Nie musi to jednak być partia wpisana do ewidencji partii politycznych, wpis powoduje bowiem, że nabywa ona osobowość prawną i może korzystać z praw wynikających z ustaw. Brak wpisu nie pozbawia jej przymiotu partii politycznej. Jest nią już na etapie jej tworzenia, jeśli spełnia kryteria wskazane w ustawie o partiach politycznych. Por. *Prawo administracyjne*, E. Ura (red.), Rzeszów 1997, s. 554.

[47] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*… (komentarz do art. 81 ustawy o ABW oraz AW); zob. także: B. Opaliński, P. Szustakiewicz, *Agencja Bezpieczeństwa Wewnętrznego*…

w ABW albo w AW aż do jego zakończenia, tj. do jego rozwiązania, funkcjonariusz nie może być członkiem takiej partii. Sprawy związane z członkostwem zostały zastrzeżone dla statutów poszczególnych partii politycznych. W tych aktach wskazuje się zarówno warunki, na jakich osoba dobrowolnie składająca oświadczenie woli o wstąpieniu do partii politycznej może się stać jej członkiem, jak i wyznacza moment, kiedy dana osoba staje się członkiem tej partii, a także, kiedy przestaje nim być – po złożeniu oświadczenia o wystąpieniu z partii. Istotne z punktu widzenia omawianej problematyki jest zatem to, że w momencie nawiązania przez osobę fizyczną stosunku służbowego nie może ona już być członkiem żadnej partii politycznej. Jeśli wystąpienie z danej partii politycznej wymaga przeprowadzenia (zwłaszcza przez organy statutowe tej partii) określonej sekwencji czynności, których wykonanie skutkuje utratą tego członkostwa, to zasadne wydaje się, że złożenie wyłącznie samego oświadczenia woli o wystąpieniu członka z tej partii (np. wniosku o wykreślenie go z listy członków) nie spełniałoby warunku, o którym mowa w art. 81 ust. 1 ustawy o ABW oraz AW. W chwili zainicjowania stosunku służbowego osoba fizyczna musi zostać definitywnie pozbawiona statusu członka partii politycznej. Zatem, jeśli statut partii politycznej przewiduje określoną procedurę z tym związaną, to musi ona zostać dopełniona. Przepis art. 81 ust. 1 ustawy o ABW oraz AW odnosi się bowiem do formalnego węzła, jaki spaja organizację (partię polityczną) z osobą fizyczną (jej członkiem). Nie obejmuje on psychicznego nastawienia danej osoby co do tego, czy ona chce czy nie chce być członkiem określonej partii politycznej. Nie ma również znaczenia, jakie czynności czy działania podejmowała osoba fizyczna lub też jaką aktywnością się wykazała w celu pozbawienia siebie statusu członka partii politycznej. Istotne jest wyłącznie to, czy w okresie trwania stosunku służbowego (od chwili jego zainicjowania do momentu jego utraty) osoba fizyczna (funkcjonariusz) formalnie ma status członka partii politycznej. Odmienna interpretacja nie wytrzymuje krytyki, gdyż osoba fizyczna, składając oświadczenie o wystąpieniu z partii politycznej (zwłaszcza jeśli takie oświadczenie złożyłaby za pośrednictwem poczty lub innego środka komunikacji na odległość), nie byłaby zobowiązana do zweryfikowania, czy rzeczywiście to oświadczenie dotarło do adresata, tj. partii politycznej, a jeśli dotarło, to czy wywołało skutek w postaci pozbawienia jej członkostwa w tej partii. Mogłoby to powodować, że taka osoba nie utraciłaby tego statusu w okresie trwania stosunku służbowego. Należy podkreślić, że ten obowiązek dotyczy wyłącznie formalnego węzła łączącego partię polityczną z jej członkiem. Pozbawienie członkostwa musi polegać na definitywnym zerwaniu tej więzi. Nie może zatem nim być ani zawieszenie członkostwa, ani zawieszenie wykonywania praw członkowskich w partii politycznej.

Z treści art. 63 ust. 2 ustawy o Policji wynika, że z chwilą przyjęcia policjanta do służby ustaje jego dotychczasowe członkostwo w partii politycznej[48]. Ustawa o ABW

[48] Tak samo w: art. 139 ust. 2 ustawy o Służbie Ochrony Państwa, art. 163 ust. 2 ustawy o Służbie Więziennej, art. 68 ust. 2 ustawy o Straży Granicznej, art. 57c ust. 2 ustawy o Państwowej Straży Pożarnej, art. 106 ust. 3 ustawy o służbie wojskowej żołnierzy zawodowych, a także w art. 50 ust. 2 nieobowiązującej ustawy o Urzędzie Ochrony Państwa.

oraz AW nie zawiera podobnie brzmiącego przepisu. Jeśli kandydat przed przyjęciem go do służby w ABW albo AW był członkiem partii politycznej, to musi z własnej inicjatywy podjąć aktywność zmierzającą do definitywnego pozbawienia go tego statusu. Samo nawiązanie stosunku służbowego nie powoduje bowiem *ipso iure* takiego skutku.

Pragmatyka służbowa, chociaż posługuje się pojęciem członkostwo, to nie wyjaśnia, czym ono w istocie jest. Również w ustawie o partiach politycznych nie zawarto definicji legalnej tego pojęcia. Ze względu na jej brak należałoby się odnieść do znaczenia, jakie ono ma w języku potocznym. „Członkostwo" to przynależność do jakiejś organizacji[49]. Z kolei „członek" to osoba lub jednostka prawna należące do jakiejś grupy, organizacji[50]. W uzupełnieniu wypada jedynie wskazać, że przez „przynależność" należałoby rozumieć sformalizowaną więź prawną skutkującą tym, że osoba fizyczna staje się elementem składowym danej organizacji – tworzy jej szeregi. Trzeba również zaznaczyć, że członkostwo w partii politycznej, w kontekście dobrowolnej przynależności do tego rodzaju organizacji, jest – co do zasady – immanentnie związane z psychicznym nastawieniem obywatela RP, który utożsamiając się z określonymi ideami, poglądami, programem politycznym, chce współuczestniczyć w realizacji celu danej partii. Niemniej, jak zostało to już wcześniej zaznaczone w odniesieniu do tematu poruszanego w artykule, członkostwo w partii politycznej należy utożsamiać wyłącznie z wyżej wymienionym formalnym węzłem prawnym. Tym samym ustalenie rzeczywistego członkostwa funkcjonariusza w partii politycznej jest wystarczające do stwierdzenia, że został naruszony zakaz wynikający z pragmatyki służbowej. Nieistotne są natomiast przyczyny takiego stanu rzeczy, a zwłaszcza brak psychicznej łączności pomiędzy osobą fizyczną a organizacją.

Drugim zakazem wynikającym z art. 81 ust. 1 ustawy o ABW oraz AW jest zakaz uczestniczenia przez funkcjonariusza w działalności partii politycznej lub na jej rzecz[51]. Ten zakaz również ma charakter bezwzględny[52]. W tym przypadku chodzi o takie uczestnictwo w działalności partii politycznej lub na jej rzecz, które nie jest (nie musi być) połączone z członkostwem w tej partii. Samo członkostwo jest już objęte odrębnym

---

[49] https://sjp.pwn.pl/slowniki/cz%C5%82onkostwo.html [dostęp: 8 VII 2020].

[50] https://sjp.pwn.pl/szukaj/cz%C5%82onek.html [dostęp: 8 VII 2020].

[51] Jest to zakaz materialny prowadzenia działalności politycznej. Zob. B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*… (komentarz do art. 81 ustawy o ABW oraz AW) oraz B. Opaliński, P. Szustakiewicz, *Agencja Bezpieczeństwa Wewnętrznego*... Ten zakaz obejmuje każdą działalność na rzecz partii politycznej, np. przez uczestnictwo w jej manifestacjach lub pracy jej młodzieżówki. Zob. M. Rogalski, P. Szustakiewicz, P. Złamańczuk, *Ustawa o Służbie Ochrony Państwa. Komentarz*, Warszawa 2019, Legalis (komentarz do art. 139 ustawy o Służbie Ochrony Państwa). W. Kotowski wskazuje ponadto (w odniesieniu do policjantów), że ten zakaz obejmuje: uczestnictwo w redagowaniu pisma o charakterze politycznym, autorstwo tekstów do takich czasopism oraz członkostwo w kolegium redakcyjnym takich czasopism. Zob. W. Kotowski, *Ustawa o Policji. Komentarz*, Warszawa 2008, s. 468.

[52] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*… (komentarz do art. 81 ustawy o ABW oraz AW); także: B. Opaliński, P. Szustakiewicz, *Agencja Bezpieczeństwa Wewnętrznego*…

zakazem i nie musi być połączone z żadną działalnością funkcjonariusza na rzecz tej partii lub uczestnictwem w jej funkcjonowaniu. Naruszenie pierwszego zakazu następuje w momencie, gdy pomiędzy czynnym funkcjonariuszem a partią polityczną istnieje więź prawna, z której wynika, że przynależy on do tej organizacji jako jej członek. Nie musi przy tym wykazywać się żadną aktywnością ani w funkcjonowaniu tej partii, ani też nie musi działać na jej rzecz. Wystarczające jest ustalenie, że będąc funkcjonariuszem, jest również jej członkiem.

Uczestnictwo w działalności partii politycznej lub działanie na jej rzecz może natomiast nie być połączone z formalnym członkostwem w tej partii. Może polegać na pełnieniu jakiejś funkcji w określonych władzach lub ciałach statutowych tej partii, zajmowaniu w niej określonego stanowiska, ale również na nieformalnej przynależności do niej lub odgrywaniu określonej roli w jej strukturach. Nie ma również znaczenia, czy takie uczestnictwo ma charakter odpłatny. Chodzi zatem o każdego rodzaju aktywność związaną z działalnością partii politycznej, w tym szczególnie z uczestniczeniem w procesie jej tworzenia, w jej funkcjonowaniu, zmianach lub likwidacji, czyli o ustalenie, że działania podejmowane przez funkcjonariusza są nakierowane na to, aby brać udział w działalności danej partii.

Nie oznacza to jednak, że zakaz, o którym mowa, głęboko ingeruje w sferę prywatną osoby fizycznej, a tym samym, że zobowiązuje ją do wyzbycia się poglądów politycznych z chwilą nawiązania stosunku służbowego. Zarówno ABW i AW, jak i inne formacje zmilitaryzowane nie są bowiem organizacjami totalitarnymi. Chodzi natomiast o stworzenie pewnych granic, które uniemożliwią identyfikowanie poszczególnych funkcjonariuszy tych służb z określoną opcją polityczną. Istotą jest intensywność wyrażania przez funkcjonariuszy własnych opinii czy manifestowania swoich poglądów politycznych. Funkcjonariusz nie może przekroczyć pewnego poziomu w manifestowaniu swoich poglądów politycznych, który umożliwiłby łączenie go z konkretną partią polityczną, a w szerszym aspekcie – całej formacji z taką partią. Stąd też istnieje konieczność rezygnacji przez funkcjonariusza z określonych praw i wolności, jakie ma reszta społeczeństwa, bądź ograniczenia możliwości ich realizacji. Funkcjonariusz może mieć własne przekonania i poglądy o charakterze politycznym, może również korzystać z czynnego prawa wyborczego i głosować w wyborach na kandydata dowolnej partii politycznej, wyrażać zdanie w sprawach politycznych bądź wymieniać poglądy w tym zakresie, z tym jednak zastrzeżeniem, że nie może tego manifestować publicznie. Może również badać naukowo tę sferę i publikować wyniki przeprowadzonych badań w periodykach o charakterze naukowym, oczywiście z zachowaniem innych wymogów określonych w pragmatyce służbowej (art. 80 ustawy o ABW oraz AW). Zakaz ustanowiony w art. 81 ust. 1 ustawy ma bowiem swoje granice. Funkcjonariusz nie może być ani członkiem partii politycznej, ani uczestniczyć w działalności tej partii lub na jej rzecz. Wobec tego nie może podejmować żadnej aktywności, która skutkowałaby tym, że w społeczeństwie jako funkcjonariusz byłby identyfikowany z określoną partią lub opcją polityczną. Byłoby to, jak zaznacza Mariusz Wieczorek, niezgodne z rotą złożonego ślubowania. Funkcjonariusz, pełniąc służbę, nie

może kierować się swoimi przekonaniami czy sympatiami politycznymi, ale dobrem wspólnym[53]. Niedopuszczalne wobec tego by było, aby manifestował swoją sympatię dla określonej partii lub opcji politycznej lub też w jakikolwiek sposób agitował na jej rzecz[54]. Nic natomiast nie stoi na przeszkodzie w prowadzeniu przez funkcjonariusza dyskusji na tematy polityczne w gronie rodzinnym. Bezwzględnie niedopuszczalna byłaby tego rodzaju aktywność funkcjonariusza podejmowana przez niego podczas wykonywania czynności służbowych lub w związku z ich wykonywaniem. Mogłoby to świadczyć przede wszystkim o chęci przysporzenia zwolenników danej partii politycznej. To z kolei uzasadniałoby twierdzenie o wykonywaniu przez niego działań na rzecz określonej partii.

Należy również dodać, że zakaz uczestniczenia funkcjonariusza ABW albo AW w działalności partii politycznej lub na jej rzecz nie ma tak wyraźnie zarysowanych granic, jak w przypadku zakazu członkostwa w tego typu partii. Zakaz członkostwa wymaga bowiem wyłącznie ustalenia istnienia relacji mającej charakter sformalizowany, tj. węzła prawnego, który uprawnia do stwierdzenia, że dana osoba jest członkiem określonej partii politycznej. Nie oznacza to jednak, że zakaz uczestnictwa funkcjonariusza ABW albo AW w działalności partii politycznej lub na jej rzecz w ogóle nie ma takich granic, ale w przeciwieństwie do granic zakazu odnoszącego się do członkostwa w partii politycznej zakaz uczestnictwa ma charakter ocenny. Właściwa kwalifikacja jako naruszająca obowiązek powstrzymania się przez funkcjonariusza od uczestnictwa w działalności partii politycznej lub działania na jej rzecz jest wobec tego zależna od studium konkretnego przypadku. Trudno by było stworzyć wyczerpujący katalog sytuacji, które mieściłyby się w granicach tego zakazu. W praktyce byłoby to znacznie utrudnione lub wręcz niemożliwe. Nie może jednak budzić wątpliwości to, że taka ocena nie może mieć charakteru nieograniczonego – arbitralnego. Musi ona wskazywać na to, że określona, świadoma aktywność funkcjonariusza może być obiektywnie łączona z funkcjonowaniem partii politycznej lub jej działalnością.

Podsumowanie

Trudno się odnieść do wszystkich aspektów omawianego zagadnienia w ramach jednego opracowania. Liczba stanów faktycznych, jakie można by było wyodrębnić, jest bowiem niezliczona. W artykule skoncentrowano się wyłącznie na wskazaniu określonych obszarów tej tematyki, które pozwolą ją przybliżyć.

Jak wykazano, zakaz ustanowiony w art. 81 ust. 1 ustawy o ABW oraz AW, podobnie jak zakazy zawarte w innych pragmatykach służbowych funkcjonariuszy służb

---

[53] M. Wieczorek, *Charakter prawny stosunków służbowych*…, s. 319.

[54] Wyrok Wojewódzkiego Sądu Administracyjnego w Lublinie z 11 II 2016 r., III SA/Lu 1108/15, Legalis nr 1434512 (dotyczy policjanta); B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*… (komentarz do art. 81 ustawy o ABW oraz AW).

zmilitaryzowanych, ma swoje uzasadnienie w celach i zadaniach tych formacji. Tylko polityczna neutralność[55] członków formacji, o których mowa, pozwala na zagwarantowanie właściwej realizacji tych zadań i osiągnięcie celów. Instrumenty prawne, w jakie funkcjonariusze tych służb zostali wyposażeni, umożliwiają głęboką ingerencję w sferę praw i wolności innych osób. Muszą one zatem mieć przekonanie, że te instrumenty nie są i nie będą wykorzystywane w celach politycznych, a formacje są wolne od nacisków zewnętrznych.

Z treści art. 81 ust. 1 ustawy o ABW oraz AW wynikają dwa odrębne obowiązki (zakazy) ustanowione dla czynnego funkcjonariusza. Naruszenie pierwszego z nich następuje już w momencie ustalenia istnienia formalnego węzła, jakim jest członkostwo funkcjonariusza w partii politycznej, chociażby nie było ono połączone z żadną aktywnością z jego strony. Drugi zakaz natomiast jest związany z obowiązkiem powstrzymania się przez funkcjonariusza od podejmowania jakiejkolwiek aktywności, która wskazywałaby na istnienie jakichkolwiek relacji między tą aktywnością a funkcjonowaniem partii politycznej. Uczestnictwo w działalności partii politycznej lub na jej rzecz może objawiać się w różny sposób. Trudno więc przewidzieć wszystkie możliwe warianty, jakie mogą zaistnieć. Ocena w tym zakresie nie może jednak mieć charakteru dowolnego. Konieczne jest wykazanie w sposób obiektywny związku między aktywnością funkcjonariusza (tj. jego uczestnictwem) a działalnością partii

[55] *Ustawa o Policji. Komentarz*, K. Chałubińska-Jentkiewicz, J. Kurek (red.), Warszawa 2020, Legalis (komentarz do art. 63 ustawy o Policji) – dokonano tu rozróżnienia pojęć: neutralność polityczna i apolityczność. Przemysław Szustakiewicz wskazuje natomiast, że zakazy ustanowione w pragmatykach służbowych funkcjonariuszy służb mundurowych i żołnierzy zawodowych mają służyć zapewnieniu apolityczności formacji zmilitaryzowanej. Apolityczność rozumie on jako zakaz publicznego manifestowania poglądów politycznych i zakaz kierowania się przy wykonywaniu obowiązków służbowych własnymi przekonaniami politycznymi. Jego zdaniem „apolityczność" jest pojęciem szerszym od zakazu przynależności do partii politycznych i oznacza, że osoba pełniąca służbę w formacji zmilitaryzowanej nie wyraża ani nie realizuje w toku służby wyznawanych poglądów politycznych. Ponadto zestawia pojęcie „apolityczność" z pojęciem apartyjność, które utożsamia z zakazem przynależności do stronnictwa politycznego. Zob. P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych…*, s. 175 i nast. Wojciech Kotowski również stoi na stanowisku, że art. 63 ustawy o Policji odnosi się do apolityczności policjanta. Zob. tenże, *Ustawa o Policji…*, s. 468. W tym samym duchu wypowiada się Łukasz Czebotar. Zob. tenże i in., *Ustawa o Policji…*, s. 482. Porównaj także z *Leksykonem policyjnym*, w którym apolityczność w ujęciu formalnym sprowadzono do zakazu członkostwa funkcjonariusza (policjanta) w partii politycznej, w celu zapewnienia rzetelnego i bezstronnego wykonywania przez niego obowiązków służbowych. Zob. *Leksykon policyjny*, W. Pływaczewski, G. Kędzierska (red.), Szczytno 2001, s. 23. W tym znaczeniu pojęcie „apolityczność" jest tożsame z pojęciem „neutralność polityczna". Z kolei w *Słowniku wiedzy o Policji* wymóg apolityczności policjantów interpretuje się rozszerzająco i obejmuje się nim nie tylko zakaz członkostwa w partii politycznej, lecz także obowiązek poinformowania przełożonego o przynależności do stowarzyszeń krajowych działających poza służbą, a także wymóg zezwolenia przez Komendanta Głównego Policji lub upoważnionego przez niego przełożonego na przynależność do organizacji lub stowarzyszeń zagranicznych albo międzynarodowych. Zob. *Słownik wiedzy o Policji*, P. Bogdalski, M. Świderski, K.A. Wojtaszczyk (red.), Warszawa 2015, s. 35.

politycznej lub ustalenie, że taka aktywność (określone działanie) była nakierowana na partię polityczną.

Znajomość granic zakazów wytyczonych przez art. 81 ust. 1 ustawy o ABW oraz AW ma istotne znaczenie dla funkcjonariusza, zakreśla mu bowiem sferę dopuszczalnej aktywności. Pozwala tym samym zarówno na zminimalizowanie prawdopodobieństwa pociągnięcia go do odpowiedzialności dyscyplinarnej, a co za tym idzie – możliwości wymierzenia mu kary dyscyplinarnej, jak i ustalenia przesłanki upoważniającej do rozwiązania z nim stosunku służbowego.

De lege ferenda zasadne wydaje się uzupełnienie regulacji zawartej w ustawie o ABW oraz AW o normę prawną, która skutkowałaby pozbawieniem czynnego funkcjonariusza członkostwa w partii politycznej z mocy samego prawa w momencie zawiązania się stosunku służbowego. Pozwoliłoby to na wykluczenie przypadków naruszenia art. 81 ust. 1 ustawy o ABW oraz AW wynikających z zaniedbania samego funkcjonariusza, który mógł w przeszłości, nawet przez krótki czas, brać czynny udział w działalności określonej partii politycznej, a następnie zaniechał takiej współpracy. W takim przypadku funkcjonariusz może obecnie nie mieć pełnej świadomości, czy formalnie jest członkiem tej partii, gdyż np. zaprzestała ona swojej działalności, ale nie została zlikwidowana, nie została wpisana do właściwej ewidencji bądź niemożliwe jest dotarcie do dokumentacji tej partii lub osób ją tworzących.

Bibliografia

Chmaj M., Żmigrodzki M., *Status prawny partii politycznych w Polsce*, Toruń 1995, Wydawnictwo Adam Marszałek.

Czebotar Ł. i in., *Ustawa o Policji. Komentarz*, Warszawa 2015, Wolters Kluwer.

Dąbrowski M., *Konstytucyjny aspekt zrzeszania się cudzoziemców w partiach politycznych w Polsce*, „Przegląd Sejmowy" 2011, nr 2, s. 107–124.

Gacek P., *Nawiązanie stosunku służbowego z funkcjonariuszem Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Charakter prawny mianowania – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 98–119.

Gacek P., *Wymogi formalne niezbędne do pełnienia służby w Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 56–86.

Konstytucja RP. Tom I. Komentarz do art. 1–86, M. Safjan, L. Bosek (red.), Warszawa 2016, C.H. Beck.

Kotowski W., *Ustawa o Policji. Komentarz*, Warszawa 2008, Wolters Kluwer.

Kuczyński T., Mazurczak-Jasińska E., Stelina J., *Stosunek służbowy*, w: *System prawa administracyjnego*, t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2011, C.H. Beck.

Leksykon policyjny, W. Pływaczewski, G. Kędzierska (red.), Szczytno 2001, WSPol.

Oniszczuk J., *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w.*, Kraków 2004, Wolters Kluwer.

Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis.

Opaliński B., Szustakiewicz P., *Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu*, w: *Stosunek służbowy w formacjach mundurowych*, W. Maciejko, P. Szustakiewicz (red.), Warszawa 2016, Legalis/el.

Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Straży Granicznej. Komentarz*, Warszawa 2019, Legalis.

Prawo administracyjne, J. Boć (red.), wyd. 7, Wrocław 2001, Kolonia Limited.

Prawo administracyjne, E. Ura (red.), Rzeszów 1997, [bw].

Prawo konstytucyjne, P. Tuleja (red.), Warszawa 1995, C.H. Beck.

Prawo konstytucyjne RP, P. Sarnecki (red.), Warszawa 2011, C.H. Beck.

Rogalski M., Szustakiewicz P., Złamańczuk P., *Ustawa o Służbie Ochrony Państwa. Komentarz*, Warszawa 2019, C.H. Beck.

Skrzydło W., *Polskie prawo konstytucyjne*, Lublin 1997, Morpol.

Słownik wiedzy o Policji, P. Bogdalski, M. Świderski, K.A. Wojtaszczyk (red.), Warszawa 2015, Aspra.

Sokolewicz W., *Partie polityczne w polskim prawie konstytucyjnym: wczoraj, dziś, jutro*, „Studia Prawnicze" 1991, z. 4, INP PAN, bez paginacji.

Szustakiewicz P., *Stosunki służbowe funkcjonariuszy służb mundurowych i żołnierzy zawodowych jako sprawa administracyjna*, Warszawa 2012, Difin.

Ustawa o Krajowej Administracji Skarbowej. Komentarz, L. Bielecki, A. Gorgol (red.), Warszawa 2018, Legalis.

Ustawa o Policji. Komentarz, K. Chałubińska-Jentkiewicz, J. Kurek (red.), Warszawa 2020, Legalis.

Wieczorek M., *Charakter prawny stosunków służbowych funkcjonariuszy służb mundurowych*, Toruń 2017, Wydawnictwo Adam Marszałek.

Winczorek P., *Prawo konstytucyjne Rzeczypospolitej Polskiej*, Warszawa 2003, Liber.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej (t.j.: DzU z 2019 r. poz. 1940).

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (t.j.: DzU z 2020 r. poz. 384, ze zm.).

Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (t.j.: DzU z 2020 r. poz. 505, ze zm.).

Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej (t.j.: DzU z 2020 r. poz. 848, ze zm.).

Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej (t.j.: DzU z 2016 r. poz. 1799, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j.: DzU z 2019 r. poz. 1921, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (t.j.: DzU z 2020 r. poz. 1221, ze zm.).

Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (t.j.: DzU z 2020 r. poz. 860, ze zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j.: DzU z 2020 r. poz. 27, ze zm.).

Ustawa z dnia 27 czerwca 1997 r. o partiach politycznych (t.j.: DzU z 2018 r. poz. 580).

Ustawa z dnia 26 kwietnia 1996 r. o Służbie Więziennej (t.j.: DzU z 2002 r. nr 207 poz. 1761, ze zm.).

Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (t.j.: DzU z 2020 r. poz. 1123, ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j.: DzU z 2020 r. poz. 360, ze zm.).

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j.: DzU z 2020 r. poz. 305, ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (t.j.: DzU z 1999 r. nr 51 poz. 526).

Ustawa z dnia 30 czerwca 1970 r. o służbie wojskowej żołnierzy zawodowych (t.j.: DzU z 1997 r. nr 10 poz. 55, ze zm.).

Orzecznictwo

Wyrok Europejskiego Trybunału Praw Człowieka z 20 V 1999 r., 25390/94, Legalis nr 102542.

Wyrok TK z 10 IV 2002 r., K 26/00. Legalis nr 53826, OTK Seria A 2002, nr 2, poz. 18, DzU z 2002 r. nr 56 poz. 517.

Wyrok TK z 15 IX 1999 r., K 11/99, OTK 1999 r., nr 6, poz. 116, Legalis nr 45366.

Wyrok NSA z 29 I 2020 r., I OSK 3250/18, Legalis nr 2286751.

Wyrok NSA z 16 I 2020 r., I OSK 2949/18, Legalis nr 2282018.

Wyrok NSA z 16 I 2020 r., I OSK 2748/18, Legalis nr 2287530.

Wyrok NSA z 12 VII 2019 r., I OSK 710/17, Legalis nr 2194129.

Wyrok NSA z 18 V 2018 r., I OSK 2439/16, Legalis nr 1837307.

Wyrok NSA z 4 VIII 2017 r., I OSK 1607/16, Legalis nr 1664019.

Wyrok NSA z 8 VI 2017 r., I OSK 656/16, Legalis nr 1632706.

Wyrok NSA z 23 III 2017 r., I OSK 436/16, Legalis nr 1632185.

Wyrok NSA z 18 XII 2014 r., I OSK 611/14, Legalis nr 1330014.

Wyrok NSA z 5 V 2011 r., I OSK 53/11, Legalis nr 352235.

Wyrok WSA w Lublinie z 11 II 2016 r., III SA/Lu 1108/15, Legalis nr 1434512.

Abstrakt

Niniejszy artykuł dotyczy zakazu członkostwa funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu w partii politycznej oraz uczestnictwa w działalności tej partii lub na jej rzecz. Zakaz, o którym mowa, został ustanowiony w art. 81 ust. 1 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Służba publiczna wymaga wprowadzenia pewnych ograniczeń praw funkcjonariuszy w stosunku do reszty członków społeczeństwa. Neutralność polityczna stanowi gwarancję właściwej realizacji zadań i celów wymienionych formacji. Wskazano, że przepis art. 81 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zawiera dwie niezależne od siebie normy prawne, tj. zakaz członkostwa w partii politycznej oraz zakaz uczestnictwa w działalności partii politycznej lub na jej rzecz. Uwagę skupiono na wskazaniu granic tych zakazów. W tym aspekcie wytyczono sferę dozwolonego zachowania funkcjonariusza. Podkreślono również, że ograniczenia, o których mowa, nie naruszają praw i wolności zagwarantowanych Konstytucją RP.

Słowa kluczowe: służba w ABW lub AW, stosunek służbowy, funkcjonariusz, partia polityczna, zakaz członkostwa w partii politycznej, zakaz uczestnictwa w działalności partii politycznej lub na jej rzecz.

The prohibition of political party membership and of participation in political party activities or on its behalf imposed on officers of the Internal Security Agency and Foreign Intelligence Agency

Abstract

This paper was entirely devoted to the issues connected with the prohibition of membership in a political party of an officer of the Internal Security Agency and Foreign Intelligence Agency and the participation in the activities of that party or on its behalf. This prohibition was established in Article 81 (1) of the Act of 24 May 2002 of the Internal Security Agency and Foreign Intelligence Agency. Public service requires the introduction of certain restrictions on the rights of officers in relation to the rest of members of society. Political neutrality guarantees proper implementation of the tasks and aims of this formation. There was indicated that aforementioned provision of Article 81 (1) of the Act of 24 May 2002 of the Internal Security Agency and Foreign Intelligence Agency contains two independent legal norms i.e. prohibition of membership in a political party and prohibition of participation in the activities of political party or on its behalf. Attention was therefore focused on indicating the limits of these prohibitions. In this aspect, the sphere of official behavior has been demarcated. There was also underlined that these limits in question do not violate the rights and freedoms guaranteed by the Polish Constitution.

Keywords: service in the Internal Security Agency and in the Foreign Intelligence Agency, service relationship, officer, politcal party, prohibition of membership in a political party, prohibition of participation in the activities of political party or on its behalf.

DANIEL MIDER
ORCID: 0000-0003-2223-5997

EWA ALEKSANDRA ZIEMAK
ORCID: 0000-0003-2516-3247

DOI: 10.4467/20801335PBW.21.003.13560

Technologie wspierające prywatność – ideologia, prawo, wdrożenia

Związek technologii kryptograficznych z terroryzmem był przedmiotem analiz prowadzonych pod koniec lat 90. XX w.[1] Obszernych opracowań doczekały się również powiązania między Internetem a terroryzmem[2]. W anglo- i polskojęzycznej literaturze przedmiotu brakuje natomiast analiz skupionych na ocenie praktycznego wykorzystania w działalności terrorystycznej dostępnych i szeroko używanych narzędzi informatycznych. Nie pozwala to na realną ocenę zagrożeń, jakie stwarza mariaż kryptoanarchizmu i terroryzmu. Niebezpieczeństwa z tym związane są sygnalizowane ogólnikowo, brakuje pogłębionych analiz (zazwyczaj poprzestaje się na stwierdzeniu popartym przykładami, że w działalności terrorystycznej Internet jest wykorzystywany do szerzenia propagandy, prowadzenia rekrutacji i zdobywania środków finansowych, bez choćby pobieżnego omówienia używanych narzędzi informatycznych)[3].

Autorzy niniejszego artykułu postawili następujące pytania badawcze:

- Jakimi zasobami koncepcyjnymi i technologicznymi mogą dysponować radykalni zwolennicy prywatności w Internecie oraz cyberprzestępcy?

---

[1] D.E. Denning, W.E. Baugh, *Encryption and evolving technologies: Tools of organized crime and terrorism*, Washington 1997, s. 1–64.

[2] United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes*, New York 2012; N. Malik, *Terror in the Dark. How terrorists use encryption, the darknet, and cryptocurrencies*, Millbank 2018; B. Clifford, H. Powell, *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, Washington 2019; C. Dion-Schwarz, D. Manheim, P.B. Johnston, *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats*, Santa Monica 2019.

[3] United Nations Office on Drugs and Crime, *The use of the Internet*…, s. 3.

- Jak można skategoryzować środki chroniące prywatność – jakie obszary komunikacji oraz działań w Internecie one obejmują?
- Jaki jest potencjał technologii wspierających prywatność w sytuacjach zastosowania ich do działań niezgodnych z prawem?
- Jaki jest zakres ochrony prawnej użytkowników technologii wspierających prywatność?
- Czy na podstawie analizy wybranych rozwiązań można stworzyć zestaw modelowych charakterystyk technologii wspierających prywatność?

Sformułowane pytania prowadzą do postawienia następującej tezy: Internet, dzięki któremu pojawiły się nowe sposoby komunikowania się, dał jednostkom – zwykłym obywatelom – ogromne, niespotykane wcześniej możliwości wywierania politycznego wpływu. To doprowadziło do powstania asymetrii pod tym względem między władzą a użytkownikiem technologii wspierających prywatność. Wspomniane możliwości stały się podstawą do sformułowania przez Andrew L. Shapiro wniosku o pojawieniu się „rewolucji kontroli" (*control revolution*[4]) – zjawiska rozproszenia władzy i przekazywania jej od elit do „końcowych użytkowników", czyli obywateli. Jej źródłem jest potencjał komunikacyjny Internetu[5]. W związku z postawioną tezą oraz pytaniami badawczymi autorzy artykułu sformułowali cztery hipotezy cząstkowe:

1. Technologie chroniące prywatność obejmują najważniejsze obszary związane z wymianą oraz przechowywaniem informacji i wartości: komunikację internetową, przechowywanie informacji oraz wymianę handlową.
2. Technologie chroniące prywatność stwarzają zabezpieczenia, które są trudne lub niemożliwe do złamania, zarówno przez przestępców, jak i służby dyspozycyjne.
3. Prawo jest instrumentalnie wykorzystywane do zwiększania ochrony informatycznej narzędzi wspierających prywatność.
4. Zestaw modelowych cech technologii wspierających prywatność nie powinien ograniczać się wyłącznie do cech o charakterze technicznym, lecz obejmować także walory ergonomiczne (łatwość instalacji i używania), społeczne (dostateczne wsparcie oraz promocja i popularyzacja produktu informatycznego), konstrukcyjno-organizacyjne (decentralizacja lub co najmniej federalizacja) i własnościowe (otwartoźródłowość).

---

[4] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski (przyp. red.).

[5] A.L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York 1999, s. 13.

Ideologiczno-doktrynalne fundamenty technologii chroniących prywatność

Ochrona prywatności nabrała nowego charakteru w latach 80. XX w. wskutek rozwoju technologii informatycznych. Uformował się wówczas ruch społeczny, którego doktrynalnym podłożem było przekonanie o wadliwej ochronie prawa do prywatności przez instytucje państwowe. Twierdzono, że sprzeniewierzyły się one potrzebie dbania o tę wartość i stanowią pod tym względem największe zagrożenie obywatela. To wówczas pojawiło się określenie *Privacy Enhancing Technologies* (dalej: PET), oznaczające ogół rozwiązań technicznych zapewniających użytkownikom pełną prywatność i wyłączną kontrolę nad danymi, które tworzą i przesyłają. Na przełomie lat 80. i 90. XX w. uformowała się grupa Cypherpunks (nazwa powstała *ad hoc*, w wyniku sytuacyjnego żartu), organizująca comiesięczne spotkania poświęcone prywatności oraz kontroli informacji prowadzonej przez rząd i korporacje. Impulsem do powstania tej grupy stał się artykuł Davida Chauma *Security without Identification: Transaction Systems to Make Big Brother Obsolete*[6] opublikowany w połowie lat 80. Nieco później pojawiła się nazwa ruchu – kryptoanarchizm. Wprowadził ją w 1992 r. Timothy C. May, amerykański pisarz, inżynier elektronik, dawny pracownik firmy Intel[7]. Jest on autorem innych publikacji ważnych dla środowiska kryptoanarchistycznego, m.in. *Cyphernomicon*[8] oraz *True Nyms and Crypto Anarchy*[9]. May jest również autorem najbardziej radykalnej koncepcji kryptoanarchizmu – tzw. rynku zabójców (*assassination market*), która pokazuje stopień determinacji w dążeniu do drastycznego ograniczenia informacyjnych apetytów państw[10]. Istotne znaczenie dla rozwoju ruchu miał treściwy manifest Chucka Hammilla *Od kuszy do kryptografii, czyli psucie państwu szyków przy pomocy techniki*[11] (tytuł oryginału: *From Crossbows to Cryptography. Thwarting the State via Technology*), w którym autor argumentował, że nieskrępowane dzielenie się informacją jest silniejszym sposobem oddziaływania na władze państwowe niż przemoc. Ważnym wkładem wydaje się również praca zbiorowa zatytułowana *Crypto Anarchy, Cyberstates, and Pirate Utopias*[12]. Obecnie ruch kryptoanarchistyczny stał się mniej radykalny, jednocześnie poddał się częściowej instytucjonalizacji.

---

[6] D. Chaum, *Security without Identification. Transaction Systems to Make Big Brother Obsolete*, „Communications of the ACM" 1985, nr 10, s. 1030–1044.

[7] T.C. May, *The Crypto Anarchist Manifesto*, Activism.net, 22 X 1992 r., https://www.activism.net/cypherpunk/crypto-anarchy.html [dostęp: 20 XII 2018].

[8] T.C. May, *Cyphernomicon. Cypherpunks FAQ and More, Version 0.666*, 10 IX 1994 r., http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html [dostęp: 20 XII 2018].

[9] T.C. May, *True Nyms and Crypto Anarchy*, grudzień 2001 r., http://www.isfdb.org/cgi-bin/title.cgi?195636 [dostęp: 20 XII 2018].

[10] T.C. May, *Cyphernomicon*…

[11] Ch. Hammill, *Od kuszy do kryptografii, czyli psucie państwu szyków przy pomocy techniki*, tłum. J. Sierpiński, „Kultura i Historia" 2007, nr 11, bez paginacji, http://www.kulturaihistoria.umcs.lublin.pl,/archives/701 [dostęp: 20 XII 2018].

[12] *Crypto Anarchy, Cyberstates, and Pirate Utopias*, P. Ludlow (red.), Cambridge 2001.

Warto wskazać następującą triadę: Electronic Frontier Foundation (https://www.eff.org/) powstałą w latach 90. XX w., Free Software Foundation (https://www.fsf.org/), założoną w 1985 r. przez Richarda Stallmana, amerykańskiego informatyka i hakera, legendę ruchu wolnego oprogramowania, oraz CryptoRights Foundation. Wszystkie wymienione organizacje to amerykańskie organizacje pozarządowe, które w istotny sposób, zarówno pod względem technicznym, jak i społecznym, przyczyniły się do zwiększenia bezpieczeństwa informacyjnego indywidualnych użytkowników.

Liczny i silny ruch na rzecz prywatności stworzył – co można dostrzec z perspektywy czasu – treści mało obszerne, o niezbyt wysokim poziomie merytorycznym i nieznane szerszej grupie odbiorców. Jest to cecha charakterystyczna technologii wspierających prywatność – ich zaplecze ideologiczne jest ubogie w treści oraz niewyszukane merytorycznie. Nie stanowi to jednak o jego wartości, gdyż w jego ramach powstały i powstają liczne „technologie wolności" przeznaczone do praktycznego aplikowania. Tematyka dotycząca technologii wspierających prywatność stała się przedmiotem obszernych publikacji o charakterze syntetycznym[13].

Za cezurę w sferze ochrony prywatności jednostki należy uznać rok 1976. Wówczas dwaj niezależni amerykańscy matematycy – Whitfield Diffie i Martin E. Hellman – stworzyli rewolucyjny system szyfrowania danych[14], którego złamanie zajęłoby setki lat nawet agencjom rządowym dysponującym nieograniczonymi środkami[15]. Opisali go w publikacji zatytułowanej *New Directions in Cryptography*, co wywołało liczne reperkusje, w tym prawne. Znaczenie opracowanej przez nich metody szyfrowania asymetrycznego (klucz publiczny, klucz prywatny)[16] najtrafniej ujął niezależny dziennikarz i specjalista z zakresu cyberbezpieczeństwa Jacob Applebaum, współautor (m.in. z Julianem Assangem) książki *Cypherpunks. Freedom and the Future of the Internet*. Napisał on: *Silna kryptografia może opierać się nieograniczonemu stosowaniu przemocy. Żadna siła przymusu nigdy nie rozwiąże problemu matematycznego* (w oryginale: *Strong cryptography can resist an unlimited application of violence. No amount of coercive force will*

---

[13] Zob. *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*, G.W. van Blarkom, J.J. Borking, J.G.E. Olk (red. nauk.), Haga 2003; *Privacy-enhancing technologies. The path to anonimity*, R. Hes, J.J. Borking (red. nauk.), Haga 2000 r.; Yang Wang, A. Kobsa, *Privacy-Enhancing Technologies*, w: *Handbook of Research on Social and Organizational Liabilities in Information Security*, M. Gupta, R. Sharman (red. nauk.), New York 2009; *Protecting privacy in practice. The current use, development and limits of Privacy Enhancing Technologies in data analysis*, A. Noble (red. nauk.), The Royal Society, marzec 2019 r., https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf [dostęp: 5 VIII 2020].

[14] Ch. Makdad, *"God Rewards Fools" – Whitfield Diffie and Martin Hellman's Stand to Revolutionize Cryptography*, The Eagle Eye News, https://tyroneeagleeyenews.com/wpcontent/uploads/2017/05/Makdad_Senior_TyroneAreaHighSchool_PA.pdf [dostęp: 1 VIII 2020].

[15] W. Diffie, M.E. Hellman, *New Directions in Cryptography*, „IEEE Transactions on Information Theory" 1976, nr 6, s. 644–654.

[16] W. Gogłoza, *Cypherpunks, WikiLeaks i widmo kryptograficznej anarchii*, https://wgogloza.com/umcs/informatyka-prawnicza/cypherpunks/ [dostęp: 20 XII 2018].

ever solve a math problem)[17]. A zatem siłą gwarantującą ochronę jednostki w zakresie prywatności nie mają być prawo i instytucje powołane na jego podstawie, lecz bezstronne prawa kryptografii, niepodatne na manipulację czy naciski.

Uregulowania prawne dotyczące ochrony prywatności

Technologie zwiększające czy też chroniące prywatność to złożony fenomen – prawny, socjologiczny i informatyczny jednocześnie. Jako fundament nowożytnej dyskusji na temat prywatności w kategoriach prawnych wskazuje się publikację amerykańskich prawników Samuela D. Warrena oraz Louisa D. Brandeisa zatytułowaną *The Right to Privacy*[18]. Autorzy zwrócili w niej uwagę na sferę życia wymagającą uregulowania z uwagi na okoliczności zaistniałe wskutek rozwoju społecznego. Obecnie prawo do prywatności lokuje się pośród praw człowieka pierwszej generacji i jest ono przedmiotem powszechnych i licznych uregulowań na poziomie prawodawstwa międzynarodowego oraz prawodawstw krajowych. Pośrednio sformułowano je w: art. 12 *Powszechnej deklaracji praw człowieka* z 10 grudnia 1948 r.[19], art. 17 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych* z 16 grudnia 1966 r.[20], art. 8 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności* z 4 listopada 1950 r.[21] oraz w art. 7 i 8 *Karty Praw Podstawowych Unii Europejskiej* z 7 grudnia 2000 r.[22] Wymienione akty określają jako bezprawną każdą arbitralną ingerencję w – co najistotniejsze z punktu widzenia niniejszej analizy – korespondencję i (lub) komunikację oraz formułują instytucjonalne prawo do ochrony prawnej przeciwko zamachowi na wskazane dobro.

Ochronę prywatności w prawie europejskim gwarantuje rozporządzenie Parlamentu Europejskiego i Rady UE z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych[23]. W art. 5 ust. 1 wskazanego rozporządzenia zostały sformułowane zasady dotyczące przetwarzania danych osobowych.

---

[17] J. Assange i in., *Cypherpunks. Freedom and the Future of the Internet*, New York–London 2012, s. 5.

[18] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, nr 5, s. 193–220.

[19] *Powszechna Deklaracja Praw Człowieka (Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana 10 grudnia 1948 r.).*

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

[21] *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* (DzU z 1993 r. nr 61 poz. 284).

[22] Dz. Urz. UE C 83 z 30 III 2010 r., s. 389.

[23] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 4 V 2016 r., s. 1).

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

To (…) *administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność")*[24]. W art. 6 ust. 1 rozporządzenia wskazano warunki, które muszą być spełnione, aby przetwarzanie było zgodne z prawem. Są one następujące:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym celu lub większej liczbie określonych celów,
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub

[24] Tamże, art. 5 ust. 2.

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W tym kontekście należałoby również zwrócić uwagę na terytorialny zakres stosowania omawianego rozporządzenia. Zgodnie z art. 3:

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:
   a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
   b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.
3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Jest to istotna zmiana dotycząca poszerzenia zakresu obowiązywania terytorialnego w porównaniu z chociażby poprzednio obowiązującą dyrektywą 95/46/WE, która posługiwała się bardzo ogólnym wyrażeniem „prowadzenie działalności gospodarczej".

Natomiast w Polsce zagadnienia dotyczące ochrony bezpieczeństwa reguluje ustawa o ochronie danych osobowych[25], która czasami odsyła do głównego aktu unijnego w zakresie ochrony danych, jakim jest omawiane wcześniej rozporządzenie Parlamentu i Rady UE. Ochronę wolności i tajemnicy komunikowania się gwarantuje art. 49 oraz – częściowo – art. 51 Konstytucji Rzeczpospolitej Polskiej[26], a także prawo karne (art. 267 *Kodeksu karnego*[27]), cywilne (art. 23 *Kodeksu cywilnego*[28]) oraz prawo autorskie (art. 82

[25] *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (t.j.: DzU z 2019 r. poz. 1781).

[26] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r*. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

[27] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

[28] *Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny* (t.j.: DzU z 2019 r. poz. 1145, ze zm.).

i 83 ustawy o prawie autorskim i prawach pokrewnych[29]). Jednak te prawa mogą być i faktycznie są ograniczane w sytuacji konfliktu z innymi wartościami, zwłaszcza bezpieczeństwem osobistym oraz szeroko pojętym bezpieczeństwem państwa. Ograniczenia, o których mowa, są sformułowane w wymienionych aktach (m.in. w art. 31 Konstytucji RP czy w art. 8 wspomnianej konwencji o ochronie praw człowieka i podstawowych wolności)[30]. Pomiędzy prawem do prywatności a bezpieczeństwem istnieje zatem nieusuwalny antagonizm.

Typologia technologii chroniących prywatność

Wartościowej, chociaż fragmentarycznej wiedzy na temat technologii chroniących prywatność dostarczają materiały publicystyczne i studia przypadków. Analiza literatury przedmiotu pokazuje, że terroryści wykorzystują w praktyce trzy grupy technologii wspierających prywatność.

Pierwsza z nich to oprogramowanie tworzone wyłącznie na potrzeby grup terrorystycznych, a konkretnie – najsilniejszej i najliczniejszej takiej grupy, tj. islamskich terrorystów. Opracowali oni własne narzędzia informatyczne. Przykładem jest Mojehedeen Secrets istniejący od 2007 r., przygotowany jako alternatywa dla Pretty Good Privacy i służący do szyfrowania korespondencji przesyłanej z użyciem poczty elektronicznej za pomocą popularnego algorytmu RSA[31] . Z kolei Tashfeer al-Jawwal, program powstały w 2013 r., umożliwia szyfrowanie urządzeń mobilnych. Jest to produkt Global Islamic Media Front, organizacji związanej z Al-Kaidą oraz innymi grupami terrorystycznymi. Ważnym, dynamicznie rozwijanym programem jest Amn al-Mujahed (opracowany w 2013 r.). Ma on zastosowanie uniwersalne – służy do szyfrowania poczty elektronicznej, wiadomości SMS oraz czatów.

Do drugiej grupy należą rozwiązania, które bazują na istniejących technologiach komunikacyjnych na zasadzie najprostszego, a jednocześnie możliwie najbardziej skutecznego użycia. Można je określić potocznym, używanym w socjolekcie internautów wyrażeniem *life hack*, oznaczającym niewyrafinowany, ale błyskotliwy sposób na coś. Korzystanie z nich wymaga znajomości technik inwigilacyjnych oraz infiltracyjnych stosowanych przez służby dyspozycyjne, przed którymi fakt komunikacji lub jej treść mają pozostać ukryte. Za przykład może posłużyć technika *dead dropping*, znana już od co najmniej trzech dekad. Polega ona na stworzeniu na koncie poczty elektronicznej wiadomości roboczej i niewysyłaniu jej, lecz

---

[29] *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych* (t.j.: DzU z 2019 r. poz. 1231).

[30] M. Pryciak, *Prawo do prywatności*, „Wrocławskie Studia Erazmiańskie" 2010, nr 4, s. 211–229.

[31] Algorytm Rivesta-Shamira-Adlemana – jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 r. przez Rona Rivesta, Adiego Shamira oraz Leonarda Adlemana. Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

podaniu odbiorcy danych logowania do danego konta poczty. Pozwala to na uniknięcie analizy i trasowania[32] takiej wiadomości, co jest czynione na przykład przez oprogramowanie inwigilacyjne Stanów Zjednoczonych należące do grupy PRISM[33]. W toku śledztwa dotyczącego zamachów w Paryżu w listopadzie 2015 r., podczas których zginęło 137 osób (w tym siedmiu sprawców), a ponad 300 zostało rannych, przypuszczano, że terroryści do komunikacji w celu zaplanowania zamachów użyli konsoli PlayStation 4. Istnieje kilka możliwości wysyłania trudnych do monitorowania wiadomości za pośrednictwem usługi gier online PlayStation Network (PSN) oraz prowadzenia rozmów głosowych lub komunikowania się za pomocą określonej gry. Dokumenty ujawnione przez Edwarda Snowdena w 2013 r. dowodzą, że Agencja Bezpieczeństwa Narodowego (dalej: NSA) i Centralna Agencja Wywiadowcza Stanów Zjednoczonych monitorowały takie gry, jak World of Warcraft, aby infiltrować komunikację islamskich terrorystów[34]. Konsola PlayStation 4 jest systemem prostym, ale trudnym do kontrolowania, trudniejszym do inwigilacji przez służby dyspozycyjne niż względnie bezpieczny komunikator WhatsApp. Innym przykładem może być używanie w latach 90. XX w. przez grupy pedofilów globalnego systemu grup dyskusyjnych Usenet[35]. Ich członkowie wymieniali się na forach dyskusyjnych zakazanymi treściami. Usenet był już wówczas starą technologią komunikacyjną, powstał bowiem w 1976 r. Postrzegany (błędnie) jako technologia schyłkowa, nie był w kręgu zainteresowania służb dyspozycyjnych. Technika wymiany zakazanych treści była banalnie prosta – plik graficzny lub filmowy zamieniano na tekst i w takiej postaci wklejano na forum. Wystarczyło skopiować wklejony blok tekstu i zastosować właściwe rozszerzenie pliku (np. jpg lub mpg), by uzyskać ukryte treści i odtworzyć je na komputerze lokalnym.

Trzecią grupę stanowi oprogramowanie powstałe w ramach szeroko rozumianego ruchu kryptoanarchistycznego. Jest ono powszechnie używane przez entuzjastów prywatności, dysydentów, ekstremistów, przestępców i cyberprzestępców oraz

---

[32] Trasowanie – wyznaczanie trasy i wysłanie nią pakietu danych w sieci komputerowej. Trasowanie ma na celu dostarczenie danych w sposób najbardziej optymalny. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

[33] D. Greene, *NSA Mass Surveillance Programs. Unnecessary and Disproportionate*, Electronic Frontier Foundation, 2014 r., https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf [dostęp: 1 VIII 2020].

[34] J. Austin, *'Traitor' Edward Snowden 'taught ISIS Paris terrorists how to avoid detection'*, „Express", 18 XI 2015 r., https://www.express.co.uk/news/world/620270/Traitor-Edward-Snowden-taught-ISIS-Paris-terrorists-avoid-detection-NSA-CIA-John-Brennan [dostęp: 2 VIII 2020]; J. Titcomb, *Did Paris terrorists really use PlayStation 4 to plan attacks?*, „The Telegraph", 16 XI 2015 r., https://www.telegraph.co.uk/technology/video-games/playstation/11997952/paris-attacks-playstation-4.html [dostęp: 1 VIII 2020]; S. Harris, *CIA's Ex-No. 2 Says ISIS 'Learned From Snowden'*, „Daily Beast", 12 VII 2017 r., https://www.thedailybeast.com/cias-ex-no-2-says-isis-learned-from-snowden [dostęp: 2 VIII 2020].

[35] E. Quayle, M. Taylor, *Paedophiles, Pornography and the Internet: Assessment Issues*, „British Journal of Social Work" 2002, nr 7, s. 863–875.

terrorystów – słowem wszystkich tych, którzy z różnych powodów pragną chronić zgromadzone dane oraz prowadzoną komunikację. Jest to zbiór narzędzi zróżnicowanych, jednak można z niego wyodrębnić oprogramowanie najpowszechniej używane i najbardziej przydatne wymienionym grupom (wydaje się, że jest to pośredni wskaźnik skuteczności takich narzędzi).

Na potrzeby artykułu oraz uniwersalnego systematyzowania narzędzi informatycznych wspierających prywatność zostaną wyróżnione trzy typy oprogramowania. Jednocześnie należy wskazać, że w literaturze przedmiotu istnieje kilka konkurencyjnych, ale niedoskonałych (co najmniej z punktu widzenia niniejszego artykułu) taksonomii technologii wspierających prywatność[36]. Na ogół wyróżnia się w nich dwa typy takich technologii – w wersji *soft* jest dopuszczane użycie jako pośrednika anonimizującego tzw. zaufanej trzeciej strony (*trusted third party*, TTP), natomiast w wersji *hard* usługa komunikacyjna musi być zdecentralizowana. Jak łatwo przewidzieć, terroryści koncentrują się na technologiach drugiego rodzaju ze względu na ich znacznie większe bezpieczeństwo.

Za podstawę wyodrębnienia trzech typów technologii wspierających prywatność przyjęto funkcję, jaką pełnią[37]. Pierwszy, podstawowy typ to technologie zapewniające anonimową lub pseudonimową komunikację (pozyskiwanie, przesyłanie, propagowanie informacji). Jako przykłady posłużyły: sieć anonimizująca The Onion Router (dalej: Tor)[38], sieć Freenet oraz dwa systemy operacyjne zaprojektowane do bezpiecznej i anonimowej komunikacji – Linux Tails oraz Whonix. Drugi typ to technologie wykorzystywane do anonimowej wymiany handlowej (zwykle wspomaganej siecią Tor), trudnej lub niemożliwej do skontrolowania. Przeanalizowano wykorzystanie takich systemów anonimowych kryptowalut, jak Monero, Zcash i Dash (tzw. *private coins*). Trzeci z typów technologii wspierających prywatność to bezpieczne przechowywanie informacji z użyciem zaawansowanych rozwiązań kryptograficznych. Za egzemplifikację posłużył program szyfrujący VeraCrypt.

Wyżej wymienione programy należą do rodziny tzw. wolnego oprogramowania (*free software*). Wolność oprogramowania niesie ze sobą istotne konsekwencje dla jakości świadczonych usług w zakresie prywatności. Warto zatem przyjrzeć się koncepcji wolności oprogramowania, jaka ukształtowała się przez ponad dwie dekady jej istnienia. Wolne oprogramowanie włącza cztery następujące uprawnienia, nazywane „wolnościami": wolność 0 – do wykorzystania programu w dowolnym celu (w tym komercyjnym), wolność 1 – do analizy kodu źródłowego, wolność 2 –

---

[36] Yun Shen, S. Pearson, *Privacy Enhancing Technologies: A Review*, HP Laboratories, sierpień 2011 r., https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf [dostęp: 1 VIII 2020]; G. Danezis, S. Gürses, *A critical review of 10 years of Privacy Technology*, Proceedings of Surveillance Cultures: A Global Surveillance Society, kwiecień 2010 r., https://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf [dostęp: 1 VIII 2020].

[37] Por. J. Heurix i in., *A taxonomy for privacy enhancing technologies*, „Computers & Security" 2015, t. 53, s. 1–17.

[38] Tor Project, https://www.torproject.org/ [dostęp: 1 VIII 2020].

do rozpowszechniania kopii (dowolnymi kanałami i w dowolnych ilościach), wolność 3 – do rozwijania oprogramowania (wolność 1 stanowi warunek niezbędny tej wolności). Anglojęzyczne określenie *free* odnosi się do wolności (*freedom*), nie zaś do darmowości (*for free*). Należy zatem rozumieć, że jest to oprogramowanie bez restrykcji lub z niewielką ich liczbą; jest więc zarówno „libre" (z hiszp. wolny, niezależny – przyp. red.), jak i „gratis". W praktyce oznacza to jednak także darmowość. Pojęcia *free software* nie należy mylić z pojęciem program otwartoźródłowy (*open source software*). O ile pierwsze z nich odnosi się do zagadnień ideologicznych, o tyle drugie – do technicznych. Jest ono pojęciem uproszczonym, zostało zawężone do konkretnego, materialnego pożytku, bez dyskusji o kwestiach światopoglądowych i etycznych. Otwartość kodu źródłowego oprogramowania oznacza, że jest ono dostępne dla analizy, a to ogranicza możliwość wprowadzenia do funkcji programu tzw. tylnych drzwi (*backdoors*) lub złotych kluczy (*golden keys*), czyli rozwiązań umożliwiających ominięcie zabezpieczających funkcji programu. Toczy się dyskusja dotycząca zasadności wprowadzania takich rozwiązań, pojawił się w niej nawet postulat konieczności ich wdrażania ze względu na potencjalne możliwości użycia takiego oprogramowania w działalności terrorystycznej[39].

Analiza wybranych narzędzi chroniących prywatność

Poniżej przeanalizowano narzędzia wspierające prywatność pod kątem ich przydatności do działalności komunikacyjnej, handlowej oraz magazynowania informacji przez ugrupowania terrorystyczne i cyberprzestępcze. Podano również uzasadnienia dotyczące wyboru poszczególnych narzędzi. Wybór najczęściej był podyktowany obserwowanym zainteresowaniem środowisk terrorystycznych i ekstremistów politycznych określonymi narzędziami informatycznymi[40].

Anonimowa komunikacja w Internecie

Niekwestionowanym liderem rozwiązań stosowanych w technologiach wspierających prywatność w zakresie komunikacji i dostępu do informacji jest wspomniana już sieć Tor. W literaturze przedmiotu jej wykorzystanie (zarówno faktyczne, jak i na poziomie hipotez i spekulacji) przez terrorystów oraz szerzej – w celach przestępczych –

[39] J.A. Lewis, D.E. Zheng, W.A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, Lanham–Boulder–New York–London 2017, s. 3.

[40] Zainteresowani systematycznym przeglądem narzędzi wspierających prywatność mogą skorzystać z witryny Privacy Tools, https://www.privacytools.io/ [dostęp: 1 VIII 2020]. Znajdują się tam systematyczny przegląd i ewaluacja produktów informatycznych wspierających prywatność w następujących kategoriach: dostawcy, przeglądarki, oprogramowanie, usługi, systemy operacyjne.

ma swoją długą i bogatą historię[41]. Związki sieci Tor z terroryzmem[42], pedofilią[43] i cyberprzestępczością[44] są w literaturze przedmiotu uznawane za oczywiste. Dlatego autorzy niniejszego artykułu skoncentrowali się na zagadnieniu dotyczącym możliwości i zakresu anonimizacji użytkownika tej sieci.

Projekt sieci anonimizującej Tor ujawniono i udostępniono jego kod źródłowy do użytku cywilnego we wrześniu 2003 r. Pierwotnie był to projekt militarny – pracowało nad nim Laboratorium Badawcze Marynarki Wojennej Stanów Zjednoczonych (United States Naval Research Laboratory). Aktualnie Tor działa na licencji BSD, jest zarządzany przez Fundację Tor Project, a kod źródłowy ma charakter otwarty, co daje częściową gwarancję transparentności projektu w postaci braku tzw. tylnych drzwi. Tor stwarza możliwość ukrycia tożsamości (geolokalizacji) konsumenta treści (tj. zwykłego użytkownika) oraz dostarczyciela treści. Umożliwia to w dwóch wymiarach: korzystania z Internetu powierzchniowego (tzw. *clearnetu*) oraz korzystania z domeny specjalnej sieci Tor – .onion. Komunikacja w sieci zachodzi z użyciem niezależnych i wielowarstwowo szyfrowanych pakietów (stąd określenie „trasowanie cebulowe" oraz nazwa projektu i domeny, w której on działa, „sieć cebulowa"). Szyfrowanie odbywa się z użyciem protokołu Diffiego-Hellmana. Połączenia z Internetem powierzchniowym odbywają się za pomocą obwodu (*circuit*) złożonego z trzech węzłów pośredniczących (kolejno: węzeł wejściowy, tj. *entry guard,* węzeł pośredniczący, tj. *middle relay*, oraz węzeł wyjściowy, tj. *exit relay*). Z kolei w usłudze ukrytej połączenie następuje za pośrednictwem sześciu węzłów (trzech dla konsumenta treści i trzech dla dostarczyciela treści). W tym przypadku kontakt z usługą ukrytą różni się od kontaktu z usługą realizowaną w Internecie powierzchniowym tym, że to usługa ukryta inicjuje połączenie (za pomocą tzw. punktu spotkania – *rendezvous point*). Ponadto usługi nigdy nie są dostępne bezpośrednio, tylko przy użyciu swoistych „skrzynek kontaktowych", które określa się mianem węzłów katalogowych. Aktualnie istnieje ponad 1400 węzłów oznaczonych flagą HSDir (*hidden service directory*), które wspólnie i na zasadzie konsensusu ogłaszanego w krótkich interwałach czasowych tworzą rozproszoną tablicę skrótów

---

41 G. Weimann, *Terror on the Internet: The New Arena, The New Challenges*, Washington 2006; G. Weimann, *Terrorism in Cyberspace: The Next Generation,* New York 2015; B. Berton, *The dark side of the web: ISIL's one-stop shop?*, raport European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 1 VIII 2020]; N. Malik, *Terror in the Dark*, raport Henry Jackson Society, Londyn 2015 r., http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf [dostęp: 1 VIII 2020]; G. Weimann, *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict & Terrorism" 2016, nr 3, s. 195–206.

42 N. Malik, *Terror in the Dark. How terrorists use encryption, the darknet, and cryptocurrencies*, Millbank 2018; G. Weimann, *Terrorist Migration to the Dark Web*, „Perspectives on Terrorism" 2016, nr 3, s. 40–44.

43 K.V. Acar, *Child abuse materials as digital goods: Why we should fear new commercial forms*, „Economics Discussion Papers" 2017, nr 15, bez paginacji.

44 D. Mider, *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 154–190.

(*distributed hash table*, DHT). To oznacza, że nigdy żadna strona kontaktu nie może poznać swojej lokalizacji.

Stan sieci Tor jest monitorowany, a wyniki obserwacji są publikowane. Monitoring jest zapewniany przez dziewięć zaufanych serwerów (od 2019 r.), znanych jako węzły katalogowe. Każdy z nich jest kontrolowany przez inną organizację. Taka budowa sieci Tor częściowo eliminuje problem zaufanej trzeciej strony (jest ich wiele, zatem podwyższa to koszty ewentualnego naruszenia anonimowości użytkownika).

Sieć Tor cieszy się globalnie rosnącą popularnością – według Tor Metrics korzysta z niej ponad 2 mln użytkowników dziennie, ma ona ponad 6 tys. węzłów, a ruch przekracza 200 Gbit/s[45]. Jej użytkownicy znajdują się głównie w Stanach Zjednoczonych, Rosji, Niemczech, Francji, Wielkiej Brytanii, Holandii i Indonezji. W tym kontekście należy zwrócić uwagę na pewien paradoks techniczny. Otóż warunkiem anonimowości w sieci Tor jest korzystanie z niej przez wiele osób, czego nie uwzględniono przy jej projektowaniu.

Najważniejszą cechą charakterystyczną jest ograniczona anonimizacja typów połączeń w sieci Tor – szyfrowane, a przez to anonimowe, są połączenia ze stronami www, polecenia powłoki systemowej (*shell*) oraz komunikatory internetowe (*instant messaging*). To oznacza, że anonimizacja następuje wyłącznie przy przeglądaniu stron internetowych, wydawaniu zdalnych rozkazów w linii poleceń oraz komunikowaniu za pomocą czatów. Z Tor należy korzystać z użyciem wtyczki HTTPS Everywhere wbudowanej w przeglądarkę, wymuszającej szyfrowanie komunikacji pomiędzy użytkownikiem a stroną internetową. Użytkownik pozostaje wówczas w pełni bezpieczny wobec następujących podmiotów:

- **hakerów** (którzy uzyskali dostęp do sieci domowej użytkownika) – znają lokalizację użytkownika i wiedzą, że używa on sieci Tor, nie wiedzą jednak, z jaką stroną się łączy, nie poznają jego loginu i hasła oraz nie dowiedzą się, jakie dane pobiera;
- **dostawców usług internetowych** (a pośrednio służb) – jw.;
- **służb dyspozycyjnych** (*via clearnet*) – jw.;
- **służb dyspozycyjnych** (*via* węzeł wyjściowy Tor) – jw., jednak nie poznają lokalizacji użytkownika;
- **usługodawców** (dostarczycieli treści, właścicieli serwera, a pośrednio służb) – poznają wszystkie informacje (i tak powinno być), z wyjątkiem lokalizacji użytkownika korzystającego z danych.

Mechanizmy anonimizacyjne mogą zostać usprawnione za pomocą usługi przekaźników mostkowych (*bridges*) oraz transportu wtykowego (*pluggable transport*).

Mosty (ich pełna nazwa to przekaźniki mostkowe) są przekaźnikami (węzłami wejściowymi) sieci Tor, które nie są wymienione w głównym katalogu Tora. Ponieważ nie ma ich pełnej publicznej listy, to nawet jeśli dostawca usług internetowych filtruje połączenia do wszystkich znanych przekaźników sieci Tor, prawdopodobnie nie będzie

[45] Tor Metrics, https://metrics.torproject.org/ [dostęp: 1 VIII 2020].

w stanie zablokować wszystkich mostów. Mają one zatem zastosowanie w sytuacji, gdy węzły wejściowe sieci Tor są blokowane (cenzura). Z przekaźnika mostkowego można korzystać na dwa sposoby: przez włączenie takiej opcji w samej przeglądarce Tor (wybór odbywa się automatycznie) albo przez wybór samodzielnie uzyskanego węzła (informację pozyskuje się po wysłaniu prośby na adres e-mail: bridges@torproject.org, wyłącznie jednak ze skrzynki założonej u jednego z dwóch dostawców: Riseup lub Gmail).

Transport wtykowy wprowadzono w celu obejścia mechanizmu cenzury. Mosty mogą być bowiem blokowane po rozpoznaniu ruchu charakterystycznego dla transmisji sieci Tor. Zwykle służą do tego specjalne urządzenia instalowane u dostawców usług internetowych, które analizują ruch sieciowy i wykrywają tę sieć, a po jej wykryciu blokują przepływ ruchu. Transport wtykowy manipuluje całym ruchem w sieci Tor między klientem a jego pierwszym przeskokiem, tak że nie można go zidentyfikować jako połączenia sieci Tor. Obecnie transport wtykowy jest realizowany za pomocą mechanizmów obfs4 (od *obfuscate*, tj. zaciemniać) oraz meek-azure. Rozwiązanie maksymalizuje bezpieczeństwo użytkownika (dostawca Internetu nie wie, że użytkownik korzysta z sieci Tor), jednak jakość połączenia (transmisja danych) maleje. Działanie tego mechanizmu polega na symulowaniu, jakoby użytkownik korzystający z Tora przeglądał dużą stronę internetową (np. Microsoft). Mechanizm meek-azure jest polecany użytkownikom z Chin, obfs4 zaś – do zastosowań globalnych.

Zdecentralizowana anonimowa sieć dystrybucji informacji – Freenet. Jest to sieć, która nie ma żadnego serwera sterującego ruchem lub przechowującego rejestr adresów, jej zasoby są więc całkowicie rozproszone. Pomysłodawcą i autorem Freenetu jest Ian Clarke. Sieć została napisana w języku Java, jest rozwijana od marca 2000 r. Zapewnia ona prywatność, ale nie anonimowość. Jej działanie jest następujące: komputery połączone w sieć są równorzędne i każdy z nich jest jednocześnie serwerem danych (węzłem komunikacyjnym). Jest to topologia siatki (*full mesh*), a więc bezserwerowa, dzięki temu, że instalując Freenet, każdy użytkownik udostępnia część przestrzeni swojego dysku twardego na potrzeby działania całości sieci. Ta przestrzeń jest ściśle odizolowana od reszty zasobów znajdujących się na komputerze, a użytkownik nie ma możliwości sprawdzenia, co jest zdeponowane, a także przesyłane przez jego komputer. Jest to architektura rozproszonej sieci peer-to-peer (P2P), jednak z tą zasadniczą różnicą, że po wprowadzeniu pliku do sieci użytkownik traci kontrolę nad jego lokalizacją. Dane w losowych interwałach są losowo przenoszone z jednego komputera (węzła sieci) na inny, a ich pobieranie nigdy nie odbywa się bezpośrednio. Adresowanie dokonuje się za pomocą kluczy będących kryptograficznymi funkcjami skrótu, nieodzwierciedlającymi fizycznej lokalizacji zasobu[46].

Warto wspomnieć w tym miejscu o projekcie, który łączy zalety sieci Tor i Freenet, a jednocześnie nie ma ich wad. Jest to Invisible Internet Project (dalej: I2P) powstały

[46] Oficjalna strona projektu Freenet: https://freenetproject.org/author/freenet-project-inc.html [dostęp: 1 VIII 2020]; D. Mider, *Czarny i czerwony*…, s. 158–159.

w 2003 r., jednak do chwili obecnej nie osiągnął on statusu RTM (*release to manufacting*, tj. stabilny i gotowy do wypuszczenia na rynek)[47].

Systemy operacyjne zogniskowane na prywatności pochodzą z rodziny systemów GNU Linux wykorzystujących sieć Tor (najczęściej w wersji ulepszonej, bardziej zaawansowanej i niedostępnej dla zwykłych użytkowników Tora). Należą do nich przede wszystkim Linux Tails[48] oraz Whonix[49]. Nowość w zakresie rozwiązań informatycznych (zarówno pod względem konstrukcji, jak i wykorzystania sieci Tor) stanowi system operacyjny Qubes OS[50], jednak ze względu na wymagania związane z kompetencjami użytkowników (na etapie instalacji, ale przede wszystkim użytkowania) nie jest to rozwiązanie, które szybko się upowszechni. Wśród innych dystrybucji systemu GNU Linux skoncentrowanych na bezpieczeństwie i w znacznym stopniu chroniących prywatność należy wskazać przede wszystkim system Debian, który istnieje od ćwierć wieku i jest uznawany za bezpieczny i stabilny. Skupia on liczną, szybko reagującą społeczność użytkowników, programistów i specjalistów w dziedzinie bezpieczeństwa. Spośród innych systemów warto wymienić Arch, Alpine i Fedorę. Każdy z nich w pewien sposób zapewnia bezpieczeństwo, ale wymaga to wiedzy, umiejętności i wysiłku ze strony użytkownika.

Wspomniane systemy Linux Tails i Whonix oparte na GNU Linux Debian jako kompleksowe rozwiązania zapewniające swoim użytkownikom maksymalną anonimowość i niewykrywalność zajmują niezwykle ważne miejsce.

Linux Tails[51] to system operacyjny polecany wśród cyberprzestępców i terrorystów[52]. Agencja Bezpieczeństwa Narodowego USA jednoznacznie klasyfikuje jego użytkowników jako ekstremistów[53]. Wśród nich znajduje się m.in. Państwo Islamskie (ISIS)[54]. Początki Linux Tails sięgają pierwszej połowy 2009 r. Powstał on jako połączenie systemów Linux Incognito LiveCD (projekt wstrzymany w 2010 r.) i Amnesia, a został opracowany przez zespół anonimowych hakerów finansowanych przez Free Press Foundation, Debian, Mozillę oraz Tor Project. Przy jego tworzeniu inspirowano się również projektami Live Privatix oraz Liberté Linux. Tails to akronim od The Amnesic Incognito Live System, w której to nazwie wskazano najważniejsze cechy produktu.

---

47 Oficjalna strona projektu Invisible Internet Project: http://www.i2p2.de/en/ [dostęp: 1 VIII 2020].

48 Linux Tails, https://tails.boum.org/ [dostęp: 1 VIII 2020].

49 Whonix. Privacy & Anonimity OS, https://www.whonix.org/ [dostęp: 1 VIII 2020].

50 Qubes OS, A Reasonably Secure Operating System, https://www.qubes-os.org/ [dostęp: 1 VIII 2020].

51 Omawiana, aktualna wersja to 4.9. z 13 VII 2020 r.

52 J. Appelbaum i in., *NSA targets the privacy-conscious*, ARD 1 Das Erste, 3 VII 2014 r.

53 H. Arora, *NSA classifies Linux Journal readers, Tor and Tails Linux users as "extremists"*, 4 VII 2014 r., https://static.techspot.com/community/topics/nsa-classifies-linux-journal-readers-tor-and-tails-linux-users-as-extremists.203649/page-3 [dostęp: 1 VIII 2020].

54 B. Goodwin, *Islamic State supporters shun Tails and Tor encryption for Telegram*, „Computer Weekly", 8 I 2017 r., https://www.computerweekly.com/news/450419581/Islamic-State-supporters-shun-Tails-and-Tor encryption-for-Telegram [dostęp: 1 VIII 2020].

„Amnesic" należy rozumieć jako wbudowany mechanizm usuwania informacji, które potencjalnie mogą doprowadzić do identyfikacji użytkownika. Linux Tails w podstawowej konfiguracji nie przechowuje żadnych plików zapisanych lub utworzonych przez użytkownika, a także żadnych jego ustawień, zainstalowanych programów, modyfikowanej konfiguracji, odwiedzonych witryn (w tym w trybie prywatnym), haseł oraz urządzeń i sieci wi-fi. Jest to możliwe dzięki Nautilus Wipe. Standardowe sposoby kasowania plików w rzeczywistości nie usuwają zawartości danego pliku (nawet po opróżnieniu kosza), jedynie czyszczą tablicę alokacji. Natomiast Nautilus Wipe czyści tę część nośnika, w której dane znajdowały się fizycznie. Własne pliki oraz zainstalowane programy (Tails oferuje aktualnie trzy bezpieczne repozytoria) można oczywiście przechowywać, ale wyłącznie wtedy, gdy przy uruchamianiu systemu (tzw. bootowaniu) wprowadzi się hasło administratora (domyślnie Tails jest pozbawiony użytkownika *root*[55] w celu maksymalizacji bezpieczeństwa) oraz stworzy się zaszyfrowany kontener przeznaczony do takiego dodatkowego oprogramowania. Bezpieczeństwo jest zapewniane również przez mechanizm nadpisywania pamięci o dostępie losowym (RAM) przy każdym wyłączaniu Linux Tails. Zapobiega to m.in. tak zwanym atakom zimnego rozruchu (*cold boot attacks*).

„Incognito" w nazwie oznacza z kolei wdrożenie zaawansowanych mechanizmów strzeżenia tożsamości użytkownika. Anonimizacja jest zapewniana dzięki użyciu systemu Tor. Tails co prawda zdradza na zewnątrz, że doszło do użycia sieci Tor, jednak implementuje funkcje, które uniemożliwiają, a co najmniej utrudniają, odróżnienie użytkowników systemu Tails od innych użytkowników. Tor chroni adres IP użytkownika, dodatkowo i opcjonalnie jest zabezpieczony adres fizyczny urządzenia sieciowego (MAC adres karty wi-fi/Ethernet). Warto jednak wiedzieć, że twórcy systemu nie zadbali o eliminowanie odcisku palca tzw. niebezpiecznej przeglądarki (*unsafe browser*). Zidentyfikowanie użytkownika systemu Tails jest jednak możliwe na podstawie pewnych wskaźników inferencyjnych (takich jak np. niegenerowanie z danej maszyny ruchu innego niż Tor; zwykły użytkownik jest źródłem takiego ruchu) – paradoksalnie zatem mechanizmy anonimizacji stają się źródłem częściowej deanonimizacji. Tails nie implementuje podstawowego mechanizmu sieci Tor, jakim jest mechanizm ochrony węzła wejściowego. Działanie chroniące węzeł wejściowy polega na przypisaniu maszynie, na której uruchomiono Tor, na stałe (okres ok. 45 dni ± 15 dni) puli węzłów wejściowych. Ten mechanizm ma chronić sieć Tor globalnie, czyli uniemożliwić lub utrudnić ataki przez analizę ruchu, to jest wyliczanie adresów IP użytkowników sieci przez obserwowane lub kontrolowane węzły wejściowe przechwytujące ruch. Utrudnienie polega również na zwiększaniu kosztów potencjalnie ponoszonych przez węzły ukryte. Z drugiej strony ten właśnie mechanizm staje się ewentualnym czynnikiem deanonimizacji z perspektywy końcowego użytkownika. Funkcja „incognito" to zatem silne i różnorodne mechanizmy szyfrowania komunikacji oraz samego systemu.

---

[55] *Root* (pol. korzeń) – tradycyjna nazwa uniksowego konta, które ma pełną kontrolę nad systemem operacyjnym. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

„Live" wskazuje na jeden z elementów systemu bezpieczeństwa (system znajduje się w niezmiennej formie i nawet po jednorazowym naruszeniu integralności zostaje przywrócony do stanu pierwotnego), ale również na wygodę użytkowania (można go uruchomić na dowolnej – z kilkoma wyjątkami – maszynie, do której jest dostęp fizyczny oraz BIOS/UEFI nie są zabezpieczone hasłem). System „live" oznacza możliwość uruchamiania w pełni funkcjonalnego systemu operacyjnego bez konieczności instalowania go na dysku twardym. Linux Tails może być uruchamiany zarówno jako „live USB", jak i „live CD", przy czym ze względów bezpieczeństwa jest zalecana ta druga opcja (istnieje znacznie większa możliwość nadpisania urządzenia pamięci masowej, tj. pendrive'a, niż płyty CD zabezpieczonej przed zapisem). Linux Tails może być uruchamiany również na maszynach wirtualnych, jednak Microsoft Windows i MacOS to oprogramowania zastrzeżone i nie można ich uznać za godne zaufania (pozostaje wykorzystanie wirtualizacji w tych systemach wyłącznie w celach testowych lub edukacyjnych).

Rękojmią prywatności oprogramowania Linux Tails jest transparentne finansowanie – we wsparciu partycypują głównie podmioty pozarządowe, a w mniejszym wymiarze – komercyjne. Są to m.in. Mozilla Open Source Support (w 2017 r. ponad 50 tys. dolarów, w 2019 r. ponad 100 tys. dolarów), Handshake (w 2019 r. ponad 100 tys. dolarów), Open Technology Fund (w 2016 r. ponad 50 tys. dolarów), Hivos People Unlimited. Linux Tails powstaje przy stałym wsparciu Tor Project Foundation (nieprzerwanie od momentu powstania, tj. od 2010 r.). Ponadto cały kod oprogramowania jest publiczny, co umożliwia niezależnym badaczom bezpieczeństwa audyt funkcji Tails w dowolnym momencie.

Przy tworzeniu systemu operacyjnego Whonix skoncentrowano się na zaawansowanych funkcjach bezpieczeństwa i anonimowości – jest on w pełni funkcjonalną, wzmocnioną (*hardening*) wersją systemu Debian. Konstrukcja tego systemu jest wyjątkowa. Whonix jest złożony z dwóch maszyn wirtualnych – Whonix-Gateway oraz Whonix-Workstation przeznaczonych do użytku w postaci zwirtualizowanej[56]. Jest to darmowy i otwarty systemem operacyjny, który został stworzony jako narzędzie przeciwko cenzurze. Jednak nie jest to rozwiązanie zapewniające bezpieczeństwo „jednym kliknięciem" – wymaga więcej kompetencji informatycznych, zarówno podczas instalacji, jak i w użytkowaniu, niż Linux Tails. System Whonix ma wbudowane zaawansowane funkcje bezpieczeństwa. Jako jedyny zapewnia ochronę przed wysoce profesjonalnymi atakami deanonimizacyjnymi, zapobiega profilowaniu i deanonimizacji na podstawie wzorców behawioralnych użytkowania klawiatury (*keystroke dynamics*, szeroko ujęta stylometria, odcisk cyfrowy klawiatury lub myszy), zapewnia szczelność, chroniąc

[56] Wirtualizacja polega na utworzeniu symulowanego (wirtualnego) środowiska komputerowego, które stanowi przeciwieństwo środowiska fizycznego; obejmuje wygenerowane komputerowo wersje sprzętu, systemów operacyjnych, urządzeń magazynujących. Whonix jest uruchamiany w pamięci RAM systemu operacyjnego gospodarza (np. Windows, innego systemu Linux) za pośrednictwem programu nazywanego maszyną wirtualną (może to być np. Oracle Virtualbox, VMware, zaleca się jednak Kernel-based Virtual Machine, KVM, działających wyłącznie w systemach GNU Linux).

przed wyciekami DNS[57] i wyciekami strefy czasowej (Dev/TimeSync). Whonix oferuje AppArmor, czyli system obowiązkowej kontroli dostępu, który ogranicza uprawnienia aplikacji zgodnie z zestawem reguł określających, do których plików dany program może uzyskać dostęp. To proaktywne podejście chroni system operacyjny i aplikacje przed zewnętrznymi lub wewnętrznymi zagrożeniami. Whonix ma wbudowany mechanizm wymuszonej anonimowości – cały ruch sieciowy jest zapośredniczany wyłącznie przez sieć Tor. Ponadto zapewnia ochronę przed profilowaniem na złośliwych węzłach wejściowych Tora, a także obsługuje mechanizm izolacji strumieni. System, o którym mowa, mnoży połączenia Tora i ustala dla każdego połączenia odrębnie marszrutę przez sieć Tor, co utrudnia śledzenie aktywności użytkownika. Klasyczny mechanizm Tora nie ma tego rozwiązania. Ciekawym pomysłem jest SecBrowser – bezpieczna, ale nieanonimowa przeglądarka. Warto nadmienić, że Whonix nie ma jeszcze funkcji nadpisywania pamięci RAM podczas zamykania systemu, którą zapewnia Linux Tails. Średnio zaawansowani użytkownicy mogą jednak wdrożyć inne mechanizmy[58].

Anonimowa wymiana handlowa

Kryptowaluty to zagadnienie wielowymiarowe – zarówno pod względem technicznym, jak i politycznym[59], prawnym[60] i ekonomicznym[61]. Aktualnie istnieje ponad 6 tys. kryptowalut o różnych parametrach informatycznych, ekonomicznych i kryptograficznych[62], a łączna kapitalizacja tego rynku sięga obecnie (sierpień 2020 r.) 347 mld dolarów amerykańskich[63]. Ideologiczno-polityczne korzenie kryptowalut silnie tkwią w środowiskach anarchistycznych, hakerskich i hipisowskich[64], same

---

[57] Domain Name System (pol. system nazw domen) – hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen. Dzięki DNS nazwa mnemoniczna, np. pl. wikipedia.org, jest tłumaczona na odpowiadający jej adres IP. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

[58] Szerzej na ten temat: *Whonix Documentation*, https://www.whonix.org/wiki/Documentation [dostęp: 1 VIII 2020].

[59] B.B. Barbirato, *Bitcoin: A Political Analysis*, maj 2016 r., https://www.researchgate.net/publication/309411431_Bitcoin_A_Political_Analysis [dostęp: 1 VIII 2020].

[60] S. Jafari i in., *Cryptocurrency: A Challenge to Legal System*, Social Science Research Network, styczeń 2018 r., https://www.researchgate.net/publication/325747817_Cryptocurrency_A_Challenge_to_Legal_System [dostęp: 1 VIII 2020].

[61] D. Stancel, *Economic Consequences of Cryptocurrencies and Associated Decentralized Systems*, https://www.researchgate.net/publication/280794376_Economic_Consequences_of_Cryptocurrencies_and_Associated_Decentralized_Systems [dostęp: 1 VIII 2020].

[62] *6,208 crypto currencies*, https://coinlib.io/coins [dostęp: 1 VIII 2020].

[63] Informacja za: TradingView, https://pl.tradingview.com/ [dostęp: 1 VIII 2020]. Podana wartość była dwukrotnie wyższa (i najwyższa w historii) w 2018 r., osiągnęła niemal 700 mld dolarów amerykańskich.

[64] B. Maurer, T.C. Nelms, L. Swartz, *When Perhaps the Real Problem Is Money Itself! The Practical Materiality of Bitcoin,* „Social Semiotics" 2013, nr 2, s. 261–277.

kryptowaluty zaś są postrzegane jako antypolityczne[65]. Liczni zwolennicy, twórcy i użytkownicy kryptowalut hołdują rozmaitym odmianom ideologii anarchistycznej, w tym libertariańskiej[66]. Raporty wykazują, że kryptowaluty są wykorzystywane przez państwa zbójeckie[67], handlarzy narkotyków[68], handlarzy innymi dobrami zakazanymi[69] (w tym do handlu bronią[70]) oraz służą do legalizacji środków finansowych pozyskanych z działalności przestępczej (pranie brudnych pieniędzy)[71]. Jeśli chodzi o finansowanie terroryzmu z użyciem kryptowalut, to zdania są podzielone. Niektórzy autorzy wskazują, że organizacje terrorystyczne chętnie używają tego typu walut, a w literaturze przedmiotu odnajdujemy studia przypadków oraz opracowania o charakterze syntetycznym na ten temat[72]. Z drugiej strony zeszłoroczny raport RAND podważa część tych ustaleń oraz wskazuje bariery sprawiające, że kryptowaluty nie stanowią optymalnego rozwiązania finansowego w działalności terrorystycznej[73]. Z punktu widzenia działalności terrorystycznej czy przestępczej (w tym cyberprzestępczej) środek płatniczy, jakim jest kryptowaluta, winien mieć następujące cechy: anonimowość, płynność, stabilność i łatwość użytkowania. W im mniejszym stopniu

---

[65] R. Herian, *The Politics of Blockchain*, „Law and Critique" 2018, nr 2, s. 129–131.

[66] I. Eyal, *Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities*, „Computer" 2017, nr 9, s. 38–49; C. Faife, *Live Free or Mine: How Libertarians Fell in Love With Bitcoin*, CoinDesk, 8 X 2016 r., https://www.coindesk.com/live-free-or-mine-how--libertarians-fell-in-love-with-bitcoin [dostęp: 1 VIII 2020]; H. Karlstrøm, *Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin*, „Distinktion: Scandinavian Journal of Social Theory" 2014, nr 1, s. 23–36. Zob. także raport z badań dotyczących sympatii ideologicznych użytkowników kryptowalut: P. Ryan, *Left, Right and Center: Crypto Isn't Just for Libertarians Anymore*, CoinDesk, 27 VII 2018 r., https://www.coindesk.com/no-crypto-isnt-just-for-libertarians-anymore [dostęp: 1 VIII 2020].

[67] G. Hurlburt, *Shining Light on the Dark Web*, „IEEE Computer" 2017, nr 4, s. 100–105.

[68] M.C. Van Hout, T. Bingham, *Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences*, „International Journal of Drug Policy" 2013, nr 5, s. 385–391.

[69] A.T. Zulkarnine i in., *Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content*, IEEE Conference on Intelligence and Security Informatics (ISI), Tucson 2016 r., s. 109–114, https://ieeexplore.ieee.org/xpl/conhome/7739307/proceeding [dostęp: 3 VIII 2020].

[70] G. Weimann, *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict and Terrorism" 2016, nr 3, s. 195–206.

[71] V. Dostov, P. Shust, *Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?*, „Journal of Financial Crime" 2014, nr 3, s. 249–263.

[72] S. Higgins, *ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide*, CoinDesk, 7 VII 2014 r., https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/ [dostęp: 1 VIII 2020]; T. Keatinge, D. Carlisle, F. Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, 2018 r., http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf [dostęp: 1 VIII 2020]; Y.J. Fanusie, T. Robinson, *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies, and Elliptic, 12 I 2018 r., http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf, s. 7 [dostęp: 1 VIII 2020].

[73] C. Dion-Schwarz, D. Manheim, P.B. Johnson, *Terrorist Use of Cryptocurrencies*…

transakcje mogą być śledzone i w im mniejszym stopniu da się je powiązać z tożsamościami użytkowników, tym bardziej taki środek płatniczy jest użyteczny. Jest to zapewniane za pomocą wielu mechanizmów kryptograficznych. Warto podkreślić, że anonimowość danej kryptowaluty nie jest nigdy dana raz na zawsze – jest to nieustanny wyścig miecza i tarczy[74]. Płynność jest rozumiana jako łatwość wymiany na inne kryptowaluty, w tym waluty fiat. To implikuje takie cechy, jak powszechność, wiedza i świadomość użytkowników, zaufanie do środka płatniczego oraz istnienie niezbędnej infrastruktury technicznej (tzw. górnicy zatwierdzający transakcje i tworzący blockchaina, portfele do przechowywania kryptowalut, oficjalne poradniki itp.). Wiąże się to z łatwością użytkowania pod względem oprogramowania (wygodne w użyciu portfele, dostępne zarówno na komputerach, jak i na tabletach lub smartfonach) oraz nieskomplikowaną obsługą. Istotną cechą, aktualnie niespełnialną w odniesieniu do kryptowalut, jest stabilność, ze względu na silne i raczej nieprzewidywalne wahania ich kursów. Zadowalająca jest względna stabilność finansowa, a więc wystarczająco długi czas istnienia i kapitalizacji.

Warto odnotować, że najpopularniejsza kryptowaluta – bitcoin, jakkolwiek używana w celach przestępczych czy terrorystycznych, nie spełnia wszystkich wymienionych warunków. Po pierwsze, bitcoin nie jest anonimowy, lecz pseudonimowy (eliminacja funkcji śledzących odbywa się przez tzw. miksery bitcoinów[75]), po drugie, nie jest on walutą wygodną w transakcjach (koszt transakcji). Zapewnienie anonimowości podczas wymiany z użyciem bitcoinów jest możliwe, jednak wymaga użycia dodatkowych środków (sposoby nabycia, użycie protokołów anonimizujących, np. Tor, I2P).

Dostępne są liczne kryptowaluty wspierające anonimowość użytkownika (*private coins*). Jest to nazwa zbiorcza i należy podkreślić, że ta prywatność bywa rozmaicie wywodzona, rozumiana i implementowana[76]. Pośród systemów *private coins* liczących się w rankingu wymienia się Monero (XMR) – zajmujące 15. miejsce w globalnym rankingu kryptowalut, Dash – 25. miejsce, Zcash – 26. miejsce, a także inne, mniej znaczące, jak: Verge (XVG) – opierający się na sprawdzonych rozwiązaniach anonimizacji (Tor i I2P), Horizen (ZEN) – mający mechanizmy anonimizacji homologiczne jak w systemie Zcash, a także Komodo (KMD), stanowiący tzw. *fork*, czyli rozwidlenie,

---

[74] A. Greenberg, *The dark web's favorite currency is less untraceable than it seems*, „Wired", 27 III 2018 r., https://www.wired.com/story/monero-privacy/ [dostęp: 1 VIII 2020].

[75] T. de Balthasar, J. Hernandez-Castro, *An Analysis of Bitcoin Laundry Services*, Nordic Conference on Secure IT, Tartu 2017 r., https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services [dostęp: 4 VIII 2020].

[76] Pogłębionej analizy motywów oraz sposobów rozumienia prywatności wybranych kryptowalut na podstawie analizy 333 tzw. *whitepapers* (dokument dostarczany przez twórców danej kryptowaluty, obejmujący techniczne, ekonomiczne i społeczno-polityczne założenia i cele projektu) dokonali: J. Harvey, I. Branco-Illodo, *Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in 'Privacy Coin' Whitepapers*, „Journal of Political Marketing" 2020, nr 1–2, s. 107–136.

projektu Zcash[77]. Wymienione systemy kryptowalut znajdują się w orbicie zainteresowań cyberprzestępców i terrorystów, stanowiąc jednocześnie istotną konkurencję dla Bitcoina i Litecoina (LTC)[78]. Poniżej omówiono trzy najważniejsze ekosystemy kryptowalut: Monero, Zcash i Dash.

Monero (XMR) lokuje się na pierwszym miejscu wśród *private coins* przede wszystkim ze względów technicznych oraz stopnia rozpowszechnienia (większość sklepów w domenie specjalnej .onion – darkmarketów – akceptuje tę kryptowalutę podobnie jak bitcoina). Monero istnieje od 2014 r., podczas gdy pozostałe analizowane waluty – od 2016 r. Kapitalizacja rynkowa na sierpień 2020 r. wyniosła ponad 1,5 mld dolarów amerykańskich (1 653 750 000), co daje najwyższy poziom kapitalizacji pośród *private coins*. Wolumen obrotu przekracza 83 mln dolarów, a kurs oscyluje tuż poniżej 100 dolarów[79]. Warto odnotować trzy udokumentowane przypadki wykorzystania kryptowaluty monero w działalności cyberprzestępczej. Pierwszym z nich jest darkmarket AlphaBay (pwoah7foa6au2pul.onion) należący do nieżyjącego już Alexandre'a Cazesa, działający od września 2014 r. do lipca 2017 r., który wdrożył transakcje z użyciem monero w lipcu 2016 r. Federalne Biuro Śledcze przejęło z serwera sklepu 11 993 monero[80] o wartości ok. 0,5 mln dolarów, jednak nie było możliwości całościowego oszacowania kwoty transakcji. Drugim przykładem jest hakerska grupa Shadow Brokers[81], która w czerwcu 2017 r. ogłosiła, że akceptuje płatności w monero obok dotychczas używanej kryptowaluty zcash (notabene: instrukcja odnosząca się do sposobu płatności zawierała błąd, który mógł ujawnić nabywców, a z płatności w monero szybko zrezygnowano)[82]. Trzeci przypadek to operatorzy *ransomware*[83] WannaCry,

---

[77] Według raportu Recorded Future w 2018 r. na wschodnioeuropejskich giełdach obok bitcoina dominował litecoin (35% wolumenu transakcji w porównaniu z bitcoinem), dash (24%) oraz bitcoin cash (BCH) (15%). Obecne były również ethereum (ETH) i zcash (ZEC), monero (XMR) zaś stanowiło zaledwie 3% transakcji. Z kolei w anglojęzycznych darkmarketach dominował bitcoin, a z użyciem monero dokonywano zaledwie 11% transakcji. Zob. A. Barysevich, A. Sola, *Litecoin Emerges as the Next Dominant Dark Web Currency*, Recorded Future, 8 II 2018 r., https://go.recordedfuture.com/hubfs/reports/cta-2018-0208.pdf, s. 5 [dostęp: 1 VIII 2020].

[78] T. Keatinge, D. Carlisle, F. Keen, *Virtual currencies and terrorist financing*…

[79] Por. *Monero (XMR)*, CoinGecko, https://www.coingecko.com/pl/waluty/monero [dostęp: 1 VIII 2020].

[80] Warto zwrócić uwagę na dwa istotne fakty. Po pierwsze, oprócz monero używano w sklepie bitcoinów, etherów oraz zcashów, a wszystkie z nich przejęto z serwerów AlphaBay. Po drugie, z prywatnych portfeli Cazesa FBI przejęła wszystkie kryptowaluty z wyjątkiem monero. Szerzej na ten temat: *United States of America vs. Alexandre Cazes. Verified complaint for forfeiture In Rem*, 2017 r., https://www.justice.gov/opa/press-release/file/982821/download [dostęp: 1 VIII 2020].

[81] Grupa ujawniała zarówno tajemnice Agencji Bezpieczeństwa Narodowego USA, jak i narzędzia informatyczne służące tej agencji do naruszania prywatności użytkowników komputerów i telefonów.

[82] J. Cox, *Cryptocurrency Transactions May Uncover Sales of Shadow Broker Hacking Tools*, „Vice", 28 VI 2018 r., https://www.vice.com/en_us/article/j5k7zp/zcash-shadow-brokers-uncover-hacking-tool-sales [dostęp: 1 VIII 2020].

[83] *Ransomware* (nazwa jest zbitką angielskich słów: *ransom* – okup i *software* – oprogramowanie) – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt

którzy usiłowali nieudolnie zalegalizować środki z działalności cyberprzestępczej, wymieniając bitcoiny na monero za pośrednictwem szwajcarskiej usługi giełdowej ShapeShift. Organizacja ta rozpoczęła współpracę z organami ścigania USA i w ten sposób udało się uwierzytelnić zaledwie kilkadziesiąt tysięcy dolarów[84]. Monero jest w pełni anonimową kryptowalutą, wykorzystującą następujące funkcjonalne instancje bezpieczeństwa: RingCT zabezpieczające samą transakcję, podpis pierścieniowy (*ring signature*) chroniący nadawcę, ukryty jednorazowy adres odbiorcy (*stealth address*) oraz mechanizm ukrywający adres IP nadawcy (Dandelion++). RingCT (*confidential transaction*) ukrywa kwotę transakcji, tj. umożliwia nadawcy udowodnienie posiadania wystarczającej kwoty bez ujawniania na zewnątrz informacji o wolumenie transakcji. W przypadku większości kryptowalut kwoty transakcji są przesyłane w postaci zwykłego tekstu, widocznego dla każdego obserwatora. Z kolei sygnatura pierścieniowa jest raczej mechanizmem zaciemniania niż całkowitej anonimizacji nadawcy środków. Polega na grupowym dokonywaniu transakcji – łączone są klucze z wielu wyjść i wpisywane do blockchaina, aby utrudnić rozpoznanie prawdziwego nadawcy środków. Natomiast *stealth address* (*one-time address*, *burn-after-reading*) chroni odbiorcę przez utworzenie losowego adresu jednorazowego, tak aby różne płatności dokonane na rzecz tego samego odbiorcy stały się niemożliwe do połączenia. Mechanizm Dandelion++ jest mechanizmem anonimizacji stosunkowo nowym dla systemu Monero, lecz znanym od dawna (pierwotnie zaprojektowany dla systemu Bitcoin, którego społeczność odmówiła przyjęcia tego rozwiązania)[85]. Do Monero wdrożył go w lipcu 2020 r. deweloper Lee Clagett. W uproszczeniu polega on na skierowaniu transakcji do odległego węzła, aby ukryć adres IP nadawcy, co uniemożliwia deanonimizację nawet w sytuacji ataków na dużą skalę[86]. W przyszłości jest planowane wdrożenie mechanizmu Triptych multiplikującego liczebność sygnatur pierścieniowych, co istotnie zwiększy anonimowość transakcji. Warto podkreślić, że w określonych warunkach deanonimizacja użytkowników systemu Monero jest możliwa[87]. Ograniczone, zgodnie w powyższymi

---

zapisanych w nim danych (często wykorzystując techniki szyfrujące), a następnie żąda okupu od ofiary za przywrócenie stanu pierwotnego. Za: Wikipedia [dostęp: 18 I 2021 r.] – przyp. red.

[84] T. Fox-Brewster, *Wannacry hackers are using this Swiss company to launder $142,000 Bitcoin ransoms*, „Forbes", lipiec 2017 r., https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacryhackers-use-shapeshift-to-launder-bitcoin [dostęp: 1 VIII 2020].

[85] S.B. Venkatakrishan, G. Fanti, P. Viswanath, *Dandelion: Redesigning the Bitcoin Network for Anonymity*, Sigmetrics'17, 5–9 VI 2017 r., Urbana-Champaign, http://publish.illinois.edu/science-of-security-lablet/files/2016/07/Dandelion-Redesigning-BitCoin-Networking-for-Anonymity.pdf [dostęp: 1 VIII 2020]; G. Fanti i in., *Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonimity Guarantees*, „Proceedings of the ACM on Measurement and Analysis of Computing Systems" 2018, nr 2, https://arxiv.org/pdf/1805.11060.pdf [dostęp: 1 VIII 2020].

[86] L. Clagett, *Dandelion Onions: Protecting Transaction Privacy in Monero*, Monero Konferenco, 22–23 VI 2019 r., https://www.monerooutreach.org/monero-konferenco/lee-clagett.html [dostęp: 1 VIII 2020].

[87] M. Möser i in., *An Empirical Analysis of Traceability in the Monero Blockchain*, „Proceedings on Privacy Enhancing Technologies" 2018, nr 3, s. 143–163, https://arxiv.org/pdf/1704.04299/

rozważaniami, informacje na temat transakcji dokonanych w kryptowalucie monero są dostępne w eksploratorach: monerovision.com, moneroblocks.info, xmr.tokenview.com, blockchair.com.

Zcash (ZEC) powstał w 2016 r. (wcześniej był znany jako Zerocoin). Obecnie jego kapitalizacja rynkowa wyniosła ponad 928 mln dolarów, w obiegu znalazło się blisko 10 mln monet, a aktualny kurs to ok. 100 dolarów amerykańskich. Zcash jest obecny na globalnych giełdach, jak BKEX, Binance, YoBit i OKEx. Nie jest to kryptowaluta używana do dużych transakcji (wymiana powyżej 100 tys. dolarów amerykańskich stanowi mniej niż 7 proc. wszystkich transakcji[88]). System Zcash zapewnia opcjonalną anonimowość, a wszystkie transakcje są odnotowywane w blockchainie; sam jego kod jest *open source*. Analizy transakcji w systemie Zcash dokonuje się z użyciem eksploratorów: explorer.zcha.in, zecblockexplorer.com, zcash.tokenview.com, blockchair.com. Anonimowość ZCash ma charakter opcjonalny i jest realizowana przez wdrożenie dwóch typów adresów: prywatnych (*shielded, z-addr*) – rozpoczynających się literą „z" oraz transparentnych (*transparent, t-addr*) – rozpoczynających się literą „t". Te dwa typy adresów współdziałają ze sobą, co oznacza, że przepływ środków między nimi jest możliwy. W praktyce mniejszość transakcji jest anonimowa – analitycy wskazują, że forma *private* jest wybierana w ok. 6 proc. wszystkich transakcji, a w praktyce niemożliwe do wyśledzenia jest 0,9 proc. z nich[89]. Możliwość wyboru między transakcjami prywatnymi i transparentnymi ma znaczenie nie tylko techniczne i praktyczne, lecz także polityczne – istnieje bowiem mniejsze ryzyko objęcia kryptowaluty negatywnymi regulacjami prawnymi. Anonimowość jest zapewniana przez nowy algorytm zk-SNARK (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*). Jest to konstrukcja dowodowa umożliwiająca udowodnienie posiadania pewnych informacji lub zasobów (w tym przypadku środków zcash i pseudonimowej tożsamości), bez bezpośredniego ujawniania tych informacji. Jest to tzw. dowód wiedzy zerowej (*zero-knowledge proof*), pozwalający potwierdzającemu udowodnić drugiej stronie (weryfikującemu), że informacje są prawdziwe, bez ujawniania jakichkolwiek danych wykraczających poza ważność samego oświadczenia. Należy podkreślić, że bezpieczeństwo systemu Zcash jest hipotetyczne, jest to bowiem nowa forma kryptografii, której podatności są jeszcze nieznane. Na technicznych założeniach kryptowaluty zcash oparto kryptowalutę komodo (KMD) – dziedziczy ona wiele funkcji bezpieczeństwa pierwowzoru[90].

[dostęp: 1 VIII 2020]. Warto odnotować inicjatywę United States Internal Revenue Services, który zaoferował nagrodę w wysokości 650 tys. dolarów za pomoc w złamaniu anonimowości Monero, https://beta.sam.gov/opp/3b7875d5236b47f6a77f64c19251af60/ [dostęp: 29 I 2021].

88 Por. *ZCash (ZEC)*, CoinGecko, https://www.coingecko.com/pl/waluty/zcash [dostęp: 1 VIII 2020].

89 Claire Ye i in., *Alt-Coin Traceability*, International Association for Cryptologic Research, 18 V 2020 r., https://eprint.iacr.org/2020/593.pdf, s. 16–21 [dostęp: 1 VIII 2020].

90 *Advanced Blockchain Technology, Focused on Freedom*, Komodo, https://komodoplatform.com/wp-content/uploads/2018/06/Komodo-Whitepaper-June-3.pdf [dostęp: 1 VIII 2020].

Dash (DASH) wprowadzono na rynek w 2014 r. z wykorzystaniem jako podstawy protokołu systemu Bitcoin. Pierwotnie był znany jako XCoin, następnie jako Darkcoin, a po zaakceptowanym przez społeczność rebrandingu jako Dash (co jest skrótowcem utworzonym od *digital cash*). Kapitalizacja wynosi 937 mln dolarów, a w obrocie jest obecnie nieco ponad 9640 tys. monet dash. Dash jest otwartoźródłowy, nieinflacyjny (może powstać nie więcej niż 19 mln dashów) oraz częściowo zdecentralizowany. Instancją umiarkowanie centralizującą są tzw. węzły zarządzające (*masternodes*), a ich sieć tworzy zdecentralizowaną autonomiczną organizację (DAO). Służą one utrzymywaniu funkcjonowania sieci: potwierdzaniu i przesyłaniu transakcji, zapewnianiu anonimowości części z nich (na żądanie), a właściciele tych węzłów mają prawo głosu w sprawach istotnych dla społeczności Dash. Taka struktura zakłada częściowe zaufanie do podmiotów pośredniczących w transakcjach, czyli właścicieli *masternodes*. Dash oferuje dwa typy transakcji o różnym przeznaczeniu: natychmiastowe (InstantSend) i prywatne (PrivateSend). Oba typy transakcji są realizowane przez węzły zarządzające. Transakcje prywatne wykorzystują zmodyfikowaną i ulepszoną wersję protokołu CoinJoin, pierwotnie przeznaczoną do częściowej anonimizacji kryptowaluty bitcoin[91]. Istotą tej metody jest miksowanie polegające na rozmienianiu monet służących do transakcji na mniejsze nominały i wymieszaniu ich z monetami innych użytkowników przed dokonaniem transakcji. Każda runda jest miksowana na innym węźle. W rezultacie oryginalny adres, z którego transakcja została zainicjowana, jest trudny lub niemożliwy do wyśledzenia (mechanizm nieopłacalności nakładów). Maksymalna liczba dashów przesłana z użyciem transakcji prywatnej wynosi 1 tys.[92]

Anonimizacyjne parametry techniczne spowodowały, że od 2019 r. z monero, zcash i dash rezygnują liderzy giełd kryptowalut: Coinbase, OKEx, UpBit, BitBay – argumentując za wytycznymi The Financial Action Task Force (dalej: FATF), że te środki pieniężne mogłyby być wykorzystywane do działań nielegalnych[93].

Bezpieczne przechowywanie informacji

Technologie chroniące prywatność są stosowane nie tylko w komunikacji (tzw. *data-in-motion*, czyli dane w ruchu), lecz także w przechowywaniu informacji (tzw. *data-in-rest*, czyli dane w spoczynku)[94] znajdujących się w bazach danych, systemach plików i magazynowanych za pomocą innych metod (np. systemów pamięci masowej online). W celu zabezpieczenia tego typu danych korzysta się z mechanizmów kryptografii, co przy wystarczającej wprawie i znajomości tych narzędzi może chronić przed każdym,

---

[91] E. Duffield, D. Diaz, *Dash: A Privacy-Centric Crypto-Currency*, https://www.zioncoins.co.uk/wp-content/uploads/2015/06/Dash-Whitepaper.pdf, s. 7–8 [dostęp: 1 VIII 2020].

[92] Zob. *Dash FAQ*, https://www.dash.org/pl/faq/ [dostęp: 1 VIII 2020].

[93] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paryż 2019 r., http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html [dostęp: 1 VIII 2020].

[94] Lyong S.L. Liu, R. Kuhn, *Data Loss Prevention*, „IT Professional" 2010, nr 2, s. 10–13.

w tym wysoce profesjonalnym, nieautoryzowanym dostępem. Współcześnie używane mechanizmy kryptograficzne są uznawane za względnie trudne do przełamania, dlatego też władze podejmują równolegle dwa typy działań, których celem jest techniczne oraz prawne umożliwienie pozyskania informacji zabezpieczonych kryptograficznie. W przypadku pierwszego typu działań opinia publiczna nie jest w pełni świadoma możliwości, jakimi dysponują władze[95]. Informatyczno-techniczne aspekty kryptoanalizy mogą być jednak ewaluowane przez pryzmat wdrażanych rozwiązań prawnych. W wielu krajach wprowadzono prawny obowiązek ujawniania kluczy kryptograficznych pod karą grzywny lub pozbawienia wolności[96] (tzw. *key disclosure laws*), w wielu innych forsuje się lub rozważa implementację takich rozwiązań. To zjawisko potrzebuje szerszego omówienia ze względu na jego rangę. Ochronę informacji w kontekście wspomnianego obowiązku zapewnia szyfrowanie danych stanowiących tzw. wiarygodne zaprzeczenie (*plausible deniability*), a wspierają je produkty ochrony prywatności oparte na kryptografii (VeraCrypt, a dawniej TrueCrypt, czy steganografia polegająca na ukrywaniu jednej informacji w innej, np. obrazu w pliku tekstowym). Poszczególne kraje starają się radzić sobie i z takimi rozwiązaniami – wprowadzają rozmaite uregulowania prawne, które w skrajnych przypadkach naruszają prawo do niedostarczania dowodów na swoją niekorzyść i prawo do milczenia (zasada prawna: *nemo se ipsum accusare tenetur*[97]), czy po prostu ujawniają prywatne dane osobowe. Tak twarde prawo obowiązuje np. we Francji, gdzie prokurator lub sędzia może zmusić każdą osobę do przekazania kluczy lub odszyfrowania danych w celu udostępnienia informacji potrzebnych do prowadzenia dochodzenia. Za nieprzestrzeganie tego prawa grożą trzy lata więzienia lub grzywna. Przewidziana kara wzrasta do pięciu lat i grzywny nawet w wysokości 75 tys. euro, jeśli przestrzeganie przepisów zapobiegłoby przestępstwu lub złagodziło jego skutki[98]. Na mniej rygorystyczne przepisy zdecydował się belgijski ustawodawca, który daje sędziemu możliwość nakazania – zarówno operatorom systemów komputerowych, jak i dostawcom usług telekomunikacyjnych – udzielenia pomocy organom ścigania, w tym polegającej na odszyfrowaniu danych, oraz zachowania swojej pomocy w tajemnicy. Takiego działania nie można jednak podjąć wobec podejrzanego lub jego rodziny. Za nieprzestrzeganie grozi kara od sześciu

---

[95] Typologia i skuteczność ataków są znane wyłącznie w publicznym, naukowym dyskursie. Nie wiadomo, w jakim stopniu kryptoanaliza służb dyspozycyjnych i organów ścigania różni się od tej znanej publicznie. Dostępna jest wiedza na przykład o możliwościach i ograniczeniach ataków typu: *brute force*, *meet in the middle*, statystyczne, przez analizę różnicową, urodzinowe, zimnego rozruchu, algebraiczne i inne. Zob. np.: Ch. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking,* New Jersey 2008, rozdz. 5.

[96] Dotyczy to obywateli (np. Australia), dostawców usług informatycznych (np. Belgia) oraz innych osób – m.in. ekspertów (np. Holandia).

[97] Z łac. nikt nie jest zobowiązany do oskarżania siebie (przyp. red.).

[98] *Loi relative à la sécurité quotidienne* (ustawa o powszechnym bezpieczeństwie), nr 2001–1062, 15 XI 2001 r., http://www.ejustice.just.fgov.be/eli/loi/2000/11/28/2001009048/justel [dostęp: 26 VIII 2020].

miesięcy do roku więzienia lub grzywna w wysokości od 130 do 100 tys. euro[99]. Natomiast Polska jest jednym z krajów, w których nie ma podobnych regulacji w tej kwestii. *Kodeks postępowania karnego*[100] (dalej: kpk) w art. 74 § 1 stanowi, że oskarżony nie ma obowiązku dowodzenia swojej niewinności ani obowiązku dostarczania dowodów na swoją niekorzyść. Ponadto art. 182 kpk statuuje prawo odmowy zeznań: § *1. Osoba najbliższa dla oskarżonego może odmówić zeznań; § 2. Prawo odmowy zeznań trwa mimo ustania małżeństwa lub przysposobienia; § 3. Prawo odmowy zeznań przysługuje także świadkowi, który w innej toczącej się sprawie jest oskarżony o współudział w przestępstwie objętym postępowaniem*. Porównywalne gwarancje, znane polskiemu prawu, zawiera art. 14 ust. 3 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych* oraz art. 6 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*.

Wskazane uregulowania prawne stały się silnym impulsem do opracowania i wdrożenia mechanizmów samoobrony przed sankcjonowanym wymogiem ujawnienia kluczy kryptograficznych. Określa się je powszechnie mianem wiarygodnego zaprzeczenia. Wiarygodne zaprzeczenie jest to pewna informatyczna właściwość programu kryptograficznego umożliwiająca odszyfrowanie zaszyfrowanej informacji do dwóch różnych, wiarygodnie wyglądających tekstów w zależności od dostarczonego klucza kryptograficznego. To oznacza, że jeśli do dekryptażu zastosuje się klucz kryptograficzny A, to otrzyma się informację B, a przy użyciu klucza B po odszyfrowaniu odczyta się informację C. Nie ma przy tym możliwości stwierdzenia, czy zaszyfrowany obszar mieści jedną czy dwie informacje[101]. Frazy „wiarygodna zaprzeczalność" jako pierwszy użył w literaturze przedmiotu Michael Roe w swojej dysertacji[102], a omawiana koncepcja szybko doczekała się rozszerzenia i dookreślenia[103]. Jej istotę doskonale oddaje następujące zdanie: *Przedstawienie wiarygodnego dowodu jest nieodmiennie bardziej wiarygodne niż oświadczenie 'wymazałem' lub 'zapomniałem'*[104]. Pierwsze praktyczne wdrożenie mechanizmu wiarygodnej zaprzeczalności odbyło się w 1999 r., gdy przedstawiono prototyp zaprzeczalnego systemu plików o nazwie StegFS[105]. W 2004 r. powstał program TrueCrypt (wersja 1.0), który stał się niekwestionowanym

---

[99] *Loi du 28 novembre 2000 relative à la criminalité informatique* (ustawa o przestępstwach komputerowych), nr 2001009035, 28 XI 2000 r., https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2000112834&table_name=loi [dostęp: 26 VIII 2020].

[100] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: DzU z 2021 r. poz. 534).

[101] M. Kędziora, Yang-Wai Chow, W. Susilo, *Threat Models for Analyzing Plausible Deniability of Deniable File Systems*, „Journal of Software Networking" 2017, nr 1, s. 241–242.

[102] M. Roe i in., *Cryptography and Evidence*, Cambridge 1997 r., University of Cambridge, https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-780.pdf, s. 11 [dostęp: 26 VIII 2020].

[103] R. Canetti i in., *Deniable Encryption*, w: *Advances in Cryptology – CRYPTO'97*, B.S. Kaliski (red. nauk.), Berlin 1997, s. 90–104.

[104] Tamże, s. 91.

[105] M. Smith, *Mission Implausible: Defeating Plausible Deniability with Digital Forensics*, SANS Institute, 2 IV 2020 r., https://www.sans.org/reading-room/whitepapers/forensics/mission-implausible-defeating-plausible-deniability-digital-forensics-39500 [dostęp: 1 VIII 2020].

liderem programów oferujących wiarygodną zaprzeczalność. W 2014 r. organizacja The TrueCrypt Foundation zarzuciła projekt w jak dotąd niewyjaśnionych okolicznościach – oświadczenie jego twórców jest niezgodne z wynikami późniejszych audytów. Program został wycofany z oficjalnej strony oraz repozytoriów, a wspomniane oświadczenie nigdy nie było wyjaśniane, komentowane ani rozszerzane przez autorów aplikacji[106].

Następcą TrueCrypt stał się VeraCrypt – aktualnie najbardziej uniwersalny program służący do szyfrowania danych. Powstał on w 2013 r. za sprawą francuskiej firmy IDRIX. Wywodzi się (jest tzw. *forkiem*) od TrueCrypt[107]. VeraCrypt bywa wymieniany w materiałach szkoleniowych dla islamskich terrorystów[108]. Pojawiają się doniesienia, że próby pozyskania dowodów z nośników zaszyfrowanych VeraCrypt podejmowane przez służby specjalne kończą się porażką[109]. Dostarczono też wielu przykładów skutecznego stawienia oporu organom ścigania przez użytkowników[110]. VeraCrypt jest programem uniwersalnym w sensie wieloplatformowości – jest dostępny dla systemów Windows, MacOS, Linux, FreeBSD. Kodów źródłowych można użyć również samodzielnie do własnej kompilacji na różne platformy sprzętowe lub systemy. Jest popularny w społeczności informatycznej, ze względu zarówno na jakość, jak i brak alternatyw szerzej rozpowszechnionych i co najmniej równie funkcjonalnych (ograniczoną popularność oraz funkcjonalność mają np. dm-crypt, TCNext, LUKS, LiberCrypt). Warto dodać, że obsługuje on zbiory zaszyfrowane z użyciem programu TrueCrypt oraz że naprawiono w nim znane podatności. VeraCrypt jest odporny m.in. na „atak złej pokojówki" (*evil maid attack*), polegający na fizycznym przejęciu zaszyfrowanego nośnika, częściowo jest uodporniony również na tzw. atak zimnego rozruchu. Program VeraCrypt jest uznawany za względnie bezpieczny, a spośród aktualnie istniejącego oprogramowania –

---

[106] A. Junestam, N. Guigo, *Open Crypto Audit Project TrueCrypt Security Assessment,* iSec Partners, 2014 r., https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [dostęp: 1 VIII 2020]; A. Balducci, S. Devlin, T. Ritter, *TrueCrypt. Cryptographic Review*, Open Crypto Audit Project, NCC Group, 2015 r., https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf, s. 1–21 [dostęp: 1 VIII 2020].

[107] A. Haertle, *Audyt Truecrypta zakończony, dwa istotne błędy w jego implementacji*, Zaufana Trzecia Strona, 2 IV 2015 r., https://zaufanatrzeciastrona.pl/post/audyt-truecrypta-zakonczony-znaleziono-dwa-istotne-bledy-w-implementacji/ [dostęp: 1 VIII 2020].

[108] *Cyber-Terrorism Activities Report No. 18*, lipiec–wrzesień 2016 r., International Institute for Counter-Terrorism, https://www.ict.org.il/UserFiles/ICT-Cyber-Review-18.pdf, s. 24 [dostęp: 1 VIII 2020].

[109] A. Ścibor, *Służbom ze sojuszu Five Eyes nie udało się złamać szyfrowania VeraCrypt*, 29 V 2019 r., Fundacja AVLab dla Cyberbezpieczeństwa, https://avlab.pl/sluzbom-ze-sojuszu-five-eyes-nie-udalo-sie-zlamac-szyfrowania-veracrypt [dostęp: 1 VIII 2020].

[110] A. Balogun, Shao Ying Zhu, *Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology*, „International Journal of Advanced Computer Science and Applications" 2013, nr 5, s. 36–40; A. Czeskis i in., *Defeating encrypted and deniable file systems: TrueCrypt v5.1a and the case of the tattling OS and applications*, w: *Proceedings of 3rd USENIX Workshop on Hot Topics in Security*, 2008 r., https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf [dostęp: 1 VIII 2020].

za najbezpieczniejszy[111]. W 2015 r. VeraCrypt przeszedł kompleksowy audyt, który wypadł pomyślnie. Stwierdzono brak jakichkolwiek „tylnych drzwi" w jego kodzie[112]. Uczestniczy w programie Bug Bounty (2020 r.) gwarantującym nagrody pieniężne za odnajdywanie luk bezpieczeństwa w oprogramowaniu. Luk poszukują członkowie informatycznej społeczności, co znacznie usprawnia prace nad bezpieczeństwem programu[113]. VeraCrypt jest krytykowany głównie za algorytm doboru liczb losowych (mechanizm entropii jest oparty na /dev/random zamiast innych, bardziej losowych mechanizmach)[114]. Czasami podaje się w wątpliwość kwestię instytucjonalną tworzenia programu: oczywisty i udokumentowany związek przedsiębiorstwa rozwijającego VeraCrypt z francuskim rządem. Niektórzy użytkownicy zgłaszają również uwagi, że Windows 10 nie współpracuje z VeraCrypt, jeśli dojdzie do aktualizacji systemu operacyjnego znajdującego się na ukrytym nośniku. Warto jednak podkreślić, że VeraCrypt jest programem zaawansowanym kryptograficznie – implementuje liczne, dodatkowe zabezpieczenia w postaci PIM (*Personal Iterations Multiplier*), plików-kluczy oraz tokenów. Zaopatrzono go w klasyczne (*Advanced Encryption Standard, Serpent, Twofish, Camelia*), jak i najnowsze (*Kuznyechik*) algorytmy kryptograficzne i haszujące, o zróżnicowanej wydajności i poziomie gwarantowanego bezpieczeństwa. Co najistotniejsze, jest on nadzwyczaj prosty i przystępny w obsłudze (*stupid-proof*). Najważniejszą cechą programu VeraCrypt jest jego wielozadaniowość. Umożliwia on utworzenie zaszyfrowanego:

- **woluminu w zwykłym pliku**. Plik poza objętością i tym, że nie da się z niego skorzystać, jest nieodróżnialny od analogicznego pliku;
- **sekretnego woluminu w zaszyfrowanym woluminie umieszczonym w zwykłym pliku (matrioszka)**. Tworzenie tzw. matrioszek ma szczególne znaczenie dla zachowania prywatności. Powstają wówczas dwa zaszyfrowane obszary i są ustalane dwa różne hasła – każde z nich odszyfrowuje inny wolumin. Jest to praktyczna realizacja koncepcji wiarygodnej zaprzeczalności, a zatem nie ma możliwości stwierdzenia, czy zaszyfrowany obszar zawiera jeden, dwa czy więcej takich woluminów;

---

[111] Interesująca dyskusja wywiązała się na forum SourceForge w 2019 r. Ze względu na anegdotyczność tego przykładu zamieszczono go w przypisie. Otóż 24 maja opublikowano na forum post, drobiazgowo opisujący historię konfiskaty sprzętu elektronicznego, w tym dysków twardych zaszyfrowanych VeraCrypt w wersji 1.13, przez służby dyspozycyjne jednego z państw. Po upływie dwóch i pół roku urządzenia zwrócono właścicielowi, który nie poniósł żadnych konsekwencji. Ponadto autor wiadomości uwiarygodnił się, wpłacając w ramach podziękowania równowartość 10 tys. dolarów w bitcoinach na rozwój VeraCrypt, a ten fakt odnotowano w łańcuchu blockchain BTC. Zob. https://sourceforge.net/p/veracrypt/discussion/general/thread/720575f74e/ [dostęp: 1 VIII 2020].

[112] Pełny raport z audytu: A. Balducci, S. Devlin, T. Ritter, *TrueCrypt*…

[113] *Public Bug Bounty List,* Bugcrowd, 2020 r., https://www.bugcrowd.com/bug-bounty-list/ [dostęp: 1 VIII 2020].

[114] Por. dyskusja: Hacker News, https://news.ycombinator.com/item?id=21185594 [dostęp: 1 VIII 2020].

- **całego nośnika pamięci** (np. nośnika USB) **lub ukrytej partycji niesystemowej** (jednej lub wielu);
- **ukrytej partycji systemowej**. Jest ona tworzona na takiej zasadzie jak w matrioszkach. W istocie powstają dwa systemy operacyjne – zaszyfrowany, ale przeznaczony do ujawnienia, oraz zaszyfrowany i mający pozostać tajnym systemem operacyjnym. Jest to również praktyczne wdrożenie mechanizmu wiarygodnego zaprzeczenia.

Podsumowanie – modelowe atrybuty technologii wspierających prywatność

George Danezis, konstruując model zagrożeń technologii wspierających prywatność, celnie wskazał ich główne źródła. Są to: koszt (*cost*), zmowa (*collusion*), przymus (*compulsion*), korupcja (*corruption*) i nieostrożność (*carelessness*)[115]. Tą koncepcją, jako szczególnie wartościową heurystycznie, posłużono się do usystematyzowania wniosków, podając wyczerpujący zestaw modelowych cech technologii wspierających prywatność.

Warunkiem umasowienia rozwiązania chroniącego prywatność jest jego niski **koszt**. Narzędzie jest tym szerzej używane, im niższy jest próg kompetencyjny jego skutecznego zastosowania – kwalifikacje wymagane od użytkownika są niewielkie, a względnie krótkie przeszkolenie wystarcza, aby mógł on wykorzystać potencjał produktu. Czynnikiem zmniejszającym koszt jest ponadto dobrze opracowana dokumentacja, a także społeczność wspierająca produkt informatyczny i jego użytkowników. Zadaniem takiej społeczności jest świadczenie wzajemnej, zbiorowej pomocy, a także wykrywanie, zgłaszanie i trwałe usuwanie usterek w funkcjonowaniu narzędzia. Analizowane programy, systemy i usługi mają wszystkie wskazane cechy. Wspomniany koszt może być również rozumiany dosłownie – jako nieodpłatna dostępność narzędzi. Tak jest w przypadku wyżej opisanych rozwiązań. Wniesienie za nie opłat ma charakter dobrowolny i nie jest wymagane, aby program, system lub usługę użytkować. Na koszt można spojrzeć także z perspektywy barier chroniących przed naruszeniem bezpieczeństwa oferowanego przez dane narzędzie wspierające prywatność. A zatem im nakłady techniczne, finansowe i organizacyjne muszą być większe, aby te bariery przełamać, tym bardziej dane narzędzie można uznać za bezpieczne. Zasada działania technologii wspierających prywatność opiera się na takim właśnie rozwiązaniu – bariery prywatności nie są całkowite ani niemożliwe do przełamania, ale ich naruszanie jest nieopłacalne (na ogół masowe, ale czasem nawet jednostkowe i jednorazowe). Nieopłacalność naruszenia anonimowości użytkowników jest wzmacniana przez mechanizmy: podobieństwa użytkowników oraz masowości. Jeśli system lub usługa każdego

[115] G. Danezis, *A Gentle Introduction to Privacy Enhancing Technologies & 2 Case Studies*, Interdisciplinary Summerschool on Privacy, 11 VII 2016 r., https://isp.cs.ru.nl/2016/danezis.pdf [dostęp: 1 VIII 2020].

z użytkowników dla zewnętrznego obserwatora wygląda tak samo (w mechanizmie zbierania elektronicznych odcisków palców), to trudne, a nawet niemożliwie jest śledzenie poszczególnych użytkowników. W przypadku takich rozwiązań, jak VeraCrypt mechanizm maksymalizacji kosztów dla przełamującego zabezpieczenia opiera się na zasadach matematycznych – zgodnie z nimi przełamanie mechanizmów kryptograficznych w akceptowalnym czasie jest niemożliwe.

Edward Snowden, doprowadzając do największego w historii Stanów Zjednoczonych wycieku tajnych informacji, unaocznił opinii publicznej rolę, jaką odgrywa mechanizm **zmowy**, w tym konkretnym przypadku tajnego (i wymuszonego) porozumienia Agencji Bezpieczeństwa Narodowego i głównych przedsiębiorstw będących dostawcami usług, systemów i urządzeń informatycznych. Uniknięcie takiej intrygi jest możliwe przez instytucjonalne rozwiązanie przyjętego modelu biznesowego, polegające na transparentności wytwarzania, a następnie zarządzania produktem lub usługą. Środkiem najłatwiejszym do wdrożenia jest udostępnienie kodu źródłowego oraz bieżący monitoring tego kodu przez oddolnie tworzoną, opartą na samorekrutacji, zdecentralizowaną społeczność. Najważniejsze znaczenie ma tu decentralizacja, a więc brak instancji zarządzających narzędziem i brak własności intelektualnej dotyczącej tego narzędzia. Jeśli całkowite spłaszczenie struktur nie jest możliwe (sieć Tor), wówczas zadowalającym rozwiązaniem jest federalizacja. Ten typ struktury zakłada wielość, na ogół równorzędnych, ośrodków zarządczych, w związku z czym kontrolowanie ich wszystkich lub ich wystarczającej liczby jest nieopłacalne. W takiej sytuacji zmowa nie jest możliwa, a taki model (decentralizacji – Freenet, federalizacji – Tor) jest dominujący w krajobrazie PET.

Analogiczny schemat może być realizowany w celu zapobiegania mechanizmom **korupcji**. Są one również przezwyciężane przez uczynienie właścicielem produktu lub usługi całej społeczności oraz – na etapie jej funkcjonowania – przez częściową lub całkowitą jej decentralizację, a więc eliminację instytucji zaufanej trzeciej strony. Taka strategia antykorupcyjna jest w oczywisty sposób skuteczna. Rozwiązanie wykorzystane w sieci Tor zakłada liczebną i rozproszoną „zaufaną trzecią stronę" w postaci licznych i zmiennych węzłów. W przypadku sieci Freenet taki mechanizm nie występuje, sieć tworzą bowiem sami użytkownicy. Podobne zasady są stosowane w społecznościach blockchainowych, będących zbiorowymi właścicielami i zarządcami określonej kryptowaluty (np. węzły zarządzające w Dash). Z kolei twórcy takich systemów, jak Linux Tails czy Whonix zapobiegają mechanizmom korupcji inferencyjnie – przez ujawnienie kodu źródłowego i animowanie społeczności mogącej dokonywać audytu, a także pozostają otwarci na współpracę z programistami, którzy chcą uczestniczyć w projekcie.

Twórcy narzędzi wspierających prywatność coraz częściej biorą pod uwagę problem **przymusu**, rozumianego jako uregulowania prawne utrudniające lub uniemożliwiające korzystanie z tych narzędzi do celów przestępczych lub innych. Z reguły te rozstrzygnięcia przyjmują formę norm prawnych, które narzucają określonej stronie (użytkownikowi, dostawcy usług lub wytwórcy oprogramowania) ściśle określone wymogi (i w jakimś stopniu penalizujące używanie tych narzędzi). W odpowiedzi na to

wdrożono wiele innowacji informatycznych (w przypadku sieci Tor stosuje się mechanizm „zaciemniający" – obfs4, a dla VeraCrypt – mechanizm wiarygodnego zaprzeczenia). Rozwiązaniem uzupełniającym, które służy do zminimalizowania przymusu prawnego, jest stosowanie przemyślanych, systemowych wybiegów paraprawnych[116].

Przezwyciężanie mechanizmów zmowy, korupcji oraz przymusu jest wzmacniane przez postawy ideologiczno-polityczne środowiska tworzącego i wykorzystującego technologie wspierające prywatność. Jak wskazano, są one nastawione co najmniej krytycznie, jeśli nie negatywnie, do instytucji państwa, z reguły traktują je jako główne zagrożenie prywatności. Ich sympatie oscylują wokół szeroko pojętego anarchizmu czy libertarianizmu.

W technologiach wspierających prywatność najważniejszą rolę odgrywa **nieostrożność**. Brak luk bezpieczeństwa lub znane mechanizmy pozbawiające anonimowości sprawiają, że często jedyną możliwością deanonimizacji użytkownika przez służby dyspozycyjne jest błąd przez niego popełniony. Można przytoczyć wiele przykładów zaniedbania bezpieczeństwa operacyjnego przez użytkowników, co doprowadziło do aresztowań. Błędy wynikające z niewiedzy lub nieostrożności użytkowników technologii wspierających prywatność przyczyniły sie do licznych sukcesów służb dyspozycyjnych[117].

Model technologii wspierających prywatność obejmuje przemyślaną mozaikę rozwiązań informatycznych, których podstawą są kryptografia oraz rozwiązania prawne.

---

[116] *Warrant canary* to potoczne określenie odnoszące się do regularnie upublicznianego (dowolną drogą) oświadczenia, zgodnie z którym usługodawca nie otrzymał nakazu służb dyspozycyjnych dotyczącego współpracy ze służbami lub uzyskania przez nie dostępu do nośników informacji usługodawcy. Zgodnie z rozstrzygnięciami prawnymi w niektórych krajach (np. w USA) ujawnienie współpracy jest penalizowane. Działanie, które nie narusza istniejącego prawa, a jednocześnie ostrzega usługobiorców, polega na nieaktualizowaniu oświadczenia lub usunięciu go, a więc opiera się na zasadzie logicznego mechanizmu kontrapozycji. W latach 2016–2019 istniała organizacja Canary Watch (https://canarywatch.org/), koncentrująca wysiłki na zbadaniu cech *warrant canary* oraz informowaniu społeczności o inicjatywach poszczególnych usługodawców w tym zakresie. Więcej na ten temat: K. Opsahl, *Warrant Canary Frequently Asked Questions*, Electronic Frontier Foundation, 10 IV 2014 r., https://www.eff.org/deeplinks/2014/04/warrant-canary-faq [dostęp: 1 VIII 2020]. W kontekście zagrożeń bezpieczeństwa narodowego zob. R. Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, „The Yale Law Journal" 2014, nr 158, http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design, strony nienumerowane [dostęp: 1 VIII 2020].

[117] Długą listę otwierają twórcy sklepów ze środkami psychoaktywnymi w sieci Tor, począwszy od Rossa Ulbrichta (znanego jako Dread Pirate Roberts), przez twórcę Alpha Bay Alexandre'a Cazesa, właściciela Sheep Marketplace Tomáša Jiříkovský'ego, a na administratorach Dream Market skończywszy. Analogiczną nieświadomością i lekkomyślnością w stosowaniu zasad bezpieczeństwa operacyjnego wykazali się Eric Eoin Marques, twórca i administrator największego hostingu w sieci Tor – Freedom Hosting, oraz liczni użytkownicy oferowanej przez niego usługi. Warto zasygnalizować również niedawny przypadek Bustera Hernandeza – tu również przyczyną zatrzymania była lekkomyślność cyberprzestępcy. Zob. *United States of America v. Buster Hernandez*, United States District Court, https://casetext.com/pdf-email?slug=united-states-v-hernandez-1195, s. 1–28 [dostęp: 1 VIII 2020].

Ponadto do cech konstytutywnych należy zdecentralizowany lub co najmniej sfederalizowany (rozproszony, wieloośrodkowy) model narzędzia. Najważniejszym warunkiem powodzenia tych technologii jest łatwość instalacji i obsługi, wsparta czytelnymi mechanizmami stosowania zabezpieczeń zapobiegających sprzeniewierzeniu się zasadom bezpieczeństwa operacyjnego. Własność intelektualna winna spoczywać w rękach społeczności, a kod źródłowy oprogramowania powinien być wolny. Cechy dodatkowe to masowość użytkowania oraz podobieństwo użytkowników dla obserwatora zewnętrznego.

Technologie wspierające prywatność intensywnie rozwijają się w trzech głównych obszarach funkcjonowania Internetu: komunikacji, przechowywania danych oraz wymiany handlowej. Z technicznego punktu widzenia omawiane technologie wykorzystują dwa rozwiązania – szyfrowanie oraz anonimizację lub pseudonimizację. Dodatkowe narzędzie stanowi prawo, które jest wykorzystywane instrumentalnie w celu wzmocnienia ochrony informatycznej (popatrz: *warrant canary*). Należy podkreślić, że kilkadziesiąt lat lobbingu legislacyjnego na rzecz ochrony prywatności nie powstrzymało erozji wartości prywatności (przynajmniej w oczach niektórych obserwatorów), a technologie wspierające prywatność pojawiły się jako odpowiedź na braki legislacyjne[118].

Technologie wspierające prywatność to narzędzia podwójnego zastosowania. Mogą posłużyć i są faktycznie wykorzystywane zarówno do oddolnej samoobrony jednostek przed działaniami ujawniającymi dane wrażliwe, jak i do działań cyberprzestępczych (zwłaszcza przestępczości o charakterze ekonomicznym, politycznym i obyczajowym). Pierwotne przeznaczenie technologii wspierających prywatność do ochrony jednostki w kontekście działań cyberprzestępczych oraz agresywnego marketingu jest niepodważalne i nie budzi wątpliwości ani etycznych, ani prawnych[119]. Mogą się one pojawić, jeśli spojrzy się na to zagadnienie z technicznego punktu widzenia: stopień zaawansowania i jakość rozwiązań wydają się nadmierne do ochrony dóbr zagrożonych w tym sensie, że można te dobra z powodzeniem chronić przy użyciu prostszych narzędzi i rozwiązań. Dualizm tych zastosowań jest nierozerwalny, a przez to dylemat penalizacji środków wspierających prywatność wydaje się nierozwiązywalny z użyciem działań legislacyjnych lub technicznych. Jako jedyne rozwiązanie problemu wskazuje się czasochłonną i kosztochłonną społeczną redefinicję pojęcia p r y w a t n o ś ć[120].

---

[118] P.E. Agre, M. Rotenberg, *Technology and Privacy: The New Landscape*, Cambridge 1997; C.J. Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca 1992; D. Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, New York–London 2003.

[119] R.V. Clarke, *Technology, criminology and crime science,* „Crime and Deviance in Cyberspace" 2004, nr 1, s. 441–450; A.S. Wilner, *Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation,* „International Journal: Canada's Journal of Global Policy Analysis" 2018, nr 2, s. 308–316.

[120] F. Stalder, *The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy*, „Sociological Research Online" 2002, nr 2, s. 25–39.

Bibliografia

Acar K.V., *Child abuse materials as digital goods: Why we should fear new commercial forms*, „Economics Discussion Papers" 2017, nr 15, bez paginacji.

Assange J. i in., *Cypherpunks. Freedom and the Future of the Internet*, New York–London 2012, OR Books.

Balogun A., Zhu Shao Ying, *Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology*, „International Journal of Advanced Computer Science and Applications" 2013, nr 5, s. 36–40.

Canetti R. i in., *Deniable Encryption*, w: *Advances in Cryptology – CRYPTO'97*, B.S. Kaliski (red. nauk.), Berlin 1997, Springer, s. 90–104.

Chaum D., *Security without Identification. Transaction Systems to Make Big Brother Obsolete*, „Communications of the ACM" 1985, nr 10, s. 1030–1044.

Clarke R.V., *Technology, criminology and crime science*, „Crime and Deviance in Cyberspace" 2004, nr 1, s. 441–450.

Clifford B., Powell H., *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram, Program on Extremism*, Washington 2019, The George Washington University.

Crypto Anarchy, Cyberstates, and Pirate Utopias, P. Ludlow (red.), Cambridge 2001, Bradford Books.

Denning D.E., Baugh W.E, *Encryption and evolving technologies: Tools of organized crime and terrorism, Working group on organized crime*, Washington 1997, National Strategy Information Center, s. 1–64.

Diffie W., Hellman M.E., *New Directions in Cryptography*, „IEEE Transactions on Information Theory" 1976, nr 6, s. 644–654.

Dion-Schwarz C., Manheim D., Johnson P.B., *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats*, Santa Monica 2019, RAND Corporation.

Dostov V., Shust P., *Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?*, „Journal of Financial Crime" 2014, nr 3, s. 249–263.

Eyal I., *Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities*, „Computer" 2017, nr 9, s. 38–49.

Fanti G. i in., *Dandelion ++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees*, „Proceedings of the ACM on Measurement and Analysis of Computing Systems" 2018, nr 2, https://arxiv.org/pdf/1805.11060.pdf [dostęp: 1 VIII 2020].

Hammill Ch., *Od kuszy do kryptografii, czyli psucie państwu szyków przy pomocy techniki*, tłum. J. Sierpiński, „Kultura i Historia" 2007, nr 11, http://www.kulturaihistoria.umcs.lublin.pl/archives/701 [dostęp: 20 XI 2018].

Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents, G.W. van Blarkom, J.J. Borking, J.G.E. Olk (red. nauk.), Haga 2003, PISA Consortium.

Harvey J., Branco-Illodo I., *Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in 'Privacy Coin' Whitepapers*, „Journal of Political Marketing" 2020, nr 1–2, s. 107–136.

Herian R., *The Politics of Blockchain*, „Law and Critique" 2018, nr 2, s. 129–131.

Heurix J. i in., *A taxonomy for privacy enhancing technologies*, „Computers & Security" 2015, t. 53, s. 1–17.

Hurlburt G., *Shining Light on the Dark Web*, „IEEE Computer" 2017, nr 4, s. 100–105.

Karlstrøm H., *Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin*, „Distinktion: Scandinavian Journal of Social Theory" 2014, nr 1, s. 23–36.

Kędziora M., Chow Yang-Wai, Susilo W., *Threat Models for Analyzing Plausible Deniability of Deniable File Systems*, „Journal of Software Networking" 2017, nr 1, s. 241–264.

Lewis J.A., Zheng D.E., Carter W.A, *The Effect of Encryption on Lawfull Access to Communications and Data, Rowman & Littlefield*, Lanham–Boulder–New York–London 2017, Rowman&Littlefield.

Liu Lyong S.L., Kuhn R., *Data Loss Prevention*, „IT Professional" 2010, nr 2, s. 10–13.

Malik N., *Terror in the Dark. How terrorists use encryption, the darknet, and cryptocurrencies*, Millbank 2018, The Henry Jackson Society.

Maurer B., Nelms T.C., Swartz L., *When Perhaps the Real Problem Is Money Itself! The Practical Materiality of Bitcoin*, „Social Semiotics" 2013, nr 2, s. 261–277.

Mider D., *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 154–190.

Möser M. i in., *An Empirical Analysis of Traceability in the Monero Blockchain*, „Proceedings on Privacy Enhancing Technologies" 2018, nr 3, s. 143–163, https://arxiv.org/pdf/1704.04299/ [dostęp: 1 VIII 2020].

Privacy-enhancing technologies. The path to anonimity, R. Hes, J.J. Borking (red. nauk.), Haga 2000, Registratiekamer.

Pryciak M., *Prawo do prywatności*, „Wrocławskie Studia Erazmiańskie" 2010, nr 4, s. 211–229.

Quayle E., Taylor M., *Paedophiles, Pornography and the Internet: Assessment Issues*, „British Journal of Social Work" 2002, nr 7, s. 863–875.

Shapiro A.L., *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York 1999, Perseus Books.

Stalder F., *The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy*, „Sociological Research Online" 2002, nr 2, s. 25–39.

Swenson Ch., *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, rozdz. 5, New Jersey 2008, John Wiley&Sons.

United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes*, New York 2012.

Van Hout M.C., Bingham T., *Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences*, „International Journal of Drug Policy" 2013, nr 5, s. 385–391.

Wang Yang, Kobsa A., *Privacy-Enhancing Technologies*, w: *Handbook of Research on Social and Organizational Liabilities in Information Security*, M. Gupta, R. Sharman (red. nauk.), New York 2009, IGI Global.

Warren S.D., Brandeis L.D., *The Right to Privacy*, „Harvard Law Review" 1890, nr 4, s. 193–220.

Weimann G., *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict & Terrorism" 2016, nr 3, s. 195–206.

Weimann G., *Terror on the Internet: The New Arena, The New Challenges*, Washington 2006, United States Institute of Peace.

Weimann G., *Terrorism in Cyberspace: The Next Generation*, New York 2015, Columbia University Press.

Weimann G., *Terrorist Migration to the Dark Web*, „Perspectives on Terrorism" 2016, nr 3, s. 40–44.

Wexler R., *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, „The Yale Law Journal" 2014, nr 158, http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design, bez paginacji [dostęp: 1 VIII 2020].

Wilner A.S., *Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation*, „International Journal: Canada's Journal of Global Policy Analysis" 2018, nr 2, s. 308–316.

Źródła internetowe

Advanced Blockchain Technology, *Focused on Freedom*, Komodo, https://komodoplatform.com/wp-content/uploads/2018/06/Komodo-Whitepaper-June-3.pdf [dostęp: 3 VIII 2020].

Arora H., *NSA classifies Linux Journal readers, Tor and Tails Linux users as "extremists"*, 4 VII 2014 r., https://static.techspot.com/community/topics/nsa-classifies-linux-journal readers-torand-tails-linux-users-as-extremists.203649/page-3 [dostęp: 1 VIII 2020].

Austin J., *'Traitor' Edward Snowden 'taught ISIS Paris terrorists how to avoid detection'*, „Express", 18 XI 2015 r., https://www.express.co.uk/news/world/620270/Traitor Edward-Snowden-taught-ISIS-Paris-terrorists-avoid-detection-NSA-CIA-John-Brennan [dostęp: 2 VIII 2020].

Barbirato B.B., *Bitcoin: A Political Analysis*, maj 2016 r., https://www.researchgate.net/publication/309411431_Bitcoin_A_Political_Analysis [dostęp: 1 VIII 2020].

Barysevich A., Sola A., *Litecoin Emerges as the Next Dominant Dark Web Currency*, Recorded Future, 8 II 2018 r., https://go.recordedfuture.com/hubfs/reports/cta-2018 0208.pdf [dostęp: 1 VIII 2020].

Berton B, *The dark side of the web: ISIL's one-stop shop*?, raport European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 1 VIII 2020].

Balducci A., Devlin S., Ritter T., *TrueCrypt. Cryptographic Review*, Open Crypto Audit Project, NCC Group, 2015 r., https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf, s. 1–21 [dostęp: 2 VIII 2020].

Clagett L., *Dandelion Onions: Protecting Transaction Privacy in Monero*, Monero Konferenco, 22–23 VI 2019 r., https://www.monerooutreach.org/monero-konferenco/lee-clagett.html [dostęp: 1 VIII 2020].

Cox J., *Cryptocurrency Transactions May Uncover Sales of Shadow Broker Hacking Tools*, „Vice", 28 VI 2018 r., https://www.vice.com/en_us/article/j5k7zp/zcash-shadow-brokers-uncoverhacking-tool-sales [dostęp: 1 VIII 2020].

Cyber-Terrorism Activities Report No. 18, lipiec–wrzesień 2016 r., International Institute for Counter-Terrorism, https://www.ict.org.il/UserFiles/ICT-Cyber-Review-18.pdf, s. 24 [dostęp: 1 VIII 2020].

Czeskis A. i in., *Defeating encrypted and deniable file systems: TrueCrypt v5.1a and the case of the tattling OS and applications*, w: *Proceedings of 3rd USENIX Workshop on Hot Topics in Security*, 2008 r., https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf [dostęp: 1 VIII 2020].

Danezis G., *A Gentle Introduction to Privacy Enhancing Technologies & 2 Case Studies*, 11 VII 2016 r., https://isp.cs.ru.nl/2016/danezis.pdf [dostęp: 1 VIII 2020].

Danezis G., Gürses S., *A critical review of 10 years of Privacy Technology*, Proceedings of Surveillance Cultures: A Global Surveillance Society, kwiecień 2010 r., https://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf [dostęp: 1 VIII 2020].

De Balthasar T., Hernandez-Castro J., *An Analysis of Bitcoin Laundry Services*, Nordic Conference on Secure IT, Tartu 2017 r., https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services [dostęp: 4 VIII 2020].

Duffield E., Diaz D., *Dash: A Privacy-Centric Crypto-Currency*, https://www.zioncoins.co.uk/wp-content/uploads/2015/06/Dash-Whitepaper.pdf, s. 7–8 [dostęp: 1 VIII 2020].

Faife C., *Live Free or Mine: How Libertarians Fell in Love With Bitcoin*, CoinDesk, 8 X 2016 r., https://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin [dostęp: 1 VIII 2020].

Fanusie Y.J., Robinson T., *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies and Elliptic, 12 I 2018 r., http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf, s. 7 [dostęp: 1 VIII 2020].

FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paryż 2019 r., http://www.fatfgafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html [dostęp: 1 VIII 2020].

Fox-Brewster T., *Wannacry hackers are using this Swiss company to launder $142,000 Bitcoin ransoms*, „Forbes", lipiec 2017 r., https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacryhackers-use-shapeshift-to launder-bitcoin [dostęp: 1 VIII 2020].

Gogłoza W., *Cypherpunks, WikiLeaks i widmo kryptograficznej anarchii*, https://wgogloza.com/umcs/informatyka-prawnicza/cypherpunks/ [dostęp: 20 XII 2018].

Goodwin B., *Islamic State supporters shun Tails and Tor encryption for Telegram,* „Computer Weekly", 8 I 2017 r., https://www.computerweekly.com/news/450419581/Islamic-State-supporters-shun-Tails-and-Tor-encryption-for-Telegram [dostęp: 1 VIII 2020].

Greenberg A., *The dark web's favorite currency is less untraceable than it seems*, „Wired", 27 III 2018 r., https://www.wired.com/story/monero-privacy/ [dostęp: 1 VIII 2020].

Greene D., *NSA Mass Surveillance Programs. Unnecessary and Disproportionate*, Electronic Frontier Foundation, 2014 r., https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf [dostęp: 1 VIII 2020].

Haertle A., *Audyt Truecrypta zakończony, dwa istotne błędy w jego implementacji*, Zaufana Trzecia Strona, 2 IV 2015 r., https://zaufanatrzeciastrona.pl/post/audyt-truecryptazakonczony-znaleziono-dwa-istotne-bledy-w-implementacji/ [dostęp: VIII 2020].

Harris S., *CIA's Ex-No. 2 Says ISIS 'Learned From Snowden'*, „Daily Beast", 12 VII 2017 r., https://www.thedailybeast.com/cias-ex-no-2-says-isis-learned-from-snowden [dostęp: 1 VIII 2020].

Higgins S., *ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide*, CoinDesk, 7 VII 2014 r., https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist movements/ [dostęp: 1 VIII 2020].

Jafari S. i in., *Cryptocurrency: A Challenge to Legal System*, Social Science Research Network, styczeń 2018 r., https://www.researchgate.net/publication/325747817_Cryptocurrency_A_Challenge_to_Legal_System [dostęp: 1 VIII 2020].

Junestam A., Guigo N., *Open Crypto Audit Project TrueCrypt Security Assessment*, iSec Partners, 2014 r., https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [dostęp: 1 VIII 2020].

Keatinge T., Carlisle D., Keen F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, 2018 r., http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)60497 _EN.pdf [dostęp: 1 VIII 2020].

Makdad Ch., *"God Rewards Fools" – Whitfield Diffie and Martin Hellman's Stand to Revolutionize Cryptography*, The Eagle Eye News, https://tyroneeagleeyenews.com/wp content/uploads/2017/05/Makdad_Senior_TyroneAreaHighSchool_PA.pdf [dostęp: 1 VIII 2020].

Malik N., *Terror in the Dark*, London 2015 r., raport Henry Jackson Society, http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf [dostęp: 4 VIII 2020].

May T.C., *Cyphernomicon. Cypherpunks FAQ and More, Version 0.666,* 10.09.1994, http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html [dostęp: 20 XII 2018].

May T.C., *The Crypto Anarchist Manifesto*, Activism.net, 22 XI 1992 r., https://www.activism.net/cypherpunk/crypto-anarchy.html [dostęp: 20 XII 2018].

May T.C., *True Nyms and Crypto Anarchy*, 2001, http://www.isfdb.org/cgi-bin/title.cgi?195636 [dostęp: 20 XII 2018].

Opsahl K., *Warrant Canary Frequently Asked Questions*, Electronic Frontier Foundation, 10 IV 2014 r., https://www.eff.org/deeplinks/2014/04/warrant-canary-faq [dostęp: 1 VIII 2020].

Protecting privacy in practice. The current use, development and limits of Privacy Enhancing Technologies in data analysis, A. Noble (red. nauk.), The Royal Society, marzec 2019 r., https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy enhancing-technologies-report.pdf [dostęp: 5 VIII 2020].

Public Bug Bounty List, Bugcrowd, 2020 r., https://www.bugcrowd.com/bug-bounty-list/ [dostęp: VIII 2020].

Roe M. i in., *Cryptography and Evidence*, Cambridge 1997 r., University of Cambridge, https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-780.pdf, s. 11 [dostęp: 26 VIII 2020].

Ryan P., *Left, Right and Center: Crypto Isn't Just for Libertarians Anymore*, CoinDesk, 27 VII 2018 r., https://www.coindesk.com/no-crypto-isnt-just-for-libertarians-anymore [dostęp: 1 VIII 2020].

Shen Y., Pearson S., *Privacy Enhancing Technologies: A Review*, HP Laboratories, sierpień 2011 r., https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf [dostęp: 5 VIII 2020].

Smith M., *Mission Implausible: Defeating Plausible Deniability with Digital Forensics*, SANS Institute, 2 IV 2020 r., https://www.sans.org/reading-room/whitepapers/forensics/mission-implausible-defeating-plausible-deniability-digital-forensics-39500 [dostęp: 1 VIII 2020].

Stancel D., *Economic Consequences of Cryptocurrencies and Associated Decentralized Systems*, https://www.researchgate.net/publication/280794376_Economic_Consequences_of_Cryptocu rencies_and_Associated_Decentralized_Systems [dostęp: 1 VIII 2020].

Ścibor A., *Służbom ze sojuszu Five Eyes nie udało się złamać szyfrowania VeraCrypt*, Fundacja AVLab dla Cyberbezpieczeństwa, 29 V 2019 r., https://avlab.pl/sluzbom-ze-sojuszu-five--eyes-nie-udalo-sie-zlamac-szyfrowaniaveracrypt [dostęp: 3 VIII 2020].

United States of America v. Buster Hernandez, United States District Court, https://casetext.com/pdf-email?slug=united-states-v hernandez-1195, s. 1–28 [dostęp: 1 VIII 2020].

Titcomb J., *Did Paris terrorists really use PlayStation 4 to plan attacks?,* „The Telegraph", 16 XI 2015 r., https://www.telegraph.co.uk/technology/videogames/playstation/11997952/paris-attacks-playstation-4.html [dostęp: VIII 2020].

Venkatakrishan S.B, Fanti G., Viswanath P., *Dandelion: Redesigning the Bitcoin Network for Anonymity*, Sigmetrics'17, 5–9 VI 2017 r., Urbana-Champaign, https://dl.acm.org/doi/10.1145/3078505.3078528 [dostęp: 1 VIII 2020].

Ye Claire i in., *Alt-Coin Traceability*, International Association for Cryptologic Research, 18 V 2020 r., https://eprint.iacr.org/2020/593.pdf, s. 16–21 [dostęp: 1 VIII 2020].

Zulkarnine A.T. i in., *Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content*, IEEE Conference on Intelligence and Security Informatics (ISI), Tucson 2016 r., s. 109–114, https://ieeexplore.ieee.org/xpl/conhome/7739307/proceeding [dostęp: 3 VIII 2020].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

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 (DzU z 1993 r. nr 61 poz. 284).

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

Powszechna Deklaracja Praw Człowieka (*Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana 10 grudnia 1948 r.).*

Karta Praw Podstawowych Unii Europejskiej z 7 grudnia 2000 r. (Dz. Urz. UE C 83 z 30 III 2010 r., s. 389.)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – (Dz. Urz. UE L 119 z 4 V 2016 r., s. 1).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j.: DzU z 2019 r. poz. 1781).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j.: DzU z 2021 r. poz. 534).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj.: Dz.U. z 2019 r. poz. 1231).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j.: Dz.U. z 2019 r. poz. 1145, ze zm.).

Abstrakt

Technologie wspierające prywatność (*Privacy Enhancing Technologies*, PET) stwarzają zagrożenie ładu społecznego. Wskazuje na to analiza ich ideologiczno-politycznych fundamentów oraz uregulowań prawnych wprowadzających ograniczenia w zakresie ich używania, a także analiza ich faktycznych zastosowań w działalności cyberprzestępczej. Opracowanie ma charakter przeglądowy i praktyczny, dokonano w nim autorskiego stypologizowania technologii wspierających prywatność. Ocenie poddano wybrane instrumenty informatyczne, które są najpowszechniej używane oraz stanowią potencjalne i rzeczywiste zagrożenie. Są to: oprogramowania zapewniające anonimową komunikację (Tor, Freenet, Linux Tails, Whonix), ekosystemy kryptowalut umożliwiające anonimową wymianę handlową (Monero, Zcash, Dash) oraz aplikacja, która pozwala na szyfrowanie danych (VeraCrypt). Podsumowanie jest próbą wskazania modelowych atrybutów technologii wspierających prywatność na podstawie wcześniej przeprowadzonych analiz.

Słowa kluczowe: technologie wspierające prywatność, anonimowość, cyberprzestępczość, terroryzm, kryptoanarchizm.

Privacy Enhancing Technologies – ideology, law and implementations

Abstract

Privacy Enhancing Technologies (PET) create a threat to the social order which is shown in the analysis of their ideological as well as political foundations and legal regulations that introduce restrictions on their use. Study into their actual applications in cybercriminal activity proves it too. This paper is a review with practical purpose and includes an original typology of PET. The most commonly used IT instruments that create a potential and actual threat were selected and analysed: software ensuring anonymous communication (Tor, Freenet, Linux Tails, Whonix), cryptocurrency systems enabling anonymous trade (Monero, Zcash, Dash) and an application enabling data encryption (VeraCrypt). The summary includes an attempt to extract the model attributes of privacy-enhancing technologies on the basis of previous analyses.

Keywords: privacy enhancing technologies, anonymity, cybercrime, terrorism, crypto anarchy.

MACIEJ ALEKSANDER KĘDZIERSKI
ORCID: 0000-0003-3074-1355

DOI: 10.4467/20801335PBW.21.001.13558

Możliwość zastosowania inżynierii odwrotnej do zwalczania organizacji przestępczych typu sieciowego

Inżynieria odwrotna, określana także jako inżynieria wsteczna (ang. *reverse engineering*, RE), pozwala zrozumieć, jak „coś" (np. jakiś przedmiot) zostało wykonane – mimo dysponowania ograniczoną wiedzą na ten temat[1]. Próbuje zatem odpowiedzieć na pytanie, jak przebiegał proces tworzenia jakiegoś przedmiotu. Inżynieria odwrotna inaczej podchodzi do inżynierii niż inżynieria tradycyjna (postępowa). Ten drugi rodzaj inżynierii jest procesem przebiegającym od pomysłu, który jest generowany potrzebą stworzenia fizycznego produktu, do jego realizacji. Inżynieria odwrotna zaś – jak sama nazwa wskazuje – jest procesem przebiegającym od fizycznego produktu, którego wszystkie składowe są szczegółowo analizowane, a następnie rozwijane, do nowego fizycznego produktu w takiej samej bądź ulepszonej postaci[2]. Inżynieria odwrotna jest także dziedziną nauki zajmującą się wszelkimi metodami, które umożliwiają wprowadzenie realnego produktu do rzeczywistości wirtualnej. Nazwa „inżynieria odwrotna" pochodzi od kolejności wykonywania działań – najpierw jest obiekt rzeczywisty, a dopiero przy użyciu skanerów i zastosowaniu metod inżynierskich otrzymuje się obiekt wirtualny[3]. Inżynieria odwrotna znajduje zastosowanie głównie w „sztuce inżynierskiej", stąd też niekiedy jest nazywana „inżynierią rekonstrukcyjną". Zgodnie z definicją zaprezentowaną przez Elliota

---

1 K. Breeman, *How does reverse engineering relate to forensics and solving crimes?*, https://www.quora.com/How-does-reverse-engineering-relate-to-forensics-and-solving-crimes [dostęp: 14 IV 2020].

2 M. Szelewski, M. Wieczorowski, *Inżynieria odwrotna i metody dyskretyzacji obiektów fizycznych*, „Mechanik" 2015, nr 12, s. 183, http://www.mechanik.media.pl/pliki/do_pobrania/artykuly/22/40_183_188.pdf [dostęp: 15 IV 2020].

3 S. Kachel i in., *Zastosowanie inżynierii odwrotnej do procesu odtwarzania geometrii układu wlotowego silnika RD-33 w samolocie MIG 29*, „Prace Instytutu Lotnictwa" 2011, nr 213, s. 66 i nast., http://ilot.edu.pl/PIL/PIL_213.pdf [dostęp: 14 IV 2020].

Chikofsky'ego i Jamesa Crossa (…) *inżynieria odwrotna – to proces uzyskiwania wystarczającego zrozumienia na poziomie projektu o produkcie, który pomoże w jego utrzymaniu, ulepszeniu lub wymianie. To także jest część procesu utrzymania oprogramowania, która pomaga zrozumieć system wystarczająco do podjęcia decyzji w tej sprawie. W procesie tym nie jest wymagana zmiana systemu w jakikolwiek sposób*[4]. W przypadku inżynierii odwrotnej idea działania polega na zastosowaniu jej procesów w odniesieniu do obiektu materialnego, który jest kolejno mierzony, a następnie przekształcany w model. Otrzymany model może być przedmiotem dalszego badania i przekształcania w założonym celu.

Początkowo inżynieria odwrotna odnosiła się wyłącznie do analizy urządzenia technicznego (przedmiotu fizycznego). Obecnie jest ona stosowana w analizie programów komputerowych, np. w celu poznania, w jaki sposób dane oprogramowanie zostało użyte do popełnienia przestępstwa, wykrycia luk w projektowanym programie, ustalenia źródłowych kodów dostępu, wykrycia wirusowego (złośliwego) oprogramowania i jego analizy lub w celu odzyskania utraconych danych. Inżynieria odwrotna jest także wykorzystywana w analizie działań szpiegowskich dotyczących rozwiązań militarnych lub logistycznych przeciwnika. W tym przypadku szczególną rolę odgrywa zrozumienie badanego obiektu (systemu) i jego struktury. Omawiany rodzaj inżynierii jest więc procesem analizy mającym na celu zwiększenie ogólnego zrozumienia systemu – zarówno pod względem jego utrzymania, jak i umożliwienia jego dalszego rozwoju (doskonalenia)[5]. Inżynierię odwrotną wykorzystuje się zazwyczaj, aby uzyskać brakującą wiedzę bądź znaleźć pomysł na projektowanie, gdy takie informacje są niedostępne w chwili inicjacji zadania.

Proces RE jest podzielony na trzy fazy: przegląd, skanowanie podzespołów i ukierunkowane eksperymenty. W pierwszych dwóch fazach stosuje się metody statyczne (analiza statyczna), a w fazie końcowej – metody dynamiczne (analiza dynamiczna). Analiza statyczna sprawdza oprogramowanie, nie uruchamiając go i nie ryzykując uszkodzenia działającego programu. Za pomocą tej techniki eksperci mogą bezpiecznie dowiedzieć się więcej na temat kodowania takich programów, jak np. złośliwe oprogramowanie. Analiza dynamiczna polega na kontrolowanym uruchamianiu lub deasemblacji oprogramowania (tj. odtworzeniu kodu źródłowego z programu zapisanego w kodzie maszynowym[6]) w celu zrozumienia, w jaki sposób działa złośliwe oprogramowanie, przy jednoczesnym uniknięciu poważnego ryzyka dla rzeczywistych środowisk[7]. Dzięki oprogramowaniu komputerowemu jest możliwe nie tylko ustalenie i wykrycie

---

[4] E.J. Chikofsky, J.H. Cross II, *Reverse engineering and design recovery: a taxonomy*, „IEEE Software" 1990, nr 1, s. 13–17.

[5] E.J. Chikofsky, J.H. Cross II, *Encyclopedia of Software Engineering*, 2002, https://onlinelibrary.wiley.com/doi/abs/10.1002/0471028959.sof285 [dostęp: 15 IV 2020].

[6] *Słownik Języka Polskiego*, hasło: 'deasemblacja', https://sjp.pl/deasemblacja [dostęp: 15 IV 2020].

[7] B. Hendricks, *Reverse Engineering in Digital Forensics*, rozdział 4, lekcja 9, w: https://study.com/academy/lesson/reverse-engineering-in-digital-forensics.html [dostęp: 19 XII 2020].

powiązań sieciowych organizacji przestępczej, lecz także poznanie sposobów posługiwania się programem komputerowym przez organizację przestępczą jako instrumentem do popełniania czynów penalizowanych. Rezultat końcowy uzyskuje się w wyniku oceny relacji między elementami sieci a atrybutami cechującymi te elementy, np. na podstawie dających się zmierzyć cech (właściwości) wchodzących w skład atrybutów lub paramentów konstrukcji oprogramowania wykorzystywanych do realizacji wyznaczonego celu[8]. Taka ocena jest pomocna szczególnie wtedy, gdy organizacja przestępcza pozostająca w strukturze sieciowej dokonuje przestępstw, ataków terrorystycznych w cyberprzestrzeni albo używa specjalistycznego kodowanego oprogramowania, aby rozpowszechniać wiedzę terrorystyczną, werbować bojowników i utrzymywać kontakty ze swoimi zwolennikami. Warto zaznaczyć, że organizacje terrorystyczne również poszukują specjalistów z zakresu RE. Jest to konsekwencja chęci pójścia na skróty, braku odpowiednich środków na realizację celu i poszukiwania nowych sposobów przeprowadzania ataków terrorystycznych, np. z użyciem „brudnej broni jądrowej". Kod komputerowy napisany przez tzw. mocarstwa jądrowe może zostać przejęty (np. przez złośliwe oprogramowanie), poddany procesowi inżynierii odwrotnej, a następnie ponownie wykorzystany przez inne państwa lub podmioty niepaństwowe. Możliwe jest przyjęcie hipotetycznej sytuacji, w której grupa terrorystyczna kopiuje, a następnie poddaje procesowi RE niszczycielski wojskowy program komputerowy, utworzony na potrzeby ataku przeciw innym krajom, a następnie kieruje go na ustanowione przez siebie cele.

Powstaje więc pytanie, czy inżynierię odwrotną można zastosować nie tylko do odtwarzania, uzupełniania, udoskonalania rzeczy, oprogramowania i poszerzania wiedzy, lecz także do udoskonalenia przeprowadzonej procedury analitycznej, w której przedmiotem diagnozy jest organizacja typu sieciowego. A jeżeli jest to możliwe, to w jakim zakresie?

Wykorzystanie inżynierii odwrotnej jako obszar badawczy

Przestępczość jako zjawisko społeczne jest podporządkowana innym regułom niż działanie obiektów fizycznych. Mówi się o tzw. inżynierii społecznej (ang. *social engineering*), która odnosi się w zasadzie do socjologii (a w omawianym przypadku – mikrosocjologii) i jest związana ze stosowaniem wielu metod i technik służących osiągnięciu określonych celów, w tym manipulacji społeczeństwem (socjotechnika). Zbieżność nazwy nie oznacza jednak zbieżności pojęciowej. Natomiast sam proces działania (aktywizowania czynności) można uznać za proces inżynieryjny. Zjawiska, jakie zaszły w poprzednich latach, w tym postęp technologiczny, doprowadziły do nowego „umieszczenia" społeczeństwa w wirtualnej rzeczywistości, w której relacje społeczne

[8] Dotyczy dla przykładu: zestawu instrukcji, zaimplementowanych interfejsów i zintegrowanych danych, także utworzonych w sposób autorski, cechujący indywidualnego twórcę.

zostały ujęte ilościowo i wyrażone wzorami matematycznymi. Przeniesienie społeczeństwa do Internetu umożliwiło zastosowanie innego sposobu monitorowania zachowań jednostek – za pomocą technologii komunikacyjnych i zarządzania dystrybucją informacji. Jest to konsekwencja z jednej strony udostępniania ludziom urządzeń z różnymi niezbędnymi dla nich aplikacjami wywierającymi wpływ na ich aktywności, podejmowanie decyzji bądź planowanie działań w czasie, z drugiej zaś – umieszczania w przestrzeni publicznej przez ustawodawcę i organy władzy rozwiązań ułatwiających realizację spraw osobistych (e-bankowość, e-urząd, e-sądy) i połączenia użytkownika z tymi rozwiązaniami. Osoby korzystające z takich aplikacji zostawiają ślad w przestrzeni teleinformatycznej. Tak technologicznie (inżynieryjnie) stworzone społeczności są aktywne w matrycach zbudowanych na rozwiązaniach matematycznych, kreujących nową rzeczywistość, także tę sprzeczną z prawem. Nie byłoby możliwe zastosowanie inżynierii odwrotnej do badania zachowań struktur społecznych, gdyby nie wprowadzono do niej rozwiązań z zakresu sieci społecznych czy teorii grafów. Dzięki temu można było uporządkować zachowania jednostki i tworzone przez nią formy organizacyjne.

Działania jednostki są umieszczane na technologicznej matrycy, co umożliwia zarówno sterowanie procesami społecznymi, jak i ich kontrolowanie. Dzięki temu przy analizowaniu zjawisk społecznych można posłużyć się rozwiązaniami, które pod względem technologicznym powinny być raczej przypisane nie badaniom społecznym, a technicznym. Społeczeństwo (lub jego część) traktuje się wówczas jako układ złożony.

Systemy (układy) złożone mają pewne własności potwierdzone w praktyce, np. wrażliwość na początkowe warunki lub małe zakłócenia, mnogość interakcji między ich różnymi elementami. Wszystkich ich własności nie da się w prosty sposób przewidzieć po zbadaniu własności ich poszczególnych komponentów, ponieważ ciągle ewoluują i się rozwijają (dynamika)[9]. W celu określenia charakterystycznych cech układu będzie można zastosować następujące właściwości: miarę centralności wierzchołków[10] (charakteryzowaną przez: bliskość[11], stopień[12], promień, pośrednictwo[13],

[9] Zob. A. Fronczak, P. Fronczak, *Świat sieci złożonych: Od fizyki do Internetu*, Warszawa 2009; Z. Tarapata, *Czy sieci rządzą światem? Od Eulera do Barabasiego*, „Biuletyn Instytutu Systemów Informatycznych" 2012, nr 10, s. 37.

[10] Centralność jednostki (reprezentowanej przez węzeł w grafie) określa stopień zaangażowania jednostki w relacje z innymi jednostkami. Centralność może zostać wyrażona przez: stopień węzła, bliskość jednostki do innych jednostek, częstość występowania jednostki w charakterze pośrednika w procesie komunikacji między innymi jednostkami. Zob. P. Lula, *Analiza struktury serwisów WWW*, Uniwersytet Ekonomiczny w Krakowie, http://www.ae.krakow.pl/~lulap/WM_2009_04.pdf [dostęp: 11 II 2021].

[11] Zgodnie z tą miarą wierzchołek jest tym bardziej centralny, im jest bliżej wszystkich innych wierzchołków sieci.

[12] Stopień wierzchołka v w grafie G to liczba krawędzi dochodzących do tego wierzchołka.

[13] Pośrednictwem (ang. *betweenness*) węzła v nazywa się stosunek liczby najkrótszych ścieżek między dowolnymi dwoma węzłami przechodzących przez węzeł v do łącznej liczby wszystkich najkrótszych ścieżek.

współczynnik gronowania[14]) oraz stopień pośrednictwa elementów pośredniczących i peryferyjnych[15].

Pod pojęciem analiza sieci społecznej (ang. *social network analysis*, SNA), oznaczającym jedną z metod technicznych przedstawiających relacje między węzłami (wyznaczonymi elementami społeczności), należy rozumieć mapowanie i mierzenie relacji oraz przepływów między osobami, grupami, organizacjami, komputerami, adresami URL i innymi powiązanymi jednostkami informacji (wiedzy). Zmapowane relacje tworzą sieć, która pokazuje zależności lub przepływy między węzłami. Węzły w sieci to ludzie i grupy, podczas gdy połączenia (łącza) wskazujące na zależności lub przepływy między węzłami to krawędzie lub relacje. Analiza sieci społecznej zapewnia zarówno wizualną, jak i matematyczną ocenę relacji międzyludzkich[16].

Badania ukierunkowane na działania organizacyjne pozwoliły na stworzenie pojęć: analiza sieci organizacyjnych (ang. *organizational network analysis*, ONA), czyli zastosowanie SNA wobec organizacyjnych (sieciowych) form społecznych, oraz analiza sieci kryminalnych (przestępczych) (ang. *criminal network analysis*, CNA). Analiza sieci organizacyjnych to uporządkowany sposób wizualizacji przepływu przez organizację komunikacji, informacji i decyzji. Sieci organizacyjne składają się z węzłów i powiązań stanowiących podstawę do zrozumienia, w jaki sposób informacje przepływają w organizacji. Należy jednak pamiętać, że CNA to nie SNA. Za taką tezą stoi argument, że organizacje przestępcze z założenia działają w „niewidzialnej przestrzeni", kamuflują i zatajają swoją aktywność niezgodną z prawem, stawiają sobie inne cele i przyjmują taktykę działania odmienną od ustanowionych i akceptowanych norm państwowych i społecznych. Dlatego też trudno zakładać, że tego rodzaju struktury będą się uzewnętrzniać w sieciach społecznościowych. Można natomiast spotkać się z innymi działaniami tych struktur, które są widoczne w aktywności związanej z przygotowaniami do przestępstwa, legalizowaniem przestępczych aktywów lub ich inwestowaniem czy wręcz wynikają z popełnienia błędów polegających na zbytnim uzewnętrznianiu się ze swoim przestępczym statutem w sieci internetowej lub w świecie realnym. Te rodzaje działań wymagają prowadzenia rozpoznania również w otwartych źródłach informacji (sieć powierzchniowa), a przynajmniej w tzw. ukrytym Internecie czy czarnej sieci (ang. *Darknet*). Analiza sieci kryminalnych odnosi się do relacji

---

[14] Definiuje się go jako prawdopodobieństwo istnienia połączenia między parą węzłów, które mają przynajmniej jednego wspólnego sąsiada.

[15] Szczegółowo zob. Z. Tarapata, *Czy sieci rządzą światem?*… Podczas kształtowania się sieci społecznych dochodzi do efektu gronowania się (grupowania) ludzi o podobnych poglądach, zainteresowaniach, a także do uczestniczenia w naruszaniu prawa itp. Zob. także: M. Morzy, A. Ławrynowicz, *Wprowadzenie do analizy sieci społecznych*, Poznań 2010/2011, https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf [dostęp: 16 IV 2020].

[16] Ł. Wawrzynek, *Analiza sieci społecznych w identyfikacji i wzmacnianiu potencjału innowacyjnego zespołów pracowniczych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Research Papers of Wrocław University of Economics" 2017, nr 496, s. 183 i nast.

zachodzących w ramach nieformalnych, kryminalnych bądź terrorystycznych form organizacyjnych.

Rozwiązania przedstawione w artykule pozwalają przenieść relacje społeczne za pomocą wzorów matematycznych w obszar, który będzie można badać z wykorzystaniem RE. Metody stosowane w analizie sieci służą odtajnieniu i ujawnieniu ukrytych w niej danych oraz przedstawieniu ich jako wzorce ludzkich możliwości. Niezależnie od stosowanych określeń odnoszących się do organizacyjnych form popełniania przestępstw (zorganizowana przestępczość, organizacja terrorystyczna) występują różnice wewnątrzorganizacyjne, charakterystyczne dla danej organizacji, co wyróżnia ją spośród innych, podobnych form przestępczych. Dlatego też najpierw powinno się podjąć czynności zmierzające do oceny funkcjonowania takiej organizacji w sieci społecznej. Będzie można ocenić stopień integracji (stan zespolenia) oraz charakterystyczne zachowania przynależne jedynie tej organizacji (wewnętrzny kod organizacyjny) oraz wzajemne relacje organizacji z otoczeniem. Zastosowanie RE i analizy sieci społecznych powinno umożliwić zdobycie wiedzy o niewidocznych relacjach, a nie tylko o prostych, formalnie zdefiniowanych powiązaniach. Więzi nieformalne często w większym stopniu determinują i odzwierciedlają sposób pracy niż wyznaczone role i pozycje w strukturze formalnej (dane relacyjne i atrybuty)[17]. Wynikiem zastosowania RE i CNA powinno być nie tylko odtworzenie zachowań węzłów i samej organizacji jako sieci (jak w analizie kryminalistycznej[18]), lecz także „wytworzenie" tych relacji, które dotychczas były ukryte dla organów ścigania i dlatego nie zostały poddane czynnościom weryfikacyjnym czy sprawdzeniowym[19]. Odnosi się to zarówno do niewykrytych zachowań osób fizycznych, jak i zaszyfrowanych komunikatów (relacji) w sieci teleinformatycznej, korzystania z zamkniętych forów dyskusyjnych oraz ukrytego Internetu. Brak takiej wiedzy może spowodować przyjęcie niewłaściwej taktyki zwalczania przestępczości oraz niepoprawne wytypowanie sprawców, zleceniodawców i kierownictwa organizacji. Na przedmiot objęty analitycznym podejściem RE należałoby spojrzeć z dwóch stron. Pierwszej, w której przedmiotem jest organizacja przestępcza jako nieformalny twór przynależności i wspólnego działania kryminalnego (ujmowany w kategorii interpersonalnego związku przestępczego). Drugiej zaś, w której organizacja przestępcza jest określana jako podmiot organizacyjny (firma, sieć sprzedaży,

---

[17] Tamże, s. 189. Relacje (komunikacja, współdziałanie) wskazują na właściwą merytorycznie i rzeczywistą rolę danej jednostki w organizacji.

[18] W ramach badań kryminalistycznych poszczególnych przedmiotów, typowanych jako przedmioty (dowody) przestępstwa, również jest możliwe zastosowanie RE. Zob. T. Kurzynowski i in., *Proces inżynierii odwrotnej w zastosowaniach kryminalistycznych*, „Problemy Kryminalistyki" 2014, nr 285, s. 4–46.

[19] Działania uzupełniające mogą być konsekwencją przekazania dodatkowych informacji ze źródeł krajowych, zagranicznych jednostek policji czy służb, wykonania międzynarodowej analizy przez np. Interpol czy Europol, wykonania analizy informacji finansowej przez krajową Jednostkę Analityki Finansowej (GIIF) lub też na potrzeby dokonania ponownej analizy materiałów przez jednostkę prowadzącą daną sprawę.

instytucja finansowa) będący pod kontrolą grupy osób. W tym przypadku przedmiot organizacyjny staje się całościowo instrumentem do popełnienia określonego rodzaju przestępstwa (np. podmioty gospodarcze powołane w celu dokonania przestępstwa oszustwa na szeroką skalę – piramidy finansowe).

Próba oceny możliwości zastosowania inżynierii odwrotnej do badań nad sieciowymi strukturami przestępczymi

Wysoka technologizacja zachowań społecznych pozwala na rozważenie możliwości wprowadzenia RE w obszar zjawisk międzyludzkich (społecznych). Będzie można wówczas zbadać, dlaczego ktoś nie zachował się tak, jak powinien, lub też spowodować, aby ktoś zachował się tak, jak to zostało zaplanowane. Tego rodzaju elementy byłyby możliwe do wykorzystania na potrzeby taktyki zwalczania przestępstw, w tym do prowadzenia przez agenta swoistej gry z przeciwnikiem, np. w ramach operacji specjalnej jako czynności operacyjno-rozpoznawcze. Inżynieria odwrotna może być pomocna nie tylko przy wskazywaniu przyczyn niepowodzeń w procesach wykrywczych (np. z wykorzystaniem inżynierii postępowej), lecz także służyć poprawianiu efektów tych procesów przez wykrywanie ich możliwych wad (błędnej oceny poszczególnych relacji, węzłów i całości sieci).

Inżynieria odwrotna ma na celu przedstawienie schematu systemu, który pozwoli przewidzieć problemy, dokonać poprawek lub dowiedzieć się, co poszło nie tak w procesie budowania systemu lub narzędzia i gdzie popełniono błąd[20]. W przypadku oddziaływania na systemy inżynierię odwrotną można postrzegać technicznie przez pryzmat zastosowanych i modelowanych programów komputerowych (np. poszukując luk w oprogramowaniu, ustalając tzw. *zero-day*[21] stosowany w celu użycia złośliwego oprogramowania) lub przez usystematyzowane procesy przeciwdziałania popełnianiu przestępstw. Uporządkowanie procesów wykrywczych w ramach prowadzonych czynności operacyjnych i kryminalistycznych pozostaje więc istotne z punktu widzenia taktyki zwalczania przestępczości, która powinna uwzględniać podejście systemowe. Oznacza to również, że na nieuporządkowane działanie społeczne, w tym niezgodne z prawem, należy reagować w adekwatny sposób. Taktyka działań będących reakcją na zdarzenie przestępcze powinna zostać usystematyzowana, a przede wszystkim powinna znormalizować rzeczywistość, ale również powinna być odbierana jako działanie organu ścigania. Oznacza to możliwość przyjęcia określonego wzorca dla modelu postępowania, od którego odchylenia będą świadczyły o nieprawidłowościach. Ich ocena sytuacyjna będzie zmierzała do

[20] ABL Engineering, *What Are the Different Types of Reverse Engineering Tools?*, https://ablengineering.com.au/What-Are-the-Different-Types-of-Reverse-Engineering-Tools-~69 [dostęp: 19 XII 2020].

[21] Atak *zero-day* to atak, który wykorzystuje lukę *zero-day* w celu zainstalowania złośliwego oprogramowania.

ustalenia, czy odchylenie pozostaje w normie i nie narusza dobra chronionego prawem, czy też stanowi czyn karalny z punktu widzenia ustawodawcy. Takie postępowanie wynika z potrzeby wyodrębnienia z działań społecznych takich z nich, które – zgodnie z wolą ustawodawcy – są działaniami przestępczymi (stanowią więc specyficzne działania niezgodne z przyjętymi normami społecznymi) i nie mieszczą się w granicy postępowania dozwolonego prawem. Systemowe podejście do czynności mieszczących się w zakresie przeciwdziałania i zwalczania przestępczości ma ten walor, że w ramach RE jest możliwe przeanalizowanie zaistniałych procesów decyzyjnych, sprawdzenie ich zgodności z przyjętymi wzorcami oraz skorygowanie realizacji zadań.

Zastosowanie metody inżynierii odwrotnej jest pomocne nie tylko w przeprowadzeniu audytu bezpieczeństwa, wykryciu oszustwa lub ukrywania się przestępców w sieci, lecz także wykryciu wykorzystania jej elementów, atrybutów lub struktury na potrzeby przestępcze. Umieszczenie forów społecznościowych, e-zakupów, e-usług (w tym finansowych). które są wykorzystywane również w celach przestępczych, w przestrzeni wirtualnej, pozwala na pozyskiwanie śladów działań przestępców i otrzymanie w ramach RE pełniejszego obrazu modelu przestępczego wykreowanego przez sprawcę (elementy sieci). Użycie instrumentów z przestrzeni wirtualnej pozwala też na budowanie schematu postępowania zarówno w fazie przygotowania, jak i dokonania przestępstwa.

Istotnymi elementami postępowania sprawców przestępstw jest ich kamuflowanie się, tajność, zacieranie przez nich śladów oraz wprowadzanie w błąd. Dlatego też organy ścigania podejmują wysiłki, aby odtworzyć przebieg zdarzenia przestępczego, wytypować konkretną osobę jako sprawcę czynu przestępczego oraz przypisać jej dokonanie tego czynu. Niestety, wielokrotnie ten obraz jest niepełny, zawiera luki w wiedzy o przebiegu zdarzenia, które nie ułatwiają wykazania związku przyczynowo-skutkowego między zdarzeniami lub pozwalają przypisać winę i popełnienie przestępstwa danej osobie jedynie w określonym stopniu. Inżynieria odwrotna daje organom ścigania dodatkowe możliwości uzupełnienia dotychczasowego obrazu przestępstwa przez rozbicie go na czynniki pierwsze i wykorzystanie metod oraz technik umożliwiających uzupełnienie luk i poszerzenie pola działania. Analizowanie przestępstwa oparte na modelowaniu inżynierskim może się odnosić między innymi do badania kryminalistycznego przedmiotów zabezpieczonych na miejscu zdarzenia (w tym otrzymania ich modelu w wersji 3D dzięki digitalizacji za pomocą skanera) lub też do przedmiotów uzyskanych w wyniku przeszukania miejsca, które zostało wytypowane jako to, w którym przebywał sprawca. Oznacza to możliwość technicznego odtworzenia brakującej części przedmiotu, istotnego ze względu na prawdopodobieństwo użycia go na miejscu zdarzenia przestępczego, wykonania całościowej ekspertyzy kryminalistycznej, a także przeprowadzenia analizy: od zdarzenia przestępczego do jego sprawcy.

Możliwość zastosowania metody RE do zwalczania organizacyjnych form przestępczych typu sieciowego (zorganizowane grupy przestępcze, organizacje terrorystyczne) jest sprawą otwartą. Inżynieria odwrotna to proces pomiarowy, zatem zmierzenie zjawisk społecznych będzie możliwe jedynie wtedy, gdy relacje społeczne

będzie można przełożyć na mierzalne modele. Im więcej obszarów społecznych będzie przedmiotem badań pomiarowych i im doskonalsze będą instrumenty badawcze, tym łatwiej będzie można przełożyć otrzymane wyniki na wzorce analityczne, które są skoncentrowane na badaniach zjawisk przestępczych[22]. Takie rozwiązania dają między innymi: teoria grafów, algebra macierzowa, statystyka, miarowanie mediów społecznościowych (ang. *social media*)[23], SNA, CNA, ale też RE, jeśli się założy istnienie racjonalnego konstruktora sieci, a w omawianym przypadku – założyciela zorganizowanej grupy przestępczej lub organizacji terrorystycznej. Stąd też RE można zastosować, gdy istnieje możliwość zmierzenia związku przestępczego (sieci przestępczej) lub czynności realizowanych przez podmiot organizacyjny (np. korzystania ze stron internetowych, mediów społecznościowych, SMS-ów, serwisu personalnego, e-maili, reklamy medialnej, sprzedaży w sklepie lub świadczenia usług) oraz gdy takie działania służyły do popełnienia przestępstwa. I w jednym, i w drugim przypadku organy ścigania mają możliwości pozyskania informacji, które będzie można przetworzyć na wyznaczniki. Te zaś będzie można zmierzyć (bilingi telefoniczne, dane z GPS samochodów, bramki poboru opłat drogowych, informacje pochodzące z obserwacji czy kontroli operacyjnej bądź analizy kryminalnej). Trudności powstają w momencie, gdy nie jest możliwe pozyskanie danych w celu poddania ich analizie. Dotyczy to drobnych przestępstw (np. oszustw), które nie są zgłaszane. Powody niezgłaszania są różne: zbyt drobne kwoty, unikanie utraty zaufania do przedsiębiorstwa, zatrzymywanie danych przez duże firmy i korporacje ze względu na chęć ograniczenia odpowiedzialności decydentów. W takich przypadkach roszczenia osób poszkodowanych są zaspokajanie z własnych funduszy firmy. W konsekwencji analityk otrzymuje niepełny obraz, a wręcz brakuje śladów istotnych przy typowaniu obszarów analitycznych. W takiej sytuacji będzie pomocne zastosowanie analizy predykcyjnej[24] lub inżynierii odwrotnej.

Kryminalistyka jako nauka wspierająca działania wykrywcze i służąca poznawaniu sposobów popełniania przestępstw wymaga gromadzenia dowodów, które następnie podlegają procesowi badawczemu (inżynieria kryminalistyczna). Aby właściwie zebrać

---

[22] Dla przykładu: modelowanie sieci bezskalowych (R. Albert, A.-L. Barabási), odkrywanie społeczności lokalnych, klik w sieciach społecznych (K. Faust, J. Scott, S. Wasserman), rozwijanie problemu hierarchii w sieciach (A.-L. Barabási, S.N. Dorogovtsev, E. Ravasz). Zob. szerzej: M. Kowalska-Musiał, *Strukturalna metodologia pomiaru sieci społecznych – rys historyczny i współczesne obszary zastosowań*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2013, nr 28, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171350117 [dostęp: 15 II 2021].

[23] Zob. M. Lewandowski, *Pomiar mediów społecznościowych jako element zarządzania wiedzą i informacją w przedsiębiorstwach*, „Acta Universitatis Nicolai Copernici. Zarządzanie" 2018, nr 4, s. 117 i nast., https://apcz.umk.pl/czasopisma/index.php/AUNC_ZARZ/article/view/AUNC_ZARZ.2018.049/17178 [dostęp: 16 IV 2020].

[24] Analityka predykcyjna (ang. *predictive analytics*; wymiennie stosuje się też pojęcia *data mining* lub *data science*) to proces wydobywania informacji z istniejących zbiorów danych w celu określenia wzorów i przewidywania przyszłych zdarzeń i trendów. Za: https://algolytics.pl/analityka-predykcyjna-slownik-pojec/ [dostęp: 15 II 2021].

dowody, śledczy muszą zrozumieć zdarzenie, z którym mają do czynienia. Ponieważ nie wszystkie zdarzenia są typu *open source* lub dobrze udokumentowane, konieczne może być zastosowanie inżynierii odwrotnej, aby uzyskać dostęp do dowodów lub zrozumieć warunki użycia danego dowodu. Przykładowo tylko niektóre programy komputerowe są typu otwartego, czyli ich użytkownicy mogą zobaczyć, jak zostały napisane. Wiele programów tego nie umożliwia – ich użytkownicy nie mogą zobaczyć kodu, udostępnić go innym osobom ani zmodyfikować (są one stosowane do zamkniętych formatów danych, rozszerzeń kompatybilności i uzupełniania brakującej części kodu). W takich przypadkach ważne jest, aby zespół zajmujący się kryminalistyką cyfrową zdekonstruował to oprogramowanie i pracował nad nim krok po kroku. Poznanie elementów oprogramowania pomaga w szukaniu dowodów przestępstwa lub lepszym zrozumieniu znaczenia dowodów już odkrytych[25]. Inżynierowie mogą więc odegrać istotną rolę w dochodzeniu w sprawie o przestępstwo i służyć specjalistyczną wiedzą oraz umiejętnościami z zakresu inżynierii odwrotnej, które – jak już wspomniano – mogą zostać wykorzystane do opracowania technologii ułatwiających pozyskiwanie dokładniejszych informacji z zebranych dowodów.

O ile możliwe jest zastosowanie RE w technice kryminalistycznej, o tyle do oceny pozostaje, czy z tego typu rozwiązania można korzystać w analizie kryminalnej[26]. Czy istnieje możliwość zastosowania metody inżynierii odwrotnej w odniesieniu do zjawisk (np. funkcjonowania nieformalnych struktur organizacyjnych) lub do postępowania przestępczego, a nie tylko do regulacji czy konstrukcji technicznych opartych na ścisłych parametrach i wyliczeniach (podobnie jak ONA, ang. *organizational network analysis*, która jest sieciową analizą organizacji wykorzystywaną do oceny i zoptymalizowania relacji w ramach organizacji sieciowej). Ponadto na przedmiotową sprawę należałoby spojrzeć zarówno z punktu widzenia posiadania odpowiednich narzędzi do pozyskania i wyliczenia technicznych (metrycznych) parametrów danej organizacji przestępczej, jej sieci lub całości zjawiska, jak i postawionego celu ostatecznego. Tym celem może być zarówno neutralizacja organizacji przestępczej, jak i ocena skali zjawiska w granicach konkretnego kontynentu czy nawet świata, a także wskazanie trendów rozwojowych i ich kierunków. Zastosowanie RE pozwala na ustalenie, jak dany produkt działa, oraz na sprawdzenie, dlaczego dany mechanizm nie zadziałał, czyli dlaczego niektóre produkty zawodzą[27]. Oceniając brak wystarczającej wiedzy, należy określić luki między obecną rzeczywistością (stanem oceny funkcjonowania nieformalnej organizacji) a pożądaną przyszłością (wypełnieniem wiedzy o niej w celu określenia sił i środków do dokonania jej optymalnej neutralizacji). Podstawowym produktem wyjściowym

[25] B. Hendricks, *Reverse Engineering*…

[26] Zob. T. Kurzynowski i in., *Proces inżynierii odwrotnej*…, s. 42–46.

[27] Zob. oceny dokonane przez Colina Gagga, wykładowcę inżynierii sądowej na Open University w Milton Keynes w Anglii. C. Gagg, *Domestic product failures – Case studies*, „Engineering Failure Analysis" 2005, nr 5.

będzie w tym przypadku konstrukt[28] organizacji przestępczej, której „wytwórcą" pozostaje analityk lub inny funkcjonariusz organów ścigania dokonujący rozpoznania nie tylko konkretnych przestępstw, lecz także nieformalnej struktury mającej wpływ na rodzaj dokonywanych działań przestępczych, ich wykonawstwo oraz ich rezultat[29].

Źródłem wiedzy o samej organizacji, jej wewnętrznym zarządzaniu, podziale ról i przypisaniu przestępstw do konkretnych sprawców pozostają zarówno osoby fizyczne, jak i techniczne instrumenty analityczne i rejestracyjne będące w dyspozycji organów ścigania. Nie zawsze zasób pozyskanej wiedzy pozwoli na ustalenie, jak działa taka organizacja. Zwłaszcza gdy charakteryzuje się ona wysokim stopniem tajności, strukturą chroniącą przywódców, zleceniodawców oraz decydentów, a także gdy organy ścigania mają niepełną wiedzę na temat liczby przestępstw popełnionych przez tę organizację. Pomocne może być rozwiązanie w zakresie zarządzania zasobami ludzkimi (ang. *human resources*, HR) dla organizacji biznesowych, które zaproponowała firma ProSky. Według niej do oceny organizacji (w sensie struktury zarządczej) przyjęcie typowego schematu organizacyjnego typu „góra–dół" nie jest rozwiązaniem uniwersalnym, a próba zmuszenia firmy do przestrzegania tych standardów nie jest skuteczna. Zamiast tego zaproponowano podjęcie czynności od dołu organizacji i kontynuowanie działania „w górę", tworząc najpierw ścieżki dla każdego pracownika w organizacji. Po wprowadzeniu tych ścieżek schemat organizacyjny jest poddawany inżynierii wstecznej na podstawie potrzeb konkretnej firmy i prawdziwej struktury władzy[30].

Należy również odróżnić pojęcie i n ż y n i e r i a s ą d o w a (kryminalistyczna) od pojęcia i n ż y n i e r i a o d w r o t n a. Pojęcie „inżynieria sądowa" jest związane z prowadzonym postępowaniem i zastosowaniem metod kryminalistycznych, np. kryminalistyki cyfrowej (ang. *digital forensic*), i polega na przeprowadzeniu badań śladów pozostawionych w wyniku aktywności sprawcy (przypuszczenie, że ślady pozostawił sprawca) lub zaniechania przez niego dokonania przestępstwa. Tym samym materiał dowodowy pozostaje bez zmian i kolejno podlega różnego rodzaju badaniom w celu przyporządkowania śladu do określonego sprawcy bądź odtworzenia przebiegu zdarzenia przestępczego. Te czynności są realizowane na potrzeby postępowania prowadzonego przed prokuratorem lub sądem. „Inżynieria odwrotna", jako pojęcie znacznie szersze

---

[28] Pewna abstrakcyjna, logiczna całość złożona z danych elementów (przyp. red.).

[29] W rzeczywistości w działaniach operacyjnych służb realizuje się zadanie polegające na sporządzeniu równoległej rekonstrukcji organizacji przestępczej, która jest rozpoznawana lub rozpracowywana. Taka rekonstrukcja może dotyczyć zarówno jej nazwy, przywódców, zakresu działania, utrzymywania kontaktów z otoczeniem, używanych środków łączności, jak i przypisania poszczególnych przestępstw członkom tej organizacji jako sprawcom. Niestety, tego rodzaju czynności analityczne są konsekwencją pozyskiwania informacji od innych funkcjonariuszy (np. na podstawie błędnych informacji od osobowego źródła, niewłaściwego zakwalifikowania meldunku informacyjnego, braku doświadczenia w czynnościach zawodowych) albo w związku z działaniami na danych świadomie obarczonych błędami, np. w celu ukrycia rzeczywistego przywództwa organizacji lub pośrednich decydentów w sieci.

[30] D. Chen, *Reverse-engineering the Org Chart*, ProSky, 19 XII 2020 r., https://talkingtalent.prosky.co/articles/reverse-engineering-the-org-chart [dostęp: 21 XII 2020].

niż pojęcie „inżynieria kryminalistyczna", jest metodą badawczą, która może, ale nie musi, służyć celom postępowania przygotowawczego. Nie jest ona zatem ograniczona ramami zarówno postępowania karnego (w tym metodyki postępowania biegłych w trakcie prowadzonej ekspertyzy), jak i skonkretyzowanej oceny w danej sprawie, chyba że zostanie w tym celu wykorzystana. Nie oznacza to jednak, że w zakresie zastosowania RE występuje pełna dowolność. Po pierwsze, zastosowanie RE przez odpowiednie organy musi odbywać się w granicach prawa. Dotyczy to zarówno ram postępowania, jak i określonego celu, który ma być osiągnięty. Po drugie, inżynieria odwrotna jest związana ze skonstruowanym już urządzeniem, opracowaniem technicznym jego funkcjonowania bądź z faktami, które już wystąpiły i zostały poddane badaniu. Inżynieria kryminalistyczna polega zazwyczaj na: odzyskiwaniu niepowiązanych obiektów systemu plików (np. usuniętych plików) czy odzyskiwaniu przez pamięć podręczną historii przeglądania i jest zwykle wykorzystywana, aby wyegzekwować prawo. Natomiast RE polega na określeniu, według jakich zasad działa produkt. W tym celu przegląda się pliki binarne (lub pliki wykonywalne), a następnie wskazuje wzorce, dekompilacje[31] plików binarnych wykonywalnych, służące określeniu intencji kodu czy przeglądaniu skrzynek. Celem jest ustalenie nominalnego zachowania w odniesieniu do danych[32]. Inżynieria odwrotna analizuje kod lub plik binarny pliku (systemu) i pokazuje, w jaki sposób jest on skonstruowany i jak działa. Zwykle RE jest stosowana do celów interoperacyjności[33]. Podsumowując, inżynieria kryminalistyczna wskazuje na to, kto i jak czegoś dokonał, a inżynieria odwrotna – jak to działa. Dlatego też inżynieria odwrotna odnosi się raczej do instrumentu, jaki został użyty, niż do tego, kto go używał.

Inżynieria odwrotna ma także swoje zastosowanie w działaniach antyterrorystycznych i antykryzysowych, a zwłaszcza w ocenie praktyki analizy wywiadowczej i prawidłowości reagowania na zagrożenie. Informacje, które się wykorzystuje, to przede wszystkim „twarde dane", np. data wjazdu do kraju, identyfikacja osób zajmujących się obsługą i komórkami logistycznymi (zapleczem terrorystycznym zapewniającym bezpieczeństwo przed dokonaniem zamachu), zarządzanie komunikacją i informacją, identyfikacja podmiotów, które dostarczyły fałszywe dokumenty tożsamości, identyfikacja kierownictwa i najważniejszego członka grupy terrorystycznej, używanej poczty elektronicznej, ustalenie liczby rekrutowanych młodych ludzi, szczegółów dotyczących przyszłych ataków. Te dane powinny być przydatne do rozpracowania sieci terrorystycznej, metod jej finansowania i zakłócenia tego procederu, identyfikacji sieci, a w konsekwencji – do aresztowania członka komórki logistycznej oraz doprowadzenia do uniknięcia zrealizowania zamachu. Traktując RE jako (…) *proces pozyskiwania informacji o fizycznym produkcie oraz*

---

[31] Odtworzenie postaci źródłowej programu na podstawie jego kodu wynikowego (przyp. red.).

[32] Chodzi tu o ustalenie wartości wielkości fizycznych charakterystycznych dla jakiegoś urządzenia, maszyny itp.

[33] Forum dyskusyjne, odpowiedź udzielona Pranitowi Kothariemu na pytanie: *What is difference between Digital Forensic and Reverse Engineering?*, https://stackoverflow.com/questions/18289773/what-is-difference-between-digital-forensic-and-reverse-engineering [dostęp: 14 IV 2020].

ich analizowania i przetwarzania w celu opracowania technicznych danych i wytworzenia nowego produktu w takiej samej bądź ulepszonej postaci[34], można zauważyć, że pozostaje ona mocniej związana z kryminalistyką badającą obiekty fizyczne niż z zachodzącymi zjawiskami przestępczymi. Wynika to prawdopodobnie ze zadecydowanie łatwiejszego włączenia konstrukcji fizycznego przedmiotu w określony schemat podlegający następnie badaniu (szczególnie przez zebranie wielu danych technicznych, które można zmierzyć, o właściwościach oraz konstrukcji przedmiotu), ale też z posiadania odpowiednich narzędzi i dokonania precyzyjnego zmierzenia badanych obiektów[35]. Dlatego też ważne jest zabezpieczanie przez organy ścigania urządzeń wykorzystywanych np. przez terrorystów do wzajemnego komunikowania się, pozyskiwania z zewnątrz środków finansowych na działalność, koordynowania zaplecza logistycznego czy przygotowania i organizacji zamachu terrorystycznego. Zwłaszcza gdy dane urządzenie zostaje przerobione na potrzeby terrorystyczne lub od początku jest świadomie wykonane w tym celu.

Inżynieria odwrotna pozwala na szczegółowe rozpracowanie schematu funkcjonowania istniejącego urządzenia albo skonstruowanie nowego, które jednocześnie stanie się mechanizmem wewnętrznego rozpoznania aktywności terrorystycznej (np. przez zamianę urządzenia na takie samo, ale kontrolowane przez organy ścigania w ramach zastosowania techniki operacyjnej). Może to ułatwić zgromadzenie śladów potrzebnych do badań kryminalistycznych lub wykorzystanych później jako materiał dowodowy w prowadzonym postępowaniu karnym bądź jako przedmiot badań biegłego. Wydaje się więc, że istnieje możliwość wykorzystania RE zarówno w taktyce śledczej (jako określony i zastosowany w danej sprawie plan działania organu ścigania, decydujący o wyborze konkretnych, najlepszych i najodpowiedniejszych środków technicznych), jak i w analizie taktyki przestępczej, czyli sposobu popełnienia przestępstwa przez sprawcę (sposoby, metody i środki przestępczego działania). Ten drugi obszar odnosi się bardziej do podejmowania działań w zakresie czynności operacyjno-rozpoznawczych. Poddany analizie „przedmiot–model" może być niekompletny, gdyż nie będzie można wprowadzić do niego np. danych o stanach emocjonalnych sprawcy, a także nie będzie możliwe pozyskanie pełnej wiedzy o przygotowaniu do popełnienia przestępstwa. Jednak szeroki wachlarz zarówno instrumentów śledczych, jak i przedmiotów lub programów używanych przez sprawcę powinien pozwolić na zbudowanie modelu na tyle kompletnego, że będzie go można odtworzyć na poziomie RE (podobnie jak przy odtworzeniu mechanizmu bez możliwości wglądu w jego rysunek konstrukcyjny i instrukcję obsługi). Przy wykonywaniu określonych czynności wykrywczych jest możliwe zaistnienie elementów indywidualnych zachowań osób realizujących te czynności, co może skutkować subiektywnym charakterem działań podejmowanych wobec przestępców. Jest to sytuacja podobna do

---

[34] M. Szelewski, M. Wieczorowski, *Inżynieria odwrotna i metody dyskretyzacji obiektów fizycznych*, I Krajowa Konferencja Naukowa „Szybkie prototypowanie. Modelowanie-Wytwarzanie-Pomiary", Rzeszów–Pstrągowa, 16–18 września 2015 r., „Mechanik" 2015, nr 12, s. 183.

[35] Należy wziąć pod uwagę także wysoki poziom wykorzystywanych metod konspirowania działań, posługiwanie się fałszywymi tożsamościami, stosowanie kodu, szyfracji lub szczególnego dialektu podczas porozumiewania się ze sobą osób należących do sieci.

tej, gdy przy odtwarzaniu określonego przedmiotu brakuje jakiegoś jego elementu i musi on zostać wykonany ręcznie ze względu na brak innych możliwości działania.Tym samym istnieje duże prawdopodobieństwo wykonania go w sposób niedoskonały. Pomocna staje się wówczas digitalizacja działania i jego automatyzacja, którą zapewnia RE.

Analogicznie jest w przypadku prowadzenia czynności wykrywczych. Przy ich realizacji może bowiem dojść do podjęcia działań rutynowych lub błędnych, a w ich konsekwencji – do przedwczesnego zamknięcia sprawy i wyjaśnienia jej w sposób niepełny. Dlatego też retrospekcyjne odwzorowanie zachowań indywidualnych lub organizacyjnych z zastosowaniem RE powinno dać asumpt do weryfikacji zrealizowanych działań, szczególnie gdy dotychczasowe czynności zakończyły się niepowodzeniem (np. nieobecność osoby w miejscu planowanego zatrzymania, niewłaściwe ustalenie zdeponowania środków w instytucji finansowej, nieprawidłowe wytypowanie miejsca i czasu dokonania przestępstwa). Do złego wytypowania może dojść, gdy istotna część procesu wykrywczego zostanie zrealizowana na podstawie modelu technicznego (analitycznego, programistycznego, predykcyjnego) w połączeniu z oceną zachowań i propozycją rozwiązań. Inżynieria odwrotna pozwala na obiektywne, oparte na informacjach o zaistniałych faktach połączonych z przestępcą, odtworzenie i ustalenie zachowania sprawcy przestępstwa w warunkach jemu przynależnych i z wytypowanym dla niego sposobem postępowania i analizy sytuacyjnej. Może być przydatna w różnych sytuacjach, także tych, w których zakłada się powtarzalność działania przestępcy (np. stosowanie przez niego takiej samej taktyki podczas napadu na kantory, okradania bankomatów czy mieszkań), wobec seryjnych morderców czy przy analizowaniu niewykrytych spraw (tzw. Archiwum X). Można ją ponadto zastosować w odniesieniu do zachowań przestępczych i taktyki zwalczania przestępczości. Warto się także zastanowić, czy można skorzystać z RE w przypadku procesów decyzyjnych i zdarzeń będących następstwem przyczynowo-skutkowym oraz reguł postępowania lub niezorganizowanego (spontanicznego) działania. Wydaje się, że jest ona dopuszczalna i stanowi „wsteczne" śledztwo, czyli daje możliwość rozebrania na elementy cząstkowe działań bardziej skomplikowanych, podlegających ocenie. Im w działaniach sprawcy przestępstwa jest mniej precyzji i obowiązujących reguł, a więcej przypadkowości, tym mniejsza możliwość zastosowania RE. Nie oznacza to jednak, że jeśli w wyniku analizy odwrotnej zostanie stwierdzony przypadek związany nie tyle z nieprzestrzeganiem reguł (których może nawet nie być), ile z przypadkowością, to przedmiotowe zdarzenie nie może być odpowiednio ocenione. Trzeba sprawdzić, czy reguła postępowania pozwalała na dowolność, czy też ten obszar stanowił nieuregulowaną lukę, której konsekwencji nie przewidziano, np. luki nie wykrył projektant (programista), a zrobiła to osoba postronna, którą był sprawca nieprawidłowości[36].

Inżynierię odwrotną stosuje się wobec tych zdarzeń, które można w jakiś sposób opisać cyfrowo. Dlatego też dane analogowe należy zamienić w postać cyfrową,

[36] Za nieprawidłowość nie należy przyjmować naruszenia, gdyż nie było co naruszać, a osiągnięcie nieprawidłowego stanu przez wykorzystanie luki.

co umożliwia umieszczenie ich w pamięci komputera. Nie można jednak twierdzić, że jedynie te dane, które będzie można skwantyfikować, mogą zostać wykorzystane w inżynierii odwrotnej. Z pewnością takie dane przysłużą się sprawnemu przeprowadzeniu postępowania. Takie procesy, jak zachowania przestępcze lub taktyka sprawców przestępstw, niekoniecznie rządzą się regułami matematycznymi i są bardziej skomplikowane, niż przewidywano. Zarówno te czynniki, jak i powtórna analiza zdarzenia rozłożonego na poszczególne elementy powinny być przyczynkiem do zbudowania nowego modelu przeciwdziałania, bardziej odpornego na aktywność przestępców i zwiększającego obiektywizm analityka kryminalnego.

Metody RE można wykorzystać do:

- oceny funkcjonalności, skuteczności oraz sposobów posługiwania się urządzeniami fizycznymi (programami) wykorzystywanymi w celach przestępczych (środki łączności, gry komputerowe, konsole, urządzenia zdalne itp.);
- prowadzenia gry operacyjnej przy wykorzystaniu urządzeń będących w dyspozycji przestępców (np. w Darknecie);
- pozyskania wiedzy z autorskich programów lub z modyfikacji programów dedykowanych wyłącznie działaniom grupy przestępczej (demontaż binarny);
- przeprowadzenia analizy niekompletnego materiału dowodowego, zwłaszcza dotyczącego wykorzystania złożonych narzędzi przestępstwa (np. oprogramowania);
- wykorzystania rynkowych instrumentów dysponowania aktywami, którymi posługują się przestępcy zgodnie z przyjętym celem kryminalnym;
- badania, kontrolowania i nadzorowania naruszeń w zakresie procedur księgowych (bilansowych) dotyczących pozyskiwania aktywów, prania pieniędzy oraz finansowania terroryzmu, zwłaszcza procedur realizowanych przy wsparciu ze strony profesjonalnych programów księgowych;
- udoskonalania stosowanych badań kryminalistycznych (w tym przy użyciu metod statystycznych);
- badania naruszeń procedur *compliance* w celu wykorzystania podmiotów gospodarczych do działań przestępczych (chodzi o zgodność działalności z normami, zaleceniami lub stosownymi praktykami);
- budowania systemów monitoringu społeczności internetowych;
- zwiększenia skuteczności analiz kryminalnych dotyczących funkcjonowania sieciowych organizacji przestępczych i terrorystycznych;
- ponownego przeanalizowania elementów w ramach prowadzenia przez organy ścigania różnych baz danych na potrzeby skuteczniejszego kojarzenia faktów pomocnych w typowaniu sprawców przestępstw;
- udoskonalenia prowadzenia taktyki śledczej, w tym w obszarze cyberprzestrzeni;
- odzyskania utraconych dowodów w sprawie lub zlokalizowania ich w miejscach dotychczas nietypowanych;
- walidacji oceny wytypowania rzeczywistego przywództwa i ważnych (pośrednich) węzłów w sieci przestępczej;
- weryfikacji wartości diagnostycznej.

Etapy procesu inżynierii odwrotnej wykorzystanej w analizie sieci przestępczych

Pierwszym etapem RE jest pozyskanie danych i analiza informacji, w tym uzyskanie modelu produktu (którym w tym przypadku jest obiekt – Podmiot A) do dalszej analizy, zawierającego również identyfikację krytycznych elementów tego produktu (dyskretyzacja[37]). W wyniku digitalizacji dane o charakterze analogowym zostają przekształcone w dane cyfrowe, które będzie można dalej przetwarzać przy wykorzystaniu programów komputerowych. Kolejne etapy RE to: opracowanie i weryfikacja oraz odzyskanie projektu utrzymanego i pochodzącego z fazy wdrażania i fazy projektowania. Proces wymaga zdefiniowania nowych oraz zmodyfikowania już istniejących wymagań dla produktu docelowego (przeprojektowanie).

Pierwszy etap jest decydujący dla przebiegu pozostałych faz, w których analitycy skupiają się na przetworzeniu pozyskanych danych, odpowiednio do wyznaczonego celu. Uzyskanie danych, gdy opracowuje się przedmiot fizyczny, nie powinno być trudne. Inaczej jest w przypadku zdarzeń, które nie są podporządkowane regułom technicznym (w takiej sytuacji należałoby mieć na uwadze potrzebę zastosowania indywidualnej metody postępowania, adekwatnej do zaistniałego problemu). W ramach procesu RE jest możliwe wystąpienie tzw. nacjonalizacji, czyli przejęcia cudzego produktu w celu uzyskania produktu krajowego (na własne potrzeby) z jednoczesnym pominięciem procedur patentowych i zastrzeżeń co do ochrony własności intelektualnej twórców urządzenia[38]. Z tego względu część działań może być podejmowana niezgodnie z prawem. W niektórych przypadkach osoby realizujące zadania inżynierii odwrotnej powinny być chronione kontratypami[39]. Może między innymi zaistnieć sytuacja, że analizowane urządzenie zostało stworzone przez wytwórcę działającego niezgodnie z przepisami prawa. Ponadto nowy produkt, mimo szerokiego odwzorowania (bez uzyskania autoryzacji), będzie miał po przetworzeniu wysoki poziom autonomizacji.

---

[37] Dyskretyzacja – pojęcie dotyczące procesu transformowania modeli i równań funkcji ciągłych na ich dyskretne odpowiedniki. Jest to zwykle pierwszy krok w procesie przygotowywania tych modeli (i równań) do ewaluacji numerycznej i implementacji na komputerach cyfrowych, za: Wikipedia, https://pl.wikipedia.org/wiki/Dyskretyzacja_(matematyka) [dostęp: 5 II 2021] – przyp. red.

[38] Nie będzie to wchodziło w grę, gdy „twórcą" projektu, urządzenia, programu będzie osoba współpracująca z organizacją przestępczą, członek tej organizacji, mający pełną świadomość przydatności opracowanych rozwiązań technicznych w realizacji celu przestępczego.

[39] W ustawodawstwie amerykańskim: zgodnie z sekcją 103 (f) ustawy *Digital Millennium Copyright Act* [17 USC § 1201 (f)] osoba będąca w posiadaniu programu może przeprowadzić proces inżynierii wstecznej i obejść jego ochronę, jeśli jest to konieczne do osiągnięcia „interoperacyjności". Istnieje ograniczone wyłączenie, które pozwala na dzielenie się zdobytą w ten sposób wiedzą i wykorzystywanie jej do celów interoperacyjności. Zob. hasło: inżynieria odwrotna, https://pl.qaz.wiki/wiki/Reverse_engineering#Source_code [dostęp: 15 II 2021]. W Unii Europejskiej obowiązuje: *Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych* (Dz. Urz. UE L 111 z 5 V 2009 r.), s. 16, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32009L0024 [dostęp: 15 II 2021].

We wszystkich tych przypadkach czynności podejmowane w ramach RE powinny być uznane za prawnie dopuszczalne.

Wykorzystanie RE wobec form organizacyjnych przestępczości można rozważyć pod kątem rozpoznania szczegółów kodu działania przestępców. Oznacza to możliwość ustalenia poszczególnych elementów, etapów i sposobów zarządzania w organizacji, które się przekładają na przygotowanie i dokonywanie konkretnych przestępstw oraz na zbudowanie zaplecza logistyczno-finansowego dla struktur organizacyjnych. Jest to część wiedzy, której organy ścigania nie będą mogły zdobyć w wyniku takich działań operacyjnych, jak: współpraca z osobowymi źródłami informacji, stosowanie techniki operacyjnej czy pozyskanie wiedzy z operacji specjalnej. Dzięki temu będzie można rozpoznać kod występujący zarówno na poziomie operacyjnym (wykonawczym), jak i na poziomie zarządzania strategicznego. Kod działania przestępców to głównie wiedza, którą dysponuje niewielka liczba osób, przede wszystkim ścisłe kierownictwo organizacji przestępczej.

Zastosowanie procesu inżynierii odwrotnej ma na celu: rozpracowanie oprogramowania, poradzenie sobie ze złożonością zadania, wygenerowanie alternatywnych rozwiązań, odzyskanie utraconych informacji, wykrycie skutków ubocznych działania oraz synteza na wyższym poziomie abstrakcji. Są to ogólne cele, które można uzupełnić tymi, które bezpośrednio wiążą się z przeciwdziałaniem przestępczości. Zalicza się do nich:

- poznanie oprogramowania opracowanego i stosowanego przez przestępców;
- poznanie sposobów wykorzystania powszechnie dostępnego oprogramowania do popełniania przestępstwa;
- zdobycie wiedzy o wewnętrznym oprogramowaniu używanym w instytucji wykorzystanej do dokonania przestępstwa;
- zdobycie wiedzy na temat szczegółów konstrukcyjnych urządzeń służących do dokonania przestępstwa;
- zdobycie wiedzy na temat konfiguracji wielu instrumentów finansowych, biznesowych i prawnych przygotowanych przez przestępców do wygenerowania zysku przestępczego, zalegalizowania środków finansowych czy zapewnienia wsparcia finansowego organizacjom terrorystycznym;
- uzyskanie produktu umożliwiającego śledzenie (monitorowanie) przedsięwzięć przestępczych bez wiedzy zainteresowanych;
- przeprowadzenie testu oprogramowania (algorytmu) przyjętego jako „bramka" lub „czerwona flaga" dla instytucji w celu zabezpieczenia jej klientów przed przestępstwem, szczególnie gdy takiego zabezpieczenia nie było;
- uniemożliwienie wykorzystania produktu do popełnienia przestępstwa.

Do czynników, które mogą oddziaływać na replikację (odwzorowanie) produktu, można zaliczyć m.in.:

- posiadanie oryginalnego obiektu stanowiącego przedmiot badań inżynieryjnych – ważne jest poznanie konstrukcji, mechanizmu działania oraz rodzaju materiału, z jakiego został on wykonany. Jest to istotne przede wszystkim

ze względu na potrzebę jak najdokładniejszego odwzorowania danych, których przedmiotowy produkt jest nośnikiem;
- tolerancja – zaakceptowanie odchyleń w dokonanych pomiarach;
- dokładność – potrzeba zapewnienia jak najbardziej precyzyjnego dokonania pomiarów, tak aby spełnić założony cel nowego produktu (dotyczy to zarówno całościowego odzwierciedlenia istniejącego przedmiotu, jak i uzyskania zmodyfikowanej konstrukcji);
- podejście pomiarowe – potrzeba dobrania odpowiedniego urządzenia pomiarowego, aby właściwie zidentyfikować dane produktu;
- cel – czyli główne założenie zastosowania RE, a także sprawdzenie, do czego ostatecznie posłuży zastosowanie inżynierii odwrotnej (np. uzyskanie odpowiedzi na pytania, jak ten produkt działa i co poszło nie tak lub co mogło pójść źle w jego działaniu)[40].

Podczas stosowania procesu RE trzeba zwrócić uwagę na następujące zasady, a także pojawiające się problemy:
- nie należy mylić hipotez z wnioskami. Inżynieria odwrotna pozwala na otrzymanie hipotezy, dlatego też trzeba dokładnie zrozumieć aplikację, zanim będzie można wyciągnąć jednoznaczne wnioski;
- należy się spodziewać wielu interpretacji, ponieważ nie ma tu jednej odpowiedzi, jak w inżynierii postępowej (tradycyjnej). Alternatywne interpretacje struktury i informacji zaczerpniętych z baz danych mogą przełożyć się na otrzymanie różnych modeli;
- nie należy zniechęcać się wynikami przybliżonymi. Trzeba dążyć do wydobycia z baz danych jak największej liczby informacji (co najmniej 80 proc.). Można użyć typowych technik inżynierii postępowej (takich jak przeprowadzanie wywiadów z użytkownikami mającymi wiedzę na ten temat), aby uzyskać pozostałe 20 proc. Wiele osób uważa ten brak doskonałości za niewygodny, ponieważ jest to zmiana paradygmatu w stosunku do inżynierii postępowej;
- należy spodziewać się uzyskania nietypowych konstrukcji. Projektanci baz danych, a także eksperci, używają czasami nietypowych konstrukcji. W niektórych przypadkach nie ma możliwości stworzenia kompletnego, dokładnego modelu bazy danych, ponieważ taki model nigdy nie istniał;
- należy utrzymać spójny styl. Bazy danych są zwykle projektowane przy użyciu spójnej strategii, w tym spójnej realizacji dobrych praktyk projektowych. Dzięki temu powinno się wywnioskować podstawową strategię[41].

---

[40] Zob. M. Knicker, *What Are The Types of Reverse Engineering and Why Does it Matter?*, Q-Puls Labs, Dimensional Measurement Blog, 8 XI 2012 r., https://www.qpluslabs.com/blog/what-are-the-types-of-reverse-engineering-and-why-does-it-matter/ [dostęp: 15 IV 2020].

[41] M.R. Blaha, *Reverse Engineering for Product Assessment*, informIT, 13 X 2001 r., https://www.informit.com/articles/article.aspx?p=23692&seqNum=6 [dostęp: 18 XII 2020]. Zob. także: tenże, *A Manager's Guide to Database Technology. Building and Purchasing Better Applications*, wyd. 1, [bmw] 2000.

Inżynieria odwrotna może znaleźć zastosowanie w odniesieniu zarówno do dziedziny programowania, jak i do opracowanych procedur postępowania w zakresie monitoringu i przeciwdziałania przestępczości, z uwzględnieniem m.in. transakcji finansowych, procedur rozpracowania grup przestępczych, taktyki działania organów ścigania i badań kryminalistycznych. Jako przykład można podać zagadnienia związane z procesem decyzyjnym przywódców organizacji, księgowością śledczą, wewnętrznymi procedurami instytucji obowiązanych dotyczącymi przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, procedurami *compliance* i przeciwdziałaniem oszustwom oraz nieprawidłowościom na szkodę instytucji finansowych. Podczas stosowania metody RE niezbędne jest rozdzielnie zdarzeń (transakcji) na podstawowe części oraz wywnioskowanie na podstawie przyjętego modelu postępowania, jakie elementy nie zadziałały, zadziałały nieskutecznie lub zadziałały w celu innym niż założony w projekcie (czyli np. posłużyły dokonaniu przestępstwa). Jest to zarazem proces zmierzający do uzyskania „kodu decyzyjnego".

Stworzony model jest stosowany przede wszystkim w instytucjach komercyjnych w celu wypracowywania zysków (podobnie jak w organizacji przestępczej). Przy realizacji wyznaczonego zadania mogą być wykorzystywane także inne modele, które stanowią wsparcie lub spełniają funkcję kontrolną czy rozliczeniową (mogą one być wprowadzane niezależnie od przyjętego modelu). Dla przykładu, model sposobu sprzedaży produktu będzie wsparty modelem rozliczeniowym, pomocnym – zgodnie z zasadami księgowania i przyjętego planu kont – przy rozliczeniu produktu między kontrahentami. Dzięki temu będzie możliwe wygenerowanie informacji, jak dany produkt jest przyjmowany przez klientów lub wykorzystywany w sposób niezaplanowany w strategii sprzedaży. W przypadku modelu przestępczego cel dotyczący dysponowania środkami będzie inaczej konstruowany i będzie uzależniony od głównego celu organizacyjnego. Stąd też istnieje możliwość zidentyfikowania innego zarządzania aktywami niż to, które jest charakterystyczne dla modelu inwestycyjnego „prawego klienta". Aby prawidłowo i efektywnie wykorzystać inżynierię odwrotną, już na wstępie projektowania określonych rozwiązań w instytucjach, które będą chciały zaakceptować te rozwiązania i wdrożyć je do swojej strategii sprzedażowej, niezbędne będzie przyjęcie ścisłej i precyzyjnej reguły (schematu) postępowania z danym produktem. Będzie to np. umieszczenie w nim „czerwonych flag", które będą świadczyć o jego wykorzystywaniu niezgodnym ze strategią produktu lub z prawem. Produkt powinien zostać zaopatrzony w szczegółową instrukcję postępowania z nim, co pozwoli – w ramach działań wstecznych – na uzyskanie modelu porównawczego wobec rozpatrywanego, ocenianego przypadku.

Przy korzystaniu z RE należałoby rozpatrzyć przynajmniej dwa tryby postępowania. Pierwszy odnosiłby się do oceny reguł postępowania z produktem i klientem występujących w danej instytucji. Drugi zaś do skonfrontowania konkretnej sytuacji z trybem „ostrzegawczym", uplasowanym w obszarze bezpieczeństwa instytucji (uzyskanym np. na podstawie przeprowadzonej analizy ryzyka). Im reguły postępowania są bardziej szczegółowe i doprecyzowane, tym skuteczniej będzie można zwrotnie ocenić

produkt w odniesieniu do oddziałujących na niego czynników i torów zgodnościowych tego postępowania (w tym objętych elementami zasad *compliance*). Zastosowanie RE w dziedzinie finansów wiąże się z potrzebą oceny zakresu i sposobu wykorzystania instrumentów finansowych (najczęściej publicznie dostępnych) w kontekście nielegalnego pozyskania aktywów, legalizowania środków pochodzących z czynów zabronionych, dystrybucji i redystrybucji aktywów w ramach sieci przestępczej oraz monitorowania „zachowań finansowych" jako zwiastunów ataków terrorystycznych.

Przedstawiona propozycja zastosowania RE odnosi się do spraw związanych z zasileniem aktywami finansowymi organizacji przestępczej (terrorystycznej). Prowadzono również badania, które dotyczyły ścisłego procesu decyzyjnego w ramach samej organizacji[42]. Za pomocą metody analizy decyzji (ang. *applied decision analysis,* ADA) zbadano procesy decyzyjne przywódców takich organizacji, jak: Al-Kaida, Hamas i Hezbollah. Identyfikacja sposobów podejmowania przez nich decyzji pozwoliła na przyjęcie taktyki najbardziej adekwatnej do stawianego celu zadania (różnej fazy aktywności) i skutecznej w przeciwdziałaniu terroryzmowi. W badaniu wykorzystano wiele modeli decyzyjnych (np. eliminację według aspektów[43], leksykograficznego[44], poliheurystycznego[45] lub maksymalizacji użyteczności[46]).

Wykorzystanie procesu RE w badaniu taktyki przestępczej będzie polegać na prześledzeniu aktywności sprawcy, tj. tego, w jaki sposób rozwiązywał dane problemy (sytuacje) na określonym etapie postępowania przestępczego. Inżynieria odwrotna znajdzie zastosowanie przede wszystkim w przypadku wielowymiarowego i wieloinstrumentalnego postępowania sprawczego, a nie działań prostych, łatwo rozpoznawalnych. Chodzi o rozbudowane formy przestępczości, które same w sobie są czynem sprawczym o dużej złożoności, jak np. przestępstwa finansowo-gospodarcze, proceder prania pieniędzy czy państwowy sponsoring działań terrorystycznych.

---

[42] Zob. szerzej: J.T. Chatagnier, A. Mintz, Y. Samban, *The Decision Calculus of Terrorist Leaders*, „Perspectives on Terrorism" 2012, nr 4–5, s. 125 i nast., https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2012/issue-4/the-decision-calculus-of-terrorist-leaders-j.tyson-chatagnier-alex-mintz-and-yair-samban.pdf [dostęp: 20 XII 2020].

[43] Model związany ze sposobem podejmowania decyzji. Polega on na tym, że wybiera się jakąś cechę-aspekt (która jest akceptowana lub nie) i dokonuje się przeglądu dostępnych opcji, eliminując te, które nie spełniają tego wymagania. Zob. T. Tyszka, *Analiza decyzyjna i psychologia decyzji*, Warszawa 1986; J. Kozielecki, *Psychologiczna teoria decyzji*, Warszawa 1977.

[44] Reguła leksykograficzna – wybierany jest wariant, który pod względem najważniejszej cechy jest najlepszy. Jeśli między wariantami zachodzi równość, porównuje się następne pod względem hierarchii cechy. Zob. M. Wójcik, *Proces podejmowania decyzji w przedsiębiorstwie*, wyd. 1, 2009, s. 16, e-book.

[45] Zob. T. Pawluszko, *Poliheurystyczna teoria podejmowania decyzji w analizie bezpieczeństwa*, „Colloquium Pedagogika – Nauki o Polityce i Administracji" 2020, nr 1, https://colloquium.amw.gdynia.pl/index.php/colloquium/article/view/164/157 [dostęp: 15 II 2021].

[46] Zob. B. Polanowska-Sygulska, *Użyteczność a maksymalizacja bogactwa: Filozoficzne zakorzenienie poglądów Chicagowskiej szkoły law & economics*, „Archiwum Filozofii Prawa i Filozofii Społecznej" 2011, nr 1, s. 5–14; O. Kapliński, *Drzewa decyzyjne i użyteczność decyzji*, http://sipb.sggw.pl/Monografia_2015/Strony%20odRekomendowane_metody-11.pdf [dostęp: 15 II 2021].

Będzie można ją wykorzystać zwłaszcza w rozpracowywaniu zorganizowanych grup przestępczych oraz ugrupowań (organizacji) terrorystycznych. Dzięki RE będzie można uzyskać wieloźródłowy i wielodecyzyjny obraz zarządzania w celu wygenerowania informacji o przygotowaniu i dokonaniu przestępstwa. Ocenie mogą być poddane: treść decyzji, szybkość jej wydania i realizacji, personalny dobór wykonawców jej treści, personalny dobór adresatów (gradacja dostępu do skali informacji). Inną kategorią spraw badanych w ramach RE będą te przestępstwa, przy których popełnianiu wykorzystuje się elektroniczne platformy atakowanych podmiotów, np. przestępstwa giełdowe, przestępstwa w bankowości elektronicznej lub dotyczące kryptowalut. Zadaniem do zrealizowania będzie rozbicie na czynniki pierwsze procesu decyzyjnego opartego na doborze sprawców oraz osób kontrolujących przebieg przestępstwa, umiejscowieniu działania w zakresie geograficznym i wirtualnym, a także podjęcie – na określonym etapie – decyzji o skorzystaniu ze współpracy z innym podmiotem przestępczym bądź wykorzystaniu firmy zarejestrowanej w strefie *offshore* (tzw. rajach podatkowych – dop. red.) itp.

W modelu odtworzeniowym należy założyć racjonalność (a nie chaos) w postępowaniu sprawcy. Zadaniem inżyniera-kryminalistyka, chcącego skorzystać z metody RE, jest zdobycie wiedzy o takim przebiegu zdarzeń, które spowodowało zmianę planowanej taktyki przestępczej i podjęcie decyzji np. o nierealizowaniu w ustalonym czasie określonych przedsięwzięć lub o posłużeniu się innymi instrumentami w realizacji przestępstwa[47]. Łatwo będzie tym samym wykryć słabe punkty w procesie decyzyjnym sprawcy oraz prześledzić planowanie alternatywnych rozwiązań, które zapewniają większą skuteczność i bezpieczeństwo (tajność) działania przestępczego. Zastosowanie RE umożliwi odtworzenie kolejności zdarzeń – od ich docelowego efektu (popełnienia przestępstwa) do początku, tj. jego zaaranżowania. Badanie można będzie wykonać niezależnie od prowadzonych czynności dochodzeniowo-śledczych i na potrzeby czynności procesowych.

Dla wspomnianej metody ADA macierz decyzyjna[48] składa się z zestawu alternatyw, wymiarów (lub kryteriów) wyboru spośród tych alternatyw oraz oceny implikacji każdego wymiaru dla każdej alternatywy. Wagi (lub poziomy ważności) mogą

---

[47] Zmiana może zajść na skutek informacji uzyskanej od organów ścigania, w tym od uznanych źródeł informacji, bądź na skutek działań neutralizacyjnych podjętych przez służby niezależnie w innej sprawie czy też pod wpływem warunków niezależnych, np. odwołania lotu samolotem, wprowadzenia blokady granicy, klęski żywiołowej

[48] Macierz decyzyjna (ang. *decision matrix analysis*, DMA) to lista wartości w wierszach i kolumnach, która umożliwia analitykowi systematyczne identyfikowanie, analizowanie i ocenianie wydajności relacji między zestawami wartości i informacji. Analiza matryc decyzyjnych jest najprostszą formą analizy decyzji wielu kryteriów (ang. *multiple-criteria decision analysis*, MCDA), znanej również jako pomoc decyzyjna o wielu kryteriach lub zarządzanie decyzjami o wielu kryteriach (ang. *multiple-criteria decision making*, MCDM). Zaawansowana MCDA może obejmować wysoce złożone modelowanie różnych potencjalnych scenariuszy przy użyciu zaawansowanej matematyki, https://steemit.com/polish/@techiwebicodi/pl-podejmowanie-decyzji-przez-wazenie-roznych-czynnikow-decision-matrix-analysis-i-przyklad-wykorzystania [dostęp: 15 II 2021].

być przypisane do każdego wymiaru. Zestaw alternatyw obejmuje prawdopodobne kierunki działań decydenta (np. lidera organizacji terrorystycznej), z uwzględnieniem rozwiązań w razie wystąpienia ewentualnych problemów decyzyjnych[49]. Dzięki analizie inżynieryjnej będzie można ocenić stopnień zaawansowania organizacyjnego grupy przestępczej (rodzaj zorganizowania struktury) oraz jej uplasowanie w ramach zewnętrznych relacji z typowanymi obiektami spoza organizacji. Ostatecznym celem RE będzie pozyskanie umiejętności w zakresie szybszego i skuteczniejszego neutralizowania organizacyjnych form przestępczości, a także zastosowanie „głębokiej" analizy samej organizacji w kontekście przywództwa, relacji między członkami czy procesu decyzyjnego.

Przed zastosowaniem RE pomocne będzie rozpatrzenie analizowanej sprawy w kategoriach porządkujących. Na czynniki porządkujące prowadzone działania operacyjnie bądź równolegle do nich prowadzone postępowanie procesowe będą miały wpływ:

- prowadzenie czynności operacyjno-rozpoznawczych zgodnie z przyjętymi regulaminami i wewnętrznymi instrukcjami uprawnionych służb;
- wprowadzenie systemu pozyskiwania i kategoryzacji informacji (wartości informacji), które będą inicjacyjne wobec dalszych czynności służbowych[50];
- wprowadzenie od samego początku sprawy w reżim (w schemat) analizy kryminalnej prowadzonej zgodnie z określonymi (znanymi) silnikami analitycznymi;
- zastosowanie, również wobec informacji pozyskanych spoza służb, reguł i schematów przynależnych strukturze schematów analitycznych, przetwarzaniu i analizie, przy czym należałoby założyć potrzebę kompatybilności własnych systemów bazodanowych i analitycznych służb z bazami danych podmiotów zewnętrznych (również z wbudowanym elementem predykcyjnym);
- pozyskanie informacji o funkcjonalności działania całościowych i lokalnych matryc przeznaczonych dla społeczności internetowych;
- rozważanie wprowadzenia zindywidualizowanego programu analitycznego ze znanym silnikiem analitycznym na potrzeby danej sprawy;

---

[49] J.T. Chatagnier, A. Mintz, Y. Samban, *The Decision Calculus of Terrorist Leaders*…, s. 128.

[50] Zob. dla przykładu: *Decyzja nr 338 Komendanta Głównego Policji z dnia 12 października 2016 r. w sprawie Systemu Informacji Operacyjnych*, Dz. Urz. KGP z 2016 r. poz. 65, https://isp.policja.pl/isp/aktualnosci/prawo/9626,Decyzja-nr-338-Komendanta-Glownego-Policji-z-dnia-12-pazdziernika-2016-r.html [dostęp: 16 IV 2020]. Meldunek informacyjny sporządza się w każdym przypadku uzyskania przez policjantów informacji przydatnych do „(…) zapobiegania, rozpoznawania, ujawniania i wykrywania przestępstw, ustalania metod ich popełniania oraz wykrywania i zatrzymywania sprawców, w tym także: 1) informacji o zdarzeniach, miejscach, pojazdach, dokumentach oraz osobach fizycznych i innych podmiotach nie będących osobami fizycznymi; 2) informacji o telekomunikacyjnych urządzeniach końcowych wykorzystywanych do przekazu informacji, z wyłączeniem danych pozyskanych w trybie określonym w art. 20c ustawy o Policji; 3) informacji o rachunkach w bankach lub innych instytucjach finansowych oraz o czynnościach bankowych, z ograniczeń dostępu do tych danych wynikających w art. 20 ust. 3 i 4 ustawy o Policji".

– klasyfikacja przez ustawodawcę w przepisach karnych schematu zachowania sprawcy, które jest penalizowane jako przestępstwo;
– realizowanie zadań pozaschematycznych w przyjętym modelu systemowym, który z założenia funkcjonalnego powinien współistnieć z ogólnymi systemami i mieć na celu porządkowanie oraz kategoryzację danych (szczególnie odnosi się to do – w miarę możliwości – całościowego i spójnego wprowadzenia modelu matematycznego sieci zbudowanej z rozpoznawanych elementów, co jest niezbędne do rekonstrukcji interakcji między elementami).

Atutem ułatwiającym rozwiązywanie zagadnień w ramach analizy prowadzonej na podstawie metod RE jest bazowanie na sieciowym schemacie (m.in. graficznym) przyjętym dla danej organizacji przestępczej lub terrorystycznej, ale też dla każdego skomplikowanego taktycznego działania przestępczego[51]. Taki schemat może być kreowany zarówno w ramach analizy kryminalnej, jak i innych rozwiązań wynikających z teorii grafów czy SNA. Ważne jest, aby przez cały czas prowadzenia sprawy utrzymywać wyznaczone schematy postępowania, nazewnictwo, metodykę pracy operacyjnej bądź śledczej, zarówno na potrzeby opisania węzłów sieci (atrybutyzacji), jak i identyfikacji relacji zachodzących między węzłami. W ten sposób sieci organizacyjne można klasyfikować na podstawie rodzaju zaangażowanych podmiotów i interakcji zachodzących między nimi. Korzystanie z takiego schematu umożliwi wnioskowanie o każdym jego elemencie, a ich ocena będzie wynikiem relacji istniejących między danym elementem a innymi elementami zakwalifikowanymi do sieci bądź elementami z bliskiego otoczenia sieci, np. występowanie stanu recesji (w działaniach sieci) lub zaktywizowanie kryminalne, zmiana przywództwa czy pobudzenie aktywności pod wypływem czynników spoza organizacji. Ponadto taki schemat pozwoli na umiejętne nazwanie atrybutów sieci i przypisanie ich do jej węzłów. Dzięki temu ocena sieci oraz schemat (katalog) zachowań przestępczych zostaną wzbogacone o wnioskowanie przeprowadzone w przeszłości, ale uzupełnione o informacje nieznane w tamtym momencie.

Ta swoista retrospekcja oprócz uzupełnienia modelu przestępstwa (organizacji) pozwala na przeanalizowanie reakcji członków grupy przestępczej oraz podział zdarzeń na planowane bądź przypadkowe. Umożliwia to rozpoznanie taktyki przestępstwa przyjętej przez sprawców oraz stosowanych przez nich metod kamuflażu. Jednocześnie można ocenić, czy reakcja organów ścigania na przestępstwo była adekwatna do zagrożenia (przeprowadzona we właściwym czasie, miejscu i w stosunku do odpowiednich osób – przy założeniu całościowej lub częściowej neutralizacji organizacji przestępczej

[51] Patrz przykładowo: program iBase zintegrowany z Analyst's Notebook. iBase zapewnia prosty mechanizm importu umożliwiający pobieranie danych z wielu źródeł, takich jak: pliki tekstowe, źródła danych zgodne z OLE lub pliki XML (schemat MS Rowset), i konwertuje je na encje (bazy danych – dop. red.) oraz łącza, zapewniając jednolity standard informacji. Crime Workbench (CWB) pozwala na tworzenie, zarządzanie i wykorzystywanie tekstowych baz danych, które mają zastosowanie w procesie analizy kryminalnej. Przydatny w sprawach wielowątkowych obejmujących duży obszar terytorialny ze złożoną strukturą organizacji przestępczych oraz dużą ilością informacji, http://www.acsys.com.pl/index_en.php?action=iBase [dostęp: 15 IV 2020].

bądź zapobieżeniu zamachowi terrorystycznemu). W podejściu sieciowym niektóre atrybuty elementów (węzłów) są możliwe do zmierzenia (zmienne losowe) i można je przeanalizować za pomocą narzędzi statystycznych. Pomocne tu będą zarówno teoria informacji, jak i sklasyfikowanie i skwantyfikowanie relacji, niezbędne przy rozpoznaniu całej działalności sprawców (węzłów sieci). Ten drugi aspekt będzie się wiązał z rodzajem popełnianych przestępstw, taktyką popełniania przestępstw przyjętą przez sprawców (w tym *modus operandi*), podejmowanymi decyzjami, np. co do narzędzi wykonawczych, schematów zabezpieczeń logistycznych działań przestępczych oraz ciągłości organizacyjnej.

W badaniach metodami stosowanymi w ramach procesu RE inne założenia należy przyjąć dla przestępczości kryminalnej, a inne dla przestępczości finansowej (ale też dla działań hybrydowych dotyczących obydwu tych sfer). Wiąże się to przede wszystkim z tym, że dotyczy to innego przedmiotu przestępstwa i odmiennej konstrukcji prawnej penalizującej zaistniałe zdarzenia. Ocena, w której analitycy posługują się wyłącznie danymi, jakimi dysponowały organy ścigania przez dokonaniem neutralizacji grupy przestępczej, jak i tymi danymi, które w wyniku zastosowania inżynierii odwrotnej wzbogacają wiedzę o sposobie przestępczego funkcjonowania, umożliwia poznanie aktywności przestępczej. Oznacza to, że ten retrospektywny model postępowania może poszerzyć i „ulepszyć" wiedzę o rozpatrywanym układzie. W konsekwencji obraz działań przestępczych będzie uzupełniony i zwiększy zakres kontrdziałań służb, w tym wykorzystania komputerów kognitywnych (tj. poznawczych, ang. *cognitive computing*, CC).

Przy pozyskiwaniu sygnałów aktywności sprawców będzie również pomocne posługiwanie się przez nich urządzeniami mobilnymi. W kryminalistyce zbieranie i analiza danych pochodzących z telefonów komórkowych obejmuje m.in. pobieranie informacji z tych telefonów, a następnie ich zidentyfikowanie i przeanalizowanie, czy uzyskane dowody są istotne dla trwającego dochodzenia. Dzięki monitorowaniu i odzyskiwaniu danych z urządzeń mobilnych jest możliwe mapowanie zachowań (co do czasu) i ich geolokalizacja. Dokonuje się tego przez odczyty aplikacji zainstalowanych przez sprawcę w telefonach komórkowych, GPS czy korzystanie z informacji zawartych w sieci Internet (korzystanie z e-zakupów, e-płatności, e-usług publicznych czy gier). Mimo preferowania całościowego podejścia do organizacji przestępczej przy przeprowadzaniu diagnozy jej funkcjonowania oraz czynności podejmowanych wobec niej przez organy ścigania, w ramach inżynierii odwrotnej można realizować zadanie przez posiłkowanie się podejściem cząstkowym do poszczególnych obszarów związanych z ocenianą (duplikowaną) organizacją[52].

Podejście całościowe wiąże się z działaniem systemowym i potraktowaniem przedmiotu badawczego jako całości. Natomiast cząstkowe obszary badawcze mogą się

[52] W takim przypadku odtworzona sieć komunikacyjna będzie świadczyła o atrybutach węzłów w sieci. Będzie to jeden z elementów branych pod uwagę przy typowaniu krawędzi sieci i istotnych, z punku widzenia wykrycia przywództwa i sprawców przestępstw, relacji zachodzących między poszczególnymi członkami organizacji uznanymi za węzły sieci.

odnosić do: wewnętrznego zarządzania organizacją, ustanawiania relacji z podmiotami zewnętrznymi (np. innymi organizacjami) czy zarządzania finansami i zapleczem logistycznym organizacji[53]. Dla inżynierii odwrotnej podejście całościowe należy uznać za cel ostateczny. Dzięki badaniom cząstkowym można połączyć impulsy (symptomy) skutkujące konkretnymi sytuacjami (faktami) wiążącymi się z poszczególnymi członkami organizacji, a co za tym idzie – zbadać wpływ tych sytuacji na całą organizację.

W ramach inżynierii odwrotnej można skorzystać również z informacji o danej sprawie uzyskanych ze źródeł cyfrowych. Są nimi m.in. sygnały (informacje) zdobyte dzięki „wyzewnętrznieniu się" członków organizacji terrorystycznych. Dotyczy to takich obszarów, jak: propaganda, wojna psychologiczna, rekrutacja, zbieranie funduszy, eksploracja danych, zbieranie informacji o atakach komputerowych, dystrybucja oprogramowania, kupowanie fałszywych dokumentów (tożsamości), działalność szkoleniowa. Oznacza to, że w przypadku prowadzenia sprawy o wyższym stopniu skomplikowania, ale bez zastosowania analizy kryminalnej, będzie możliwe przedstawienie schematu działania grupy przestępczej w formie wizualizacji wirtualnej, co zapewnia jego większą przejrzystość, dostępność, zwiększa obszar analizy i wnioskowania o dalszych działaniach operacyjnych lub procesowych. Proces RE ma na celu nie tylko weryfikację istniejącego obiektu[54], lecz także stworzenie takiego jego duplikatu, który będzie stanowić poszerzoną wersję modelu wyjściowego lub też jego udoskonalenie. Nowa wersja stanie się zaś obiektem wyjściowym dla podjęcia czynności wykonawczych skutkujących neutralizacją obiektu wyjściowego lub modelem służącym w przyszłości do nauki (wsparcie procesu decyzyjnego).

Podstawowe działanie RE wobec organizacyjnej formy przestępczej przeprowadzone z wykorzystaniem programów komputerowych przebiega w następujących etapach:

- za materiał wyjściowy należałoby uznać efekt analityczny (konstrukcja sieciowa rozpoznawanego obiektu) uzyskany w wyniku zastosowania określonego oprogramowania analitycznego oraz dostępne dane zgromadzone w celu poznania konstrukcji sieciowej rozpracowywanego obiektu;
- zebranie jak największej liczby informacji (śladów sieciowych) o aktywności analizowanej organizacyjnej formy przestępczej na temat zdarzeń (koncentracji w sprawie), które będzie można poddać pomiarom (społeczności sieci wprowadziły wiele różnych systemów pomiarowych do zbierania i prezentowania informacji o właściwościach sieci, np. protokoły, techniki, narzędzia, nakładki, ramy, archiwa);

---

[53] Zob. P. Klimas, *Podejście sieciowe w logistyce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 249, s. 36 i nast.; W. Czakon, *Sieci w zarządzaniu strategicznym*, Warszawa 2012.

[54] Wprowadzone pojęcie o b i e k t odnoszące się do podmiotu zawiera w sobie zarówno analizę osób fizycznych, prawnych, relacji, jak i procesów decyzyjnych, stylu myślenia, psychologii. Jest to zabieg upraszczający, świadomie zastosowany na potrzeby dalszych rozważań.

- poszukanie luk, np. przyczynowo-skutkowych, komunikacyjnych czy logistycznych, w dotychczas podjętych czynnościach, m.in. w:
  - wykonaniu retrospekcyjnej analizy danych w sprawie przez przeprowadzenie działań inżynierii odwrotnej wobec uzyskanego efektu analitycznego, będącego konsekwencją wykorzystania programu analizy dostępnego organom ścigania,
  - prowadzeniu analizy danych w sprawie na podstawie dostępnych komercyjnych programów analitycznych przez przeprowadzenie działań inżynierii odwrotnej w stosunku do uzyskanego efektu analitycznego;
  - ustaleniu, czy zdefiniowana konstrukcja sieciowa uwzględnia także dane pochodzące z ukrytych obszarów komunikacyjnych (zaszyfrowanych wiadomości, informacji z sieci Tor czy Darknet), co może ostatecznie mieć wpływ na uzyskanie niepełnego efektu analitycznego;
- ustalenie zaszyfrowanych danych i dokonanie ponownej analizy konstrukcji sieci;
- weryfikacja i walidacja posiadanych danych (np. czy nie doszło do błędu w wyniku przetwarzania danych) przez organy ścigania w konkretnej sprawie oraz pozyskanie dodatkowych informacji (uzupełnienie działań odwrotnych).

W rezultacie tych czynności powinien powstać nowy obraz analizowanej struktury sieci, co zostało przedstawione na schemacie 1.

Schemat 1. Przebieg analizy przeprowadzonej z wykorzystaniem procesu inżynierii odwrotnej.

Źródło: Opracowanie własne.

Korelacja inżynierii postępowej (tradycyjnej) z inżynierią odwrotną w rozpoznawaniu struktur sieciowych

W inżynierii odwrotnej zakłada się docelowo, że uzyskany nowy model wyjściowy umożliwi skuteczniejszą reakcję organów ścigania (zarówno na poziomie śledczym, jak i operacyjnym). Rozpatrywanym obiektem może być zarówno organizacja przestępcza jako całość, jak i jej najmniej rozpoznana część, która nie została poddana badaniu ze względu na niewystarczającą liczbę informacji o samych węzłach oraz relacjach z innymi węzłami i otoczeniem. Wynikiem inżynierii postępowej jest ustalenie i zbadanie danego przedmiotu jako noszącego wartość dowodową. Stąd też jego stan odnosi się do określonego zdarzenia, czasu przeszłego oraz śladów pozyskanych w wyniku jego zbadania i przeprowadzonej analizy. W konsekwencji zarówno w fazie przedsądowej, jak i sądowej można przypisać winę sprawcy, któremu dany przedmiot (podmiot) będzie można sprawczo przyporządkować. Oznacza to zamknięcie pewnego procesu dowodowego dotyczącego określonego okresu aktywności przestępczej. Analiza RE nie poprzestaje na tym etapie. Jest to związane z dynamiką działań przestępczych, np. z „odrodzeniem się" działalności przestępczej pod innym kierownictwem, na innym obszarze geograficznym czy w innych rodzajowo obszarach, w których dotychczas grupa nie była przestępczo aktywna (np. w przestępczości narkotykowej, finansowej, kryminalnej). W przypadku inżynierii postępowej czynniki ocenne dla przedmiotu (grupy) będą charakteryzowały statyczny obraz jego działalności na dany czas. W przypadku RE będą to czynniki umożliwiające dynamiczną ocenę aktywności przestępczej w czasie i pozwalające na jej stały monitoring. Materiałem wyjściowym mogą być statyczne parametry wykorzystane w inżynierii postępowej, ale analityk będzie musiał na dalszych etapach zastosować metody dynamiczne, aby uzyskać cel postawiony na początku procesu RE. W konsekwencji powinien powstać aktualny i aktywny w czasie obraz dynamiki działań opracowywanego podmiotu. Przed rozpoczęciem analizy RE należy ocenić, z jakim rodzajem obszaru analitycznego analityk miałby do czynienia w przypadku prowadzenia czynności w ramach inżynierii postępowej. Prawdopodobnie realizowane czynności będą się skupiały na przygotowaniu materiału, który – jako włączony do postępowania – będzie materiałem dowodowym. Może, ale nie musi to ograniczać zastosowania określonej metody w ramach procesu RE. Dla przykładu, taką metodę w ramach tego procesu będzie można zastosować przy badaniu „niekompletnego" przedmiotu przestępstwa. Inżynieria odwrotna umożliwia ponowne zastanowienie się nad sprawą w zakresie wyszukania luk w procesie wykrywczym, rekapitulacji struktury sieciowej rozpracowywanej organizacji, zidentyfikowania rzeczywistego przywództwa itp., zwłaszcza gdy struktura przestępcza wymaga dłuższego czasu do jej rozpoznania. Dotyczy to różnych aktywności w Internecie, m.in. kontaktów z osobami spoza sieci przestępczej (np. przez czaty komunikacyjne Telegram i Signal czy w sieci Darknet), pozyskiwania technologii w celu jej konwersji na potrzeby przestępcze (po dokonaniu ponownego skonfigurowania i wykorzystania kodu, dodając tym samym

niepowtarzalną funkcjonalność i (lub) kontrolę danych)[55], wzrostu działań w obszarze logistycznym (zakup: broni, fałszywych kart, tożsamości, złośliwego oprogramowania czy pozyskiwanie środków finansowych), zmiany dotychczasowego systemu komunikacji, kamuflowania przywództwa i procesów decyzyjnych w sieci, deszyfracji danych, badania dialogu informacyjnego prowadzonego przez media zależne od organizacji terrorystycznych, nielegalnego wytwarzania elementów broni (w tym zakazanej proliferacją). Na schemacie 2 przedstawiono zastosowanie metod RE w rozpracowywaniu przestępczości zorganizowanej.

Schemat 2. Proces inżynierii odwrotnej zastosowany w odniesieniu do obiektu Podmiot A (do organizacji przestępczej).

Źródło: Opracowanie własne.

Zgodnie z powyższym schematem obiekt Przedmiot A (określany jako „Podmiot A") był wynikiem odwzorowania cyfrowego istniejącego w rzeczywistości. Podstawowym modelem analizowanym (mierzonym i przekształcanym) w procesie inżynierii odwrotnej jest Podmiot A (jako docelowy dla inżynierii postępowej i początkowy dla inżynierii odwrotnej). Inżynieria postępowa dotyczyła obszaru przestępstw dokonywanych wyłącznie lub w znacznej części w obszarze internetowym. W przypadku inżynierii odwrotnej będzie prowadzona analiza sieci komputerowej. Sieć zazwyczaj

[55] K. Podiņš, K. Geers, *Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code*, w: *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, T. Minárik, R. Jakschis, L. Lindström (red.), Tallinn 2018, NATO CCD COE Publications, https://ccdcoe.org/uploads/2018/10/Art-10-Aladdins-Lamp.-The-Theft-and-Re-weaponization-of-Malicious-Code.pdf [dostęp: 21 XII 2020].

składa się z wielu małych sieci, które są administrowane przez różne podmioty, nie ma więc jednego miejsca, z którego można uzyskać pełny obraz określonej sieci docelowej. Także internet jest różnorodny, tak więc podejście uznane za przydatne w stosunku do jednych sieci może nie być skuteczne w innych miejscach[56]. Metoda RE może być pomocna również w przypadku zaginięcia części akt sprawy i potrzeby odtworzenia określonych wątków, przede wszystkim tych, które mają wartość dowodową lub zawierają plany realizacji sprawy.

Przedstawiona konstrukcja działania RE wobec Podmiotu A zakłada podejście blokowe (sektorowe) przy zrekonstruowaniu kategorii problemów, które powstają w konsekwencji funkcjonowania tego obiektu. Pozwala również – na podstawie posiadanych danych – na odtworzenie takiego samego obiektu lub uzyskanie innego, odpowiadającego w większym stopniu rzeczywistemu funkcjonowaniu badanego obiektu niż ten, który powstałby w wyniku czynności podjętych w ramach sprawy prowadzonej przez organy ścigania.

Poszczególne bloki (sektory) problemów mieszczą się w dokonaniu „zeskanowania" Podmiotu A przy użyciu już wcześniej zebranych aktualnych danych oraz nowych danych, a także przy użyciu metod analitycznych, w tym określenia mierzalnych parametrów matematycznych sieci przestępczej. Rozpoczęcie analizy może wynikać z wystąpienia określonego zdarzenia, np. zamachu terrorystycznego. W takiej sytuacji będzie możliwe nie tylko przeprowadzenie procesu RE w stosunku do urządzenia technicznego zniszczonego w zamachu (np. zastosowanego ładunku wybuchowego, wykorzystanych środków łączności), lecz także będzie można dokonać retrospektywnej oceny dotychczasowego rozpoznania sieci i ustalić, dlaczego nie doprowadziło ono do ujawnienia przygotowań do zamachu i określenia jego lokalizacji, a także do jego przerwania[57].

Jeżeli rezultatem zastosowania inżynierii odwrotnej będzie powstanie „doskonalszego" modelu Podmiotu A jako organizacji przestępczej, to powinno to spowodować poszerzenie wiedzy organów ścigania, dzięki czemu będzie można wyprzedzić dalszą aktywność przestępczą (analiza predykcyjna). Takie działania pozwolą skutecznie wyeliminować badaną organizację już w fazie przygotowania do przestępstwa, organy ścigania będą także mogły rozpocząć grę operacyjną, m.in. z wprowadzeniem własnej agentury czy też z wykorzystaniem imitacji takiej organizacji.

Model stworzony w wyniku procesu RE staje się pomocny m.in. przy odtwarzaniu struktury organizacji przestępczej (uzupełnianie ubytków struktury) lub rozpoznawaniu aktywności organizacji w sieci w obszarach, w których ma ona zdolności do działania bez pełnej informacji. Posługując się inżynierią odwrotną, będzie możliwe dokonanie oceny, na ile przestępcy przejęli systemy transformacyjne, transakcyjne, przemieszczania

---

[56] Hui Zhou i in., *Computer Network Reverse Engineering*, w: *Computer and Information Science 2011*, R. Lee (red.), Berlin 2011, s. 227–239, https://link.springer.com/chapter/10.1007/978-3-642-21378-6_18 [dostęp: 20 XII 2020].

[57] Przykłady zastosowania RE do urządzeń mobilnych zob. T. Heckmann, *Reverse engineering secure systems using physical attacks*, 2018, https://www.researchgate.net/publication/330618085_Reverse_engineering_secure_systems_using_physical_attacks [dostęp: 19 XII 2020].

przedmiotów, czyli na ile stworzyli alternatywne rozwiązania lub na jakim poziomie kontrolują funkcjonujące systemy dzięki kamuflowaniu swojej przestępczej działalności (dotyczy to także systemów bezpieczeństwa). Chodzi tu głównie o wyeliminowanie „fałszywego naśladownictwa" wykorzystywanego w celach przestępczych.

Podjęcie działań w zakresie inżynierii odwrotnej będzie wymagać rozłożenia na czynniki pierwsze całości wiedzy o Podmiocie A uzyskanej w danym momencie. Istotnym elementem procesu będzie ustalenie zgodności relacji „wpisanych" w konstrukcję z rzeczywiście zaistniałymi oraz stwierdzenie, czy przyjęte mierzalne relacje w sposób właściwy nadały atrybuty, a w konsekwencji – właściwości poszczególnym węzłom. Inaczej mówiąc, czy trafnie oceniono węzły na podstawie informacji o relacjach zachodzących między nimi, plasując je jako: przywódców, decydentów, pośredników i wykonawców. Ważne będzie także zbadanie, czy nie można ustalić atrybutów węzłów w inny sposób, co pomogłoby uzyskać ocenę odrębną od dotychczasowej. W ramach RE powinno być możliwe także ustalenie luk w relacjach (szczególnie tych, które były najważniejsze w ocenie węzłów) i uzupełnienie ich na tyle, żeby nowa konstrukcja umożliwiła weryfikację uzyskanego obiektu Podmiot A, a jednocześnie bardziej urealniła jego strukturę[58].

Przy założeniu, że obiekt ma strukturę sieci, jednym z działań będzie ustalenie parametrów tej struktury i sposobów ich mierzenia. Może to dotyczyć takich obszarów, jak: proces decyzyjny, posługiwanie się oprogramowaniem, wykorzystanie sieci społecznych, logistyka, lokalizacja GPS, posługiwanie się urządzaniami mobilnymi (w tym różnymi aplikacjami), transfer środków finansowych i innych aktywów. Pozyskiwanie parametrów można będzie podzielić na **wewnątrzpodmiotowe**[59] (zastosowane wyłącznie wobec analizowanego podmiotu) i **zewnątrzpodmiotowe** (uniwersalne, powszechnie stosowane wobec zachowań społecznych, indywidualnych w przestrzeni publicznej). Powinno się również wziąć pod uwagę relacje, jakie występują między węzłami (przygotowanie do dokonania statystycznej charakterystyki sieci). Podstawowym modelem analizowanym (mierzonym i przekształcanym) w procesie inżynierii odwrotnej jest Podmiot A. Uznając złożoność Podmiotu A, do jego rozłożenia na poszczególne elementy można wykorzystać analizę sieci kryminalnych jako metodę opartą na SNA (jest to związane z tym, że obiekt jest wycinkiem sieci społecznych, w których dochodzi do uzewnętrznienia działań przestępczych)[60]. Analiza sieci kryminalnych jest prowadzona

---

[58] Weryfikacja jest spowodowana tym, że w procesie inżynierii postępowej mogło dojść do zafałszowania oceny z powodu użycia wyłącznie jednego programu analitycznego, wpisania nieprawidłowych danych, subiektywnego myślenia analityka, kierowania się sugestiami lub rutyną, przyjmowania określonych zdarzeń za pewnik bez ich weryfikacji, złej oceny kodu organizacji przestępczej, pominięcia zdarzeń lub uznania niektórych za nieistotne z punktu widzenia całości prowadzonej analizy bądź przyjęcia niewłaściwego kodu typowanego dla rozpracowywanej organizacji przestępczej.

[59] Wyróżnienia w tekście pochodzą od autora (przyp. red.).

[60] Zob. K. Harężlak, M. Kozielski, *Metody analizy sieci kryminalnych*, „Studia Informatica" 2010, nr 2A, s. 35 i nast.

„do przodu" przez dokładanie komponentów do ustalonych węzłów sieci lub wprowadzanie do niej nowych węzłów (dekompozycja). W ramach procesu RE ważne będzie również ustalenie dla sieci stanu *zero-day* (czyli momentu rozpoczęcia działalności) dla luki, przez którą można zainstalować złośliwe oprogramowanie, ustalenie luk w rozwoju sieci, wskazanie pierwszego mocodawcy finansowego czy inspiratora działań przestępczych. W ramach RE należy określić stan początkowy, który będzie podstawą do „rozebrania sieci" na czynniki pierwsze. Ważne będzie ustalenie węzłów, wskazanie, jakie elementy oraz jakie rodzaje relacji wzięto pod uwagę w budowaniu krawędzi, np. czy relacje budowano na podstawie typowania udziału danej organizacji w określonym przestępstwie lub w kilku przestępstwach, o różnym stopniu rodzajowości. Czy, a jeśli tak, to jakie, relacje sieci z elementami spoza sieci (np. umieszczonymi w jej otoczeniu) wzięto pod uwagę? Co uwzględniono przy nadawaniu określonym węzłom przynależnej im wagowości (ścisłe kierownictwo, łącznicy, rekruci, bezpośredni wykonawcy, organizatorzy itp.) oraz przy badaniu relacji zachodzących między nimi (z wykorzystaniem obliczenia współczynnika korelacji r-Pearsona[61], który służy do sprawdzenia, czy dwie zmienne ilościowe są powiązane ze sobą związkiem liniowym).

Z uwagi na potrzebę dokonania ilościowej oceny poszczególnych węzłów do ich miarowania oraz skwantyfikowania ich relacji można wykorzystać **teorię grafów**. W badaniach istotne będzie także zbadanie atrybutu centralności poszczególnych węzłów zarówno w celu uzupełnienia informacji o sieci lub weryfikacji już posiadanych danych, jak i ustalenia rzeczywistego kierownictwa w sieci (mierzalność centralności stopnia, pośredniczenia lub bliskości). Przy analizie Podmiotu A należy mieć na uwadze, że wobec jego „odtworzenia" w procesie RE prawdopodobnie starano się zastosować specjalistyczne narzędzie analityczne, jakim posługują się analitycy kryminalni. Jeśli jednak wobec obiektu wykonywano czynności z zakresu SNA, to należy uwzględnić to, że analiza sieci społecznych może być nieadekwatnym (lub nie w pełni adekwatnym) instrumentem analitycznym, dlatego że różni się konstrukcją i wewnętrznymi relacjami od analizy sieci kryminalnych. Należy wziąć pod uwagę element manipulacji siecią na potrzeby kamuflażu – zarówno decydentów (w celu ich ukrycia w strukturze organizacji), jak i obszarów samej sieci, które są uznane za wrażliwe[62].

Kolejnym krokiem analizy będzie wizualizacja wyników w postaci grafu. Graf to zbiór punktów (zwanych wierzchołkami lub węzłami) połączonych krawędziami. Sieć przestępcza w znaczeniu matematycznym będzie określana jako graf wyrażony wzorem: $G = (V, E)$, gdzie V to zbiór węzłów (wierzchołków), $V(G) = \{v_1, v_2, ..., v_n\}$, a E to zbiór krawędzi: $E(G) = \{e_1, e_2, ..., e_n\}$. W większości zastosowań grafów w praktyce stosuje się grafy ważone, w których każdej krawędzi przyporządkowuje się liczbę

[61] Więcej na temat korelacji r-Pearsona zob. https://www.naukowiec.org/wiedza/statystyka/korelacja_745.html (przyp. red.).

[62] Nowatorskie badania w kierunku ujawniania kamuflażu w sieci prowadził M. Waniek. Zob. tenże, *Ukrywanie się w sieciach społecznych. Autoreferat*, https://depotuw.ceon.pl/bitstream/handle/item/2174/autoreferat-pl.pdf?sequence=3 [dostęp: 16 IV 2020].

zwaną wagą tej krawędzi[63]. W ramach procesu RE będzie możliwe uzyskanie informacji o wierzchołku początkowym, a tym samym będzie można poddać ocenie, czy właściwe zdarzenie lub pewien określony czas zostały objęte działaniami organów ścigania w celu rozpracowania działalności grupy przestępczej. Sieć zostanie poddana analizie i „odtworzeniu" przepływu czynności, które będzie można odpowiednio zakwalifikować (jako przygotowanie do popełnienia przestępstwa, rozdysponowanie zysku przestępczego, wyznaczenie członka grupy do realizacji zleconego zadania, np. do modyfikacji cyberprzestrzeni i oprogramowania).

Zastosowanie inżynierii odwrotnej w obszarze przestępczości wiąże się z weryfikacją osiągniętego wyniku (obrazu Przedmiotu A), symulacją działań przy użyciu odpowiedniego algorytmu umożliwiającą wykrycie kamuflowania się węzłów w sieci, dodaniem nowych danych nieznanych jeszcze podczas prowadzenia sprawy lub tych samych danych, ale ponownie zweryfikowanych. Ta ostatnia czynność może zostać uzupełniona o niewykryty cykl działania przestępczego, który można połączyć z potwierdzonym przestępczym „efektem" działalności członków grupy. Wynikiem analizy będzie wyciągnięcie wniosków dotyczących hierarchiczności w grupie, przyjętego procesu decyzyjnego, wariantu działań optymalnego dla osiągnięcia zysku przestępczego bądź innego, który skutkował ograniczeniem zysku, ale zapewnił wyższy poziom bezpieczeństwa nielegalnej działalności (ustalenie przyczyny podjęcia takiej decyzji). Oceniając czynności: poprzedzającą i następującą, można uzyskać wiedzę na temat tego, czy grupa przestępcza miała odpowiedni własny potencjał do realizacji przestępczego przedsięwzięcia, czy też musiała się posiłkować elementami z otoczenia, a także czy pominięto dystrybucję aktywów, informacji, udziału w realizacji zadania określonych członków, czy i co było przyczyną ograniczenia osobowego udziału w przestępczej realizacji (np. posiadanie lub pozyskanie złośliwego oprogramowania, sposób jego użycia wedle procesu RE).

Inżynier prowadzący analizę może uzyskać jednocześnie wiedzę na temat, z jakim rodzajem sieci przestępczej ma do czynienia (lub jaki potencjał ma ta sieć) oraz czy jest to sieć deterministyczna, w której czas wykonania czynności zmierzających do popełnienia przestępstwa jest jednoznacznie określony (zdeterminowany). W takim rodzaju sieci każdy zaplanowany etap musi być zrealizowany, aby osiągnąć wyznaczony cel. Analityk będzie też mógł sprawdzić, czy sieć ma charakter stochastyczny, tzn. taki, że w danym przypadku trudno będzie określić czas wykonania czynności (sieć o charakterze losowym). W tym drugim przypadku będzie można określić stopień zorganizowania w grupie oraz podporządkowania, czy grupa ma potencjał wykonawczy, czy jest on ograniczony bądź nie ma go w ogóle, a także czy występują czynniki ograniczające w czasie przygotowanie do przestępstwa. Wnioskiem może być również stwierdzenie, że organy ścigania nie miały wiedzy na temat czasu popełnienia przestępstwa, co wyzwala

[63] Szerzej zob. A. Woźniak, *Grafy i sieci w technikach decyzyjnych*, „Infrastruktura i Ekologia Terenów Wiejskich" 2010, nr 4, s. 1–188, http://agro.icm.edu.pl/agro/element/bwmeta1.element.dl-catalog--0eeb75a5-4306-49e7-ab42-ce3dd480539a [dostęp: 16 VI 2020].

potrzebę „dosztukowania" brakującego elementu całości, czyli oceny tego, gdzie i w jakim czasie doszło do przestępstwa (typowanie będzie się odbywało w przedziale czasowym między najwcześniejszym możliwym a najpóźniejszym dopuszczalnym terminem). Na schemacie 3 przedstawiono zastosowanie instrumentów analitycznych wykorzystywanych w analizie grup przestępczych metodami stosowanymi w ramach procesu RE.

Schemat 3. Zastosowanie instrumentów analitycznych na potrzeby inżynierii odwrotnej do Podmiotu A (do organizacji przestępczej).

Źródło: Opracowanie własne.

Na podstawie analizy obiektowej, zarządzania i logistyczno-finansowej oraz ze źródeł zewnętrznych będzie możliwe zgromadzenie danych o Podmiocie A. Platformą do dalszych działań w ramach RE będzie dotychczasowa platforma analityczna lub inna, wykorzystywana na potrzeby inżynierii postępowej, dlatego też przed posłużeniem się zgromadzonymi danymi w ramach RE niezbędne będzie ich techniczne opracowanie oraz weryfikacja, a czasami także walidacja. Wiąże się to przede wszystkim z potrzebą wyeliminowania błędów związanych z techniczną stroną analizy (np. użyciem różnych programów) oraz weryfikacją zapisów językowych (np. odmienności zapisów nazwisk, nazw miejscowości, co często występuje przy transkrypcji z cyrylicy lub języka arabskiego). Powodzenie całego procesu zależy od dokładności opracowywanych informacji lub danych na poszczególnych etapach. Pozyskanie danych będzie można przeprowadzić w ramach analizy obiektowej, w której należałoby także dokonać ustalenia celu, jaki został założony przy uzyskaniu Podmiotu A (analiza całościowa, częściowa realizacja założeń lub brak ich realizacji).

Stan wyjściowy dla RE jest istotny z punktu widzenia zakładanego celu, tj. czy chce się uzyskać ponową ocenę obiektu po uzupełnieniu braków w jego funkcjonowaniu (Podmiot A_1), czy dąży się do zbudowania całkiem nowego modelu (Podmiot A_n),

w przypadku, gdy uznano, że model Podmiotu A powstał w wyniku błędu. Całość działań powinna być oparta na strukturze sieciowej rozpatrywanej organizacji jako najbardziej skutecznego modelu analitycznego na potrzeby dalszych czynności w ramach RE. W grę będzie wchodziło np. przyjęcie innych niż dotychczas atrybutów do oceny węzłów tej samej sieci. Analiza obiektowa powinna więc obejmować węzły sieci, krawędzie oraz atrybuty (właściwości) węzłów (ocenie powinno się poddać wszystkie składowe, które są szczegółowo analizowane i rozwijane). Analiza obiektowa to źródło informacji o Podmiocie A. Po ponownej ocenie Podmiotu A będzie można uzyskać ten sam Podmiot A_n, który stanie się ulepszoną wersją Podmiotu A, uzyskaną w wyniku uzupełnienia wiedzy o poszczególnych jego elementach lub też nowy Podmiot A_1, który będzie stanowił odzwierciedlenie Podmiotu A, ale w nowej, „lepszej" wersji (otrzymanie docelowego modelu parametrycznego). Dzięki modelowi A_1 będzie możliwe podjęcie działań, które skuteczniej zneutralizują analizowany Podmiot A, lub zyskanie czasu na przeprowadzenie gry na potrzeby jego neutralizacji.

Pierwszy przypadek zaistnieje wtedy, gdy w wyniku zastosowania RE zostanie stwierdzone, że dotychczasowe działania prowadzone „do przodu" nie zawierają istotnego błędu, a jedynie wiedza o Podmiocie A była niepełna. Drugi natomiast – gdy po zastosowaniu RE uzna się, że kierowano się błędnymi założeniami i informacjami, w wyniku czego uzyskano Podmiot A, który jest nieadekwatny do rzeczywistości, co spowodowało niezrealizowanie zakładanego celu działania. Będzie ono uzależnione między innymi od możliwości pozyskania danych o obiekcie oraz od tego, jakich czynności analitycznych nie wykonano w ramach inżynierii postępowej. Na temat pierwszego podejścia w zakresie „uzupełnianie posiadanych informacji" pisał w swojej pracy dotyczącej poszukiwania węzłów ukrytych Marcin Waniek. Wskazał on, że (…) *ze względu na tę trudność w modyfikowaniu istniejącej sieci, kierujemy swoją uwagę na inne pytanie, mianowicie rozważamy, w jaki sposób można zbudować sieć ukrytą od zera tak, aby jej przywódcy pozostali ukryci, jak również aby utrzymywali swój wpływ na pozostałych członków sieci. Nasze rozwiązanie opiera się na pomyśle, aby otoczyć przywódców grupą zaufanych „kapitanów", których rolą jest ukrycie przywódców oraz pośredniczenie w ich komunikacji z pozostałymi członkami sieci*[64]. Tworzenie nowego modelu wydaje się bardziej możliwe do zrealizowania i sprowadza się do wykonania nieprzeprowadzonych analiz lub też ich ponownego dokonania, ale z uwzględnieniem takich konfiguracji, które w sposób najbardziej prawdopodobny wypełnią luki informacyjne dotyczące rozpoznawanego obiektu.

W inżynierii odwrotnej dodatkowym wsparciem dla analizy obiektowej są analizy: zarządzania i logistyczno-finansowa. Pozwalają one dokładniej zbadać procesy zachodzące w ramach samego Podmiotu A oraz jego relacje z otoczeniem. Powinny

[64] M. Waniek, *Ukrywanie się w sieciach społecznych*…, s. 4. Zob. także: M. Waniek, T.P. Michalak, T. Rahwan, *Hiding in Multilayer Networks*, 2019, s. 1–24, arXiv, 14 XI 2019 r., https://arxiv.org/pdf/1911.05947.pdf [dostęp: 20 XII 2020].

one być też całkowicie obiektywne[65]. Pierwsza z nich wywodzi się z wprowadzenia SNA do zarządzania strukturami organizacyjnymi, druga pozwala ocenić kanały zewnętrznego zasilania środkami finansowymi, dysponowania nimi w ramach organizacji, w tym podział na zyski osobiste oraz zapewniające bezpieczeństwo finansowe organizacji, z uwzględnieniem zaangażowania środków w przedsięwzięcia przestępcze (np. organizację przemytu narkotyków, dokonanie zamachu terrorystycznego). Analiza logistyczno-finansowa pozwala również na ocenę kanałów pozyskania i wykorzystywania logistycznych aktywów na potrzeby organizacji, np. utrzymanie „dziupli" do przechowywania i demontażu kradzionych samochodów, znalezienie miejsca na laboratorium do produkcji narkotyków syntetycznych, zapewnienie bazy szkoleniowej dla terrorystów. W ramach pozyskiwania nowych danych, zwłaszcza zewnętrznych, będzie dochodziło do procesu dyskretyzacji (digitalizacji lub kwantowania), czyli przekształcania danych zdobytych analogowo w dane cyfrowe, którymi posługuje się analiza kryminalna[66] przy budowie obiektu – Podmiotu A. W takim przypadku należy pamiętać o ocenie prawdziwości zgromadzonych danych i ich weryfikacji, tak aby nie dopuścić do wygenerowania kolejnego obiektu z błędem lub aby nie dokonać niewłaściwej korekty analizowanego obiektu. Takie dane powinny być wprzężone w proces obowiązkowej walidacji.

Przeprowadzenie wymienionych trzech etapów RE, tj. analiz: obiektowej, zarządzania i logistyczno-finansowej, powinno pozwolić na przejście do kolejnego, ostatecznego etapu procesu RE, czyli wytworzenia i wdrożenia danych. Należałoby się tu posłużyć metodą analizy kryminalnej lub innym rodzajem analizy sieciowej, która po przetworzeniu danych powinna umożliwić uzyskanie wyniku. Zarówno w analizie obiektowej, jak i zarządzania trzeba uwzględnić struktury komunikacyjne organizacji stanowiące centrum przepływów informacji w organizacji i mogące tuszować i zamazywać rzeczywistą strukturę sieci. Wsparciem będzie też analiza internetowa, dzięki której będzie można scharakteryzować zarówno poszczególne węzły, jak i sposób działania organizacji. W grę będą wchodziły takie analizy, jak: *readability analysis* (analiza, jak czytelny jest dany tekst), *structural analysis* (analiza struktury sieci), *link analysis* (analiza powiązań między węzłami w sieci), *form analysis* (analiza formularzy do wypełnienia)[67] oraz *content analysis* (analiza treści, stosowana

[65] Obiektywizm wiąże się z przyjęciem założenia, że za dane uznaje się nie informacje uzyskane od informatora, lecz te dostarczane z GPS statków wodnych, przeprowadzonych odpraw towarów w portach, towaru przyjętego do hurtowni, przemieszczania się samochodów dostawczych itp.

[66] W zakresie ponownej oceny przebiegu poszczególnych przestępstw kryminalnych, identyfikacji wielu innych przestępstw wykazujących związek z tymi zasadniczymi, określania struktury siatek przestępczych oraz analizowania zakresu i sposobu prowadzenia działalności przestępczej zob. M. Kobylas, *Analiza kryminalna dla studentów bezpieczeństwa wewnętrznego*, Szczytno 2014, s. 13.

[67] Analiza formularzy to narzędzie przeznaczone dla witryn, które aktywnie używają formularzy do wypełniania. Analiza formularzy pomaga firmom zrozumieć, w jaki sposób użytkownicy wchodzą w interakcję z formularzami w ich witrynie internetowej, a także ocenić ich formularze w celu zidentyfikowania problemów, które mogą utrudniać użytkownikom pomyślną konwersję, https://www.indicative.com/data-defined/form-analysis/ [dostęp: 20 XII 2020].

zarówno do form słownych, jak i graficznych)[68]. Przejrzenie danych w internecie w ramach analizy kryminalnej powinno być przeprowadzone zarówno na poziomie dostępnym, jak i na poziomie sieci ukrytych. Struktura sieci jest odzwierciedleniem i przestępstw jawnych, widocznych (śladów pozostawionych w sieci, w rzeczywistości), i ukrytych, niewidocznych (nieujawnionych śladów pozostawionych w sieciach internetowych i w rzeczywistości). Do przestępstw ukrytych będzie można zaliczyć: ślady sieciowe, które mogą zostać wykryte dopiero po dokonaniu grafowania, wysoko zakonspirowane sieci szpiegowskie, kradzieże podstawowego oprogramowania w systemach teleinformatycznych obrony, bezpieczeństwa itp. i zastosowanie w nich złośliwego oprogramowania, co może być wykryte dopiero po analizie wykonanej w ramach procesu RE.

Jak już wspomniano, w wyniku wykorzystania metody RE będzie można otrzymać Podmiot A_1 lub Podmiot A_n. Stworzenie nowych obiektów jest związane między innymi z wypełnieniem luki informacyjnej, luki dotyczącej zarządzania obiektem wynikającej z braku wiedzy o rozpoznawanym obiekcie bądź pozyskanej z tego obiektu, a także z niewykorzystaniem środków technicznych. Zastosowanie RE umożliwi poszerzenie wiedzy o funkcjonowaniu rozpatrywanego obiektu dotyczącej: zmiany kierownictwa, zmiany stylu zarządzania, ustalenia nowych nieznanych zdarzeń przestępczych, uzupełnienia składu osobowego organizacji, weryfikacji ról w samej organizacji i jej otoczeniu oraz przypisania członkom organizacji nowych czynów przestępczych. Będzie to możliwe w wyniku „dosztukowania" do Podmiotu A tych elementów, które dają jego obraz całościowy. Ten nowy model Podmiotu A jest rezultatem nie tylko pozyskania nowych informacji (lub przeanalizowania ich na nowo i otrzymania odmiennych wniosków), lecz także zastosowania innych technik pomiarowych i analitycznych. Tym samym zasób analiz wymienionych w opracowaniu nie jest skończony i może być uzupełniony np. o nowe analizy kryminalistyczne śladów (także te wdrożone do badań jako wynik rozwoju technologicznego czy badań naukowych). Dzięki temu będzie można ustalić sprawców, którzy byli dotychczas nieznani, lub wykazać inny przebieg zdarzenia przestępczego. Nie ulega wątpliwości, że w przypadku danych otrzymanych z badań kryminalistycznych ich odmienność lub ich większe sprecyzowanie może być wynikiem zarówno zastosowania niewykorzystanej do tej pory w sprawie metody badawczej, jak i bardziej precyzyjnych urządzeń technicznych, obliczeniowych bądź wykorzystania danych przetworzonych w bazach danych nieznanych organom ścigania.

Zastosowanie w analizowanej sprawie inżynierii postępowej jest realizowane głównie pod kątem ekonomiki postępowania organów ścigania, co może spłycać działania operacyjne oraz dowodowe jedynie do czynów możliwych do udowodnienia oraz do postawienia zarzutów kierowania i zakładania organizacji przestępczej (grupy lub związku). Tym samym będą pominięte wątki uboczne, których udowodnienie wymaga znacznego nakładu sił i środków. Taki tryb postępowania może być także

[68] J. Scoccimaro, S. Rugaber, *Reverse Engineering of Web Pages*, https://www.cc.gatech.edu/projects/PageSleuth/documents/icpc.pdf [dostęp: 30 IV 2020].

wynikiem taktyki śledczej przyjętej przez prokuratora. Rezultat końcowy – odmienna konstrukcja Podmiotu A – może zostać osiągnięty po zastosowaniu metody analizy kryminalnej, w której wykorzystano inny niż dotychczas program analityczny. W analizie zarządzania będzie można ustalić relacje między kierownictwem organizacji a wykonawcami, a także sprawdzić, czy dobór celu, wykonawców, decyzji i środków jest prowadzony na zasadzie optymalizacji zysku, czy też przez zminimalizowanie kosztów wykonawczych. Aby uwzględnić wskazane preferencje, należy zastosować grafy ważone. Ustalenie preferencji może być pomocne przy określeniu, czy przywódcy tak samo traktują wszystkich wykonawców, czy też dokonują ich gradacji, stosując obiektywne (obojętne) wyznaczniki, czy też kierują się własnymi preferencjami (subiektywne wyznaczniki). Wynikiem takiej analizy powinno być ustalenie schematu postępowania kierownictwa, które może kierować się kosztami wykonawstwa (minimum nakładów przy maksimum zysku) albo realizacją celu za wszelką cenę (bez względu na poniesione koszty).

Przeprowadzenie analizy logistyczno-finansowej obiektu będzie wymagało uwzględnienia przynajmniej dwóch płaszczyzn aktywności przestępczej – logistycznej i finansowej. Pierwsza będzie związana z korzystaniem przez sprawców przestępstw z tych systemów, które są ogólnodostępne (np. firmy świadczące usługi pocztowe, firmy kurierskie, przewozy kontenerowe statkami, transport lądowy lub kolejowy, transport międzynarodowy, sortownie, hurtownie, lokalni dystrybutorzy, giełdy towarowe). Druga płaszczyzna – finansowa – jest związana z instrumentami oferowanymi w ramach usług takich instytucji, jak banki, towarzystwa ubezpieczeniowe, ale również z usługami oferowanymi na czarnym rynku (nielegalne przemieszczanie towarów oraz środków finansowych, np. przemyt fizyczny towarów, system „czarna hawala", nielegalne rozliczenia gotówkowe, wykorzystanie podmiotów rejestrowanych na obszarach *offshore*). Przedmiotowe obszary będą wymagały badań ilościowych (liczby powiązań w określonym czasie), ale w kontekście relacji międzyosobowych.

Zastosowanie analizy sieciowej w badaniach relacji nieformalnych (społecznych, interpersonalnych) może niejednokrotnie być narzędziem służącym ujawnieniu dodatkowych informacji kryjących się w ramach istniejących sformalizowanych struktur wewnątrz- i międzyorganizacyjnych, niewidocznych dla innych ilościowych metod badawczych[69]. Na analizę logistyczno-finansową działań organizacji przestępczych należy patrzeć m.in. pod kątem typowania rozwiązań jako najbardziej optymalnych z punktu widzenia zysku biznesowego. Można pod to podciągnąć przeprowadzenie procederu legalizacji środków (prania brudnych pieniędzy), tak aby skorzystać z formalno-prawnych i organizacyjnych rozwiązań niezbędnych do wykazania legalności aktywów, które pozostają w dyspozycji organizacji. Innym przykładem będzie zapewnienie sobie kontroli lub powołanie podmiotów w obszarze logistyki i finansów, które będą źródłem pierwotnych dochodów dla organizacji przestępczej.

---

[69] C.R. Carter, L.M. Ellram, W. Tate, *The Use of Social Network Analysis in Logistics Research*, „Journal of Business Logistics" 2007, nr 1.

Analiza sieci obiektu może również ujawnić potrzebę zoptymalizowania własnych celów przestępczych przy wykorzystaniu formalnych kanałów dystrybucji towarów czy środków finansowych. Takie działania będą wynikały z konieczności zapewnienia bezpieczeństwa i tajności operacjom koordynowanym przez członków struktury przestępczej lub terrorystycznej. Poszerzenie analizy obiektu pod kątem udziału w procederze prania pieniędzy bądź finansowania terroryzmu będzie wymagało przeprowadzenia dodatkowego miarowania obiektu przy wykorzystaniu jednostki wywiadu finansowego i zastosowanej analizy opartej na ryzyku w ramach AML/CFT[70] instytucji obowiązanej oraz analizy wywiadu finansowego przeprowadzonej bezpośrednio w jednostce. Aspekty odwrotnej rekapitulacji powinny zostać uwzględnione w ramach inżynierii odwrotnej obiektu Podmiot A. W przypadku zastosowania pomiaru obiektu pod kątem analizy finansowej będzie możliwe przyjęcie rozwiązania ocennego opartego na modelu organizacji przestępczej jako modelu biznesowego przedsiębiorstwa[71]. Zarówno model zorganizowanej grupy przestępczej jako model (nielegalnego) przedsiębiorstwa, jak i model biznesowy organizacji terrorystycznej zbliżają się do modeli ekonomicznych tego rodzaju układów grupowych[72]. Model ekonomiczny uwzględnia przede wszystkim zachowania związane z nielegalną dystrybucją towarów, usługami związanymi z ich wytwarzaniem oraz z redystrybucją zysków otrzymanych w wyniku handlu nimi. Podobnie jak każde przedsiębiorstwo organizacja terrorystyczna także wymaga pewnych podstawowych zasobów, które są niezbędne do tego, aby mogła istnieć. Przy takim spojrzeniu na funkcjonowanie organizacji terrorystycznej należy mieć na uwadze to, że ze względu na jej możliwości funkcjonalne, w tym ofensywne (operacyjne), powinna ona spełniać określone wymogi absorpcji środków. Pozytywna ocena organizacji jest możliwa jedynie wówczas, gdy za dedykowane środki jest ona w stanie zrealizować cel stawiany jej przez sponsorów, czyli po prostu być skuteczna.

W ramach miarowania Podmiotu A będzie można dodatkowo przeprowadzić analizę psychocybernetyczną[73], w której wykorzystuje się metodę dynamizmu

---

[70] *Anti Money Laundering/Counter Financing of Terrorism* – zbiorcze określenie przepisów i zasad, które muszą stosować firmy świadczące usługi finansowe, aby zapobiegać praniu brudnych pieniędzy i finansowaniu terroryzmu. Procedury z tym związane polegają głównie na monitorowaniu podejrzanych transakcji. Za: https://cryps.pl/definicja/aml-cft-anti-money-laundering-counter-financing-of-terrorism/ [dostęp: 1 II 2021] – przyp. red.

[71] W zakresie modelu biznesowego organizacji przestępczej typu kryminalnego zob. D.C. Smith, *Paragons, Pariahs and Pirates: A Spectrum-Based Theory of Enterprise*, „Crime & Delinquency" 1980, nr 3.

[72] Odnośnie do modelu biznesowego organizacji terrorystycznej zob. G. Ortmann, *Deconstructing the Business of Terrorism. A Case Study of JNIM in Mali*, CERIS, http://www.ceris.be/fileadmin/library/Research-Papers-Online/Thesis-Deconstructing_the_business_of_terrorism.pdf [dostęp: 30 IV 2020].

[73] Psychocybernetyka może przyczynić się do wytypowania właściwych przywódców organizacji przestępczej, którzy są zdolni do kierowania działaniami nie tylko o charakterze wykonawczym (dokonywania przestępstw, także zorganizowanych), lecz także potrafią pokierować organizacją jako bytem organizacyjnym zdolnym do utrzymania funkcjonalnej równowagi organizacji

charakteru, zmierzającą do ustalenia rzeczywistego kierownictwa organizacji. Zastosowanie cybernetyki w odniesieniu do charakteru człowieka, głównie dynamizmu charakteru, pozwala na ocenę relacji w ramach organizacji przestępczej oraz na typowanie charakteru przywództwa organizacji. Jest to dodatkowy element, który organy ścigania muszą poddać ocenie i analizie przy planowaniu i realizowaniu działań taktycznych zarówno wobec poszczególnych członków organizacji przestępczej, jak i organizacji jako całości. Te działania mogą być nacechowane poszukiwaniem słabych punktów charakterologicznych osób angażujących się w przestępczość zorganizowaną i działania terrorystyczne (profilowanie cybernetyczne)[74]. Tym samym miarowanie będzie mogło być wynikiem zastosowania zarówno metod ilościowych (wynikających z zastosowania SNA), jak i jakościowych (analiza psychocybernetyczna).

Zwieńczeniem procesu inżynierii odwrotnej zastosowanego wobec Podmiotu A (jako obiektu wyjściowego) powinno być przeprowadzenie czynności analitycznych w ramach analizy kryminalnej lub alternatywnego programu analitycznego umożliwiającego taką ocenę dotychczasowych danych, które mogą wykreować obiekty: A_1 lub A_n. Zastosowanie alternatywnego programu analitycznego może przyczynić się do tego, że zostanie przeprowadzona analiza jakościowa tego samego obiektu pod kątem nasycenia go takimi wnioskami i oceną faktów, które przyczynią się do skutecznej reakcji organów ścigania i w rezultacie – do neutralizacji struktury przestępczej. Reakcja powinna być skierowana na wyeliminowanie najbardziej istotnych węzłów sieci, precyzyjne określenie miejsca poszukiwania śladów (dowodów), a także ustalenie miejsca, w których jest gromadzone mienie przestępcze lub jaki jest poziom zaangażowania ich w inwestycjach.

Zastosowanie RE powinno umożliwić także opracowanie specjalnych narzędzi analitycznych przystosowanych do wybranego obiektu. Należy jednak pamiętać, że organy ścigania muszą działać w granicach prawa, a ich instrumenty przeciwdziałania, głównie te o charakterze operacyjno-rozpoznawczym, są ściśle sformalizowane i reglamentowane prawnie. Stąd też wnioskowanie będzie dotyczyło zaproponowania zmian w aktualnych przepisach, które będą obowiązywać w przyszłości. Proces RE należy ocenić pod kątem działań pragmatycznych. Bardziej zatem należałoby ją postrzegać jako wprowadzanie nowych rozwiązań, np. zastosowanie nowego programu analitycznego bądź nowej metody badawczej z zakresu kryminalistyki. Podstawową wadą wykorzystania RE będzie ryzyko stworzenia kolejnych luk w analizach, bez uzyskania optymalnego rozwiązania, które może okazać się nieefektywne i droższe w realizacji, jak również to, że sam proces pochłonie zasoby, które można by było przeznaczyć na rozwój i badania w zakresie inżynierii postępowej. Inżynieria odwrotna powinna być uznana za działanie

---

w czasie. Zob. M.A. Kędzierski, *Zastosowanie rozwinięcia teorii układów samodzielnych na potrzeby typowania przywództwa organizacji przestępczej – analiza psychocybernetyczna*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 129.

[74] Zob. tamże, s. 128 i nast.; M.H. Górny, *Psychocybernetyka w pracy Policji – zarys zagadnienia*, „Kwartalnik Prawno-Kryminalistyczny" 2010, nr 5, s. 97 i nast.

ostateczne, wprowadzone w przypadku braku powodzenia inżynierii postępowej, która wobec zorganizowanych form przestępczości wykorzystuje tradycyjne rozwiązania operacyjno-śledcze i analityczne. Metody wprowadzane w ramach procesu RE mogą być pomocne przy przygotowywaniu kolejnych etapów rozpoznania tych struktur przestępczych, które charakteryzują się wysokim poziomem przetrwania (sieci mafijne, terrorystyczne). Odwrotnością RE jest aktywne i wieloaspektowe działanie w ramach inżynierii postępowej, w różnych kierunkach i przy jak najszerszym wykorzystaniu instrumentów, jakimi dysponują organy ścigania, służby i inne podmioty w celu przeciwdziałania aktywności zorganizowanych grup przestępczych i organizacji terrorystycznych, w tym korzystanie z nowatorskich badań sieci opartych na teorii grafów.

Podsumowanie

Zastosowanie inżynierii odwrotnej do analizy organizacji przestępczych typu sieciowego wydaje się jak najbardziej możliwe. Rozwiązania proponowane obecnie wskazują na to, że jest możliwe dokonanie oceny działań organizacyjnych przez badanie procesu decyzyjnego przywódców, taktyki przestępczej czy mechanizmów stosowanych przy cyberatakach. Wykorzystanie RE w stosunku do tak rozbudowanych podmiotów, jak sieci przestępcze czy terrorystyczne, które chrakteryzują się zmiennością, a czasem małą mierzalnością atrybutów, będzie niejako kreatorem wektorowym. Oznacza to, że zastosowanie RE w bardziej wymiernych obszarach powinno się przełożyć na zwiększenie mierzalności samej sieci. Wydaje się, że RE może być stosowana głównie w badaniu przedmiotu przestępstwa (w tym zamachów terrorystycznych), procedur decyzyjnych tworzonych przez organy ścigania na potrzeby budowania taktyki kontrprzestępczej, ale także w badaniu każdego zdarzenia, w którym organizacja przestępcza posługuje się autonomicznym oprogramowaniem służącym do popełniania przestępstw. Należy pamiętać, że również same sieci przestępcze pozyskują specjalistów z zakresu inżynierii odwrotnej. Dzięki tym osobom organizacje przestępcze mogą rozpracowywać i przekształcać oprogramowania służące celom militarnym, strategicznym czy logistycznym, wykorzystywanym przez organy państwowe działające głównie w dziedzinie bezpieczeństwa i w sferze militarnej. Dlatego wielkim wyzwaniem dla organów odpowiadających za bezpieczeństwo państwa jest podejmowanie działań zabezpieczających – zarówno dotyczących dysponowania tożsamością czy technikami logistycznymi w zabezpieczeniu operacji militarnych, jak i bronią jądrową. W konsekwencji matryca aktywności w obszarze inżynierii odwrotnej, a w przypadku sieci przestępczej – „brudnej" inżynierii odwrotnej, staje się podstawą do wagowania wytypowanych elementów sieci i do prowadzenia działań analitycznych na tej strukturze organizacyjnej. Inżynieria odwrotna w zakresie analizy sieci jest działaniem wtórnym, ale strategicznym, pomocnym w modelowaniu kontrataków na poszczególne wagowane węzły oraz na całe struktury sieci (zwłaszcza te działające w cyberprzestrzeni).

Bibliografia

Blaha M.R., *A Manager's Guide to Database Technology: Building and Purchasing Better Applications*, wyd. 1, [bmw] 2000, Pearson.

Carter C.R., Ellram L.M., Tate W., *The Use of Social Network Analysis in Logistics Research*, „Journal of Business Logistics" 2007, nr 1, s. 137–168.

Chatagnier J.T., Mintz A., Samban Y., *The Decision Calculus of Terrorist Leaders*, „Perspectives on Terrorism" 2012, nr 4–5, s. 125–144, https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2012/issue-4/the-decision-calculus-of-terrorist-leaders--j.tyson-chatagnier-alex-mintz-and-yair-samban.pdf [dostęp: 20 XII 2020].

Chikofsky E.J., Cross II J.H., *Reverse engineering and design recovery: a taxonomy*, „IEEE Software" 1990, nr 1, s. 13–17.

Czakon W., *Sieci w zarządzaniu strategicznym*, Warszawa 2012, Wolters Kluwer Business.

Fronczak A., Fronczak P., *Świat sieci złożonych: Od fizyki do Internetu*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Gagg C., *Domestic product failures – Case studies*, „Engineering Failure Analysis" 2005, nr 5, s. 784–807.

Górny M.H., *Psychocybernetyka w pracy Policji – zarys zagadnienia*, „Kwartalnik Prawno-Kryminalistyczny" 2010, nr 5, s. 92–97.

Harężlak K., Kozielski M., *Metody analizy sieci kryminalnych*, „Studia Informatica" 2010, nr 2A, s. 35–46.

Hui Zhou i in., *Computer Network Reverse Engineering*, w: *Computer and Information Science* 2011, R. Lee (red.), Berlin 2011, Springer, s. 227–239, https://link.springer.com/chapter/10.1007/978-3-642-21378-6_18; [dostęp: 20 XII 2020].

Kachel S. i in., *Zastosowanie inżynierii odwrotnej do procesu odtwarzania geometrii układu wlotowego silnika RD-33 w samolocie MIG 29*, „Prace Instytutu Lotnictwa" 2011, nr 213, s. 66–84, http://ilot.edu.pl/PIL/PIL_213.pdf [dostęp: 14 IV 2020].

Kędzierski M., *Zastosowanie rozwinięcia teorii układów samodzielnych na potrzeby typowania przywództwa organizacji przestępczej – analiza psychocybernetyczna*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 128–144.

Klimas P., *Podejście sieciowe w logistyce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 249, s. 38–48.

Kobylas M., *Analiza kryminalna dla studentów bezpieczeństwa wewnętrznego*, Szczytno 2014, WSPol.

Kowalska-Musiał M., *Strukturalna metodologia pomiaru sieci społecznych – rys historyczny i współczesne obszary zastosowań*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2013, nr 28, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171350117 [dostęp: 15 II 2021].

Kurzynowski T. i in., *Proces inżynierii odwrotnej w zastosowaniach kryminalistycznych*, „Problemy Kryminalistyki" 2014, nr 285, s. 4–46.

Lewandowski M., *Pomiar mediów społecznościowych jako element zarządzania wiedzą i informacją w przedsiębiorstwach*, „Acta Universitatis Nicolai Copernici. Zarządzanie" 2018, nr 4, s. 115–122, https://apcz.umk.pl/czasopisma/index.php/AUNC_ZARZ/article/view/AUNC_ZARZ.2018.049/17178 [dostęp: 16 IV 2020].

Pawluszko T., *Poliheurystyczna teoria podejmowania decyzji w analizie bezpieczeństwa*, „Colloquium Pedagogika – Nauki o Polityce i Administracji" 2020, nr 1, https://colloquium.amw.gdynia.pl/index.php/colloquium/article/view/164/157 [dostęp: 15 II 2021].

Polanowska-Sygulska B., *Użyteczność a maksymalizacja bogactwa: Filozoficzne zakorzenienie poglądów Chicagowskiej szkoły law & economics*, „Archiwum Filozofii Prawa i Filozofii Społecznej" 2011, nr 1, s. 5–14, http://archiwum.ivr.org.pl/1115/uzytecznosc-a-maksymalizacja-bogactwa-filozoficzne-zakorzenienie-pogladow-chicagowskiej-szkoly-law-economics/ [dostęp: 10 II 2021].

Smith D.C., *Paragons, Pariahs and Pirates: A Spectrum-Based Theory of Enterprise*, „Crime & Delinquency" 1980, nr 3, s. 358–386.

Szelewski M., Wieczorowski M., *Inżynieria odwrotna i metody dyskretyzacji obiektów fizycznych*, „Mechanik" 2015, nr 12, s. 183–188, http://www.mechanik.media.pl/pliki/do_pobrania/artykuly/22/40_183_188.pdf [dostęp: 15 IV 2020].

Tarapata Z., *Czy sieci rządzą światem? Od Eulera do Barabasiego*, „Biuletyn Instytutu Systemów Informatycznych" 2012, nr 10, s. 31–51, http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BWA0-0055-0012 [dostęp: 15 IV 2020].

Wawrzynek Ł., *Analiza sieci społecznych w identyfikacji i wzmacnianiu potencjału innowacyjnego zespołów pracowniczych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Research Papers of Wrocław University of Economics" 2017, nr 496, s. 183–204.

Wekerle T., Loures da Costa L.E.V., Trabasso L.G., *Design for Autonomy: An Integrated Product Development Tool for Reengineering of Complex Products for the Brazilian Space Sector*, w: *Transdisciplinary Engineering: Crossing Boudaries*, seria: Advances in Transdisciplinary Engineering, t. 4, 2016 r., e-book, s 632–641.

Woźniak A., *Grafy i sieci w technikach decyzyjnych*, „Infrastruktura i Ekologia Terenów Wiejskich" 2010, nr 4, s. 1–188, http://agro.icm.edu.pl/agro/element/bwmeta1.element.dl-catalog-0eeb75a5-4306-49e7-ab42-ce3dd480539a [dostęp: 16 IV 2020].

Źródła internetowe

Blaha M.R., *Reverse Engineering for Product Assessment*, informIT, 13 X 2001 r., https://www.informit.com/articles/article.aspx?p=23692&seqNum=6 [dostęp: 18 XII 2020].

Breeman K., *How does reverse engineering relate to forensics and solving crimes?*, https://www.quora.com/How-does-reverse-engineering-relate-to-forensics-and-solving-crimes [dostęp: 14 IV 2020].

Chen D., *Reverse-engineering the Org Chart*, https://talkingtalent.prosky.co/articles/reverse-engineering-the-org-chart [dostęp: 21 XII 2020].

Chikofsky E., Cross II J.H., *Encyclopedia of Software Engineering*, 2002, https://onlinelibrary.wiley.com/doi/abs/10.1002/0471028959.sof285 [dostęp: 15 IV 2020].

Heckmann T., *Reverse engineering secure systems using physical attacks*, 2018 r., https://www.researchgate.net/publication/330618085_Reverse_engineering_secure_systems_using_physical_attacks [dostęp: 19 XII 2020].

Hendricks B., *Reverse Engineering in Digital Forensics*, rozdział 4, lekcja 9, https://study.com/academy/lesson/reverse-engineering-in-digital-forensics.html [dostęp: 19 XII 2020].

Kapliński O., *Drzewa decyzyjne i użyteczność decyzji*, http://sipb.sggw.pl/Monografia_2015/Strony%20odRekomendowane_metody-11.pdf [dostęp: 11 II 2021].

Knicker M., *What Are The Types of Reverse Engineering and Why Does it Matter?*, https://www.qpluslabs.com/blog/what-are-the-types-of-reverse-engineering-and-why-does-it-matter/ [dostęp: 15 IV 2020].

Morzy M., Ławrynowicz A., *Wprowadzenie do analizy sieci społecznych*, Poznań 2010/2011, Instytut Informatyki Politechniki Poznańskiej, https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf [dostęp: 16 IV 2020].

Ortmann G., *Deconstructing the Business of Terrorism. A Case Study of JNIM in Mali*, CERIS, http://www.ceris.be/fileadmin/library/Research-Papers-Online/Thesis-Deconstructing_the_business_of_terrorism.pdf [dostęp: 30 IV 2020].

Scoccimaro J., Rugaber S., *Reverse Engineering of Web Pages*, https://www.cc.gatech.edu/projects/PageSleuth/documents/icpc.pdf [dostęp: 30 IV 2020].

Waniek M., *Ukrywanie się w sieciach społecznych. Autoreferat*, https://depotuw.ceon.pl/bitstream/handle/item/2174/autoreferat-pl.pdf?sequence=3 [dostęp: 16 IV 2020].

Waniek M., Michalak T.P., Rahwan T., *Hiding in Multilayer Networks*, 2019, s. 1–24, https://arxiv.org/pdf/1911.05947.pdf [dostęp: 20 XII 2020].

Akty prawne

*Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (*Dz. Urz. UE L 111 z 5 V 2009 r.), https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32009L0024 [dostęp: 15 II 2021].

Decyzja nr 338 Komendanta Głównego Policji z dnia 12 października 2016 r. w sprawie Systemu Informacji Operacyjnych (Dz. Urz. KGP z 2016 r. poz. 65.).

Decyzja nr 126 Komendanta Głównego Policji z dnia 5 kwietnia 2013 r. w sprawie prowadzenia w Policji zestawu zbiorów danych „System Informacji Operacyjnych" (Dz. Urz. KGP z 2013 r. poz. 29, ze zm.).

The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, grudzień 1998 r., https://www.copyright.gov/legislation/dmca.pdf [dostęp: 15 II 2021].

Abstrakt

Inżynieria odwrotna może być wykorzystana do odtwarzania lub modyfikacji obiektów fizycznych oraz zastosowana do programów komputerowych. Nowym wyzwaniem jest jej wykorzystanie w celu zwiększenia skuteczności przeciwdziałania i zwalczania przestępczości kryminalnej i terrorystycznej (zwłaszcza przestępczości zorganizowanej). Odwrócenie procesów analitycznych przez analizę obiektową, analizę zarządzania, analizę logistyczno-finansową, a także wykorzystanie analizy kryminalistycznej i psychocybernetycznej daje możliwość udoskonalenia instrumentów walki z zorganizowaną formą popełniania przestępstw. Dzięki uzupełnieniu braków stwierdzonych w analizie i ponownej ocenie obiektu będzie można otrzymać ten sam obiekt, ale we „wzbogaconej" wersji, lub inny obiekt będący „doskonalszym" modelem analizowanego podmiotu. W konsekwencji będzie możliwe skuteczniejsze i efektywniejszej zneutralizowanie organizacji przestępczej działającej w formie zorganizowanej, w obszarze kryminalnym czy terrorystycznym.

Słowa kluczowe: inżynieria odwrotna, analiza kryminalna, analiza sieci społecznych.

The possibility of using reverse engineering to combat network – type criminal organisation

Abstract

Reverse engineering for the most part now refers to the restoration or modification of physical objects and computer programmes. A new challenge in the fight against crime is the use of reverse engineering to improve the measures of preventing and combating criminal and terrorist crime. Reversing processes through object-oriented analysis, as well as through management, logistics, financial, forensic and psycho-cybernetic analyses is a new outlook on improving the instruments to fight organized crime. As a result, by remedying the identified deficiencies and re-assessing the object, one will be able to get the same object but in the "enhanced" version or another object related to the analysed entity. Consequently, it will be possible to neutralize a criminal or terrorist organization more effectively and efficiently.

Keywords: reverse engineering, criminal analysis, analysis of social networks.

II

STUDIA I ANALIZY

STUDIES AND ANALYSES

ANNA ŁASIŃSKA
ORCID: 0000-0002-0233-0885

DOI: 10.4467/20801335PBW.21.002.13559

Analiza SEM czarnego tonera na wydrukach. Część II

Wykrycie, że dokument generowany komputerowo został sfałszowany, zawsze było wyzwaniem dla śledczych i biegłych w zakresie kryminalistycznych badań dokumentów. Z punktu widzenia kryminalistyki istotna wydaje się analiza autentyczności takiego dokumentu, m.in. identyfikacja urządzenia wykonawczego. W ciągu ostatnich dwóch lat ukazało się niewiele publikacji na temat analizy wydruków z laserowych urządzeń wykonawczych. W celu wsparcia procesów badawczych Neha Verma i inni naukowcy zaproponowali zastosowanie techniki skaningowej mikroskopii elektronowej z emisją polową Schottky'ego zintegrowaną z energodyspersyjną spektroskopią rentgenowską (FE-SEM-EDS) jako najnowszego narzędzia do analizy czarnych tonerów wykorzystanych w drukarkach laserowych i kserokopiarkach[1]. Badania przeprowadzono pod kątem określenia cech morfologicznych tonerów, ich wielowymiarowej analizy oraz określenia ich składu pierwiastkowego. Analiza wielowymiarowa posłużyła autorom do opracowania „modelu klasyfikacji" wydruków na podstawie składu chemicznego tonerów. Z kolei Raj Kumar i inni zastosowali metodę ATR-FTIR[2], łącząc ją z metodami chemometrycznymi w celu szybkiej i nieniszczącej analizy wydruków z urządzeń laserowych oraz dokumentów drukowanych za pomocą drukarek atramentowych[3]. Autorzy podjęli

---

[1] N. Verma i in., *On the spectroscopic examination of printed documents by using a field emission scanning electron microscope with energy-dispersive X-ray spectroscopy (FE-SEM-EDS) and chemometric methods: application in forensic science*, „Analytical and Bioanalytical Chemistry" 2019, nr 16, s. 3477–3495.

[2] Spektroskopia osłabionego całkowitego odbicia w podczerwieni.

[3] R. Kumar, A. Samkaria, V. Sharma, *On the spectroscopic cum chemometric approach for differentiation and classification of inkjet, laser and photocopier printed documents*, „Science & Justice" 2020, nr 4, s. 347–357.

się ustalenia źródła pochodzenia nieznanych dokumentów oraz wizualizacji zmian wewnętrznych występujących w tych samych typach drukowanych dokumentów.

Celem niniejszej publikacji jest wskazanie możliwości identyfikacyjnych urządzeń wykonawczych i ocena tych możliwości na podstawie uzyskanych wydruków. Praca jest kontynuacją dwóch publikacji, które ukazały się w latach 2018–2019[4]. Do badań opublikowanych we wskazanych artykułach wykorzystano wydruki wykonane przy użyciu oryginalnych tonerów oraz ich zamienników. Przedstawione obrazy ze skaningowego mikroskopu elektronowego pozwoliły na przyporządkowanie charakterystycznych cech tonerów do poszczególnych grup urządzeń, tj. monochromatycznych drukarek laserowych, kolorowych drukarek laserowych, monochromatycznych urządzeń wielofunkcyjnych oraz kolorowych urządzeń wielofunkcyjnych. Na podstawie ustalonych kryteriów oceny indywidualnej posegregowano cechy szczególne tonerów na wydrukach uzyskanych z danego urządzenia drukującego i powielającego oraz nadano im nazwy. Kontynuując eksperyment, w niniejszym artykule zamieszczono wyniki badań wydruków uzyskanych z laserowych urządzeń drukujących dwóch firm: Brother oraz Konica Minolta.

Zakup aparatury analitycznej oraz badania zaprezentowane w niniejszej publikacji zostały zrealizowane w ramach projektu badawczego nr 0023/R/ID3/2012/02, finansowanego ze środków Narodowego Centrum Badań i Rozwoju.

Materiały i metody

Materiał badawczy

Badanie przeprowadzono na 21 wydrukach stron testowych z drukarek laserowych oraz laserowych urządzeń wielofunkcyjnych firm Brother i Konica Minolta. Wszystkie wydruki wykonano na papierze formatu A4 jednego rodzaju (standardowym kserograficznym) firmy Papyrus. Zgodnie z zapewnieniami producenta jest to papier bezdrzewny, biały, niepowlekany, matowy. Szesnaście wydruków wykonano przy użyciu oryginalnych tonerów, a pięć przy użyciu zamienników tonerów. Zamienniki „Tonery Laser Experts" pochodziły od jednego dystrybutora – firmy Jet-printer. Przeprowadzono badania jedynie nadruków czarnych. Ocenie poddano powierzchnie tych samych znaków (o, n, u) lub (E, F, G). Na każdym wydruku analizowano po trzy litery z początku, środka i końca tekstu – w sumie dziewięć liter. Każdą literę oglądano w kilku miejscach: na zaokrągleniach, brzegach, rogach i w miejscu połączeń części liter. Wydruki uzyskano z czterech typów urządzeń: kolorowych drukarek laserowych, monochromatycznych drukarek laserowych, kolorowych laserowych urządzeń wielofunkcyjnych

[4] A. Łasińska, *Assessment of the possibility of identification of black toners on printouts in Lexmark printers using SEM method*, „Journal of Microscopy and Ultrastructure" 2018, 6 nr 3, s. 145–159; taż, *Analiza SEM czarnego tonera na wydrukach. Część I*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 211–246.

oraz monochromatycznych laserowych urządzeń wielofunkcyjnych. Wyniki badań oryginalnych tonerów przedstawiono w tabeli 1, a zamienników – w tabeli 2.

Tab. 1. Testowane urządzenia drukujące Brother oraz Konica Minolta – **oryginalny toner**[5].

Lp.	MODEL	TYP URZĄDZENIA
Brother		
1.	HL-2240	monochromatyczne drukarki laserowe
2.	HL-2250DN	
3.	HL-7050	
4.	DCP-9042CDN	kolorowe laserowe urządzenia wielofunkcyjne
5.	MFC-L9570CDW	
6.	DCP-7055W	monochromatyczne laserowe urządzenia wielofunkcyjne
7.	DCP-7057E	
Konica Minolta		
8.	Bizhub c35	kolorowe drukarki laserowe
9.	Bizhub c25	kolorowe laserowe urządzenia wielofunkcyjne
10.	Bizhub 42	
11.	Bizhub c224	
12.	Bizhub c552	
13.	Bizhub c754	
14.	Bizhub 283	monochromatyczne laserowe urządzenia wielofunkcyjne
15.	Bizhub 501	
16.	Bizhub 552	

Tab. 2. Testowane urządzenia drukujące Brother oraz Konica Minolta – **zamienniki**.

Lp.	MODEL	TYP URZĄDZENIA
Brother		
1.	HL-2150N	monochromatyczne drukarki laserowe
2.	HL-2250DN	
3.	DCP9010CN	kolorowe laserowe urządzenia wielofunkcyjne
Konica Minolta		
4.	Bizhub c35	kolorowe drukarki laserowe
5.	Bizhub c25	kolorowe laserowe urządzenia wielofunkcyjne

[5] Wszystkie zdjęcia i tabele zostały opracowane przez autorkę tekstu (przyp. red.).

W celu ustalenia cech budowy charakterystycznych dla konkretnego tonera wykorzystano skaningowy mikroskop elektronowy (SEM). Sposób przeprowadzenia obrazowania mikroskopowego oraz przygotowania preparatów zostały dokładnie opisane w części artykułu. Podobnie jak poprzednio, przyjęto ustalone kryteria oceny i weryfikacji tonera naniesionego na papier, do których zaliczono:

1) sposób rozłożenia warstwy tonera na wydruku (lita czy ziarnista),
2) cechy charakterystyczne struktury powierzchni tonera,
3) cechy charakterystyczne sposobu rozłożenia ziaren tonera,
4) wielkość kształt ziaren oraz strukturę powierzchni ziaren.

Powtarzalność

W celu sprawdzenia powtarzalności otrzymanych wyników przeanalizowano wydruki uzyskane z urządzenia Brother MFC-L9570CDW, w którym zastosowano oryginalny toner. Z każdego wydruku pobrano sześć próbek i oddzielnie je przeanalizowano metodą skaningowej mikroskopii elektronowej. Ocenie poddano kilka cech charakterystycznych, m.in. nieregularne i regularne struktury na ziarnach i powierzchni litej oraz kształt ziaren. Okazało się, że mikrostruktura tonera jest taka sama na wszystkich wydrukach pochodzących z tego samego modelu urządzenia drukującego. Za każdym razem na wydrukach zaobserwowano identyczny efekt – taki sam kształt i wielkość ziaren oraz takie same struktury pojawiające się w ziarnach lub na ich powierzchni.

Badania tonerów na podłożach papierowych o dwóch różnych gramaturach

Oryginalny toner przeznaczony do urządzenia Brother MFC-L9570CDW naniesiono na dwa rodzaje arkuszy papieru o różnej gramaturze dostępnych w handlu. Toner został naniesiony na papier firmy Papyrus formatu A4 o następujących gramaturach: 80 g/m^2 (papier niepowlekany) oraz 199 g/m^2 (papier powlekany). Przed rozpoczęciem serii badań przeprowadzono testy w celu wyeliminowania ewentualnych cech pochodzących z napylania warstwą grafitu. Badano próbki liter bez napylonej powłoki. Następnie próbki pojedynczych liter wyciętych z wydruków były napylane grafitem. Stwierdzono, że rodzaj podłoża wpływa w pewnym zakresie na rozkład tonera.

Na wydrukach uzyskanych na obu typach papieru toner charakteryzował się obecnością części ziarnistej i litej. Najwięcej strefy ziarnistej i pojedynczych ziaren obserwowano na papierze o gramaturze 80 g/m^2. Na całej powierzchni litej był widoczny wyraźny zarys kształtu ziaren. Natomiast na papierze o gramaturze 199 g/m^2 strefa ziarnista była znacznie mniejsza. Ziarna i grupy połączonych ziaren występowały nielicznie w małych skupiskach wewnątrz linii nadruku i w niewielkiej ilości po zewnętrznych stronach linii wydruku. Na powierzchni litej można było zobaczyć wiele pęknięć powierzchni tonera oraz nawarstwienia, które przysłaniały powierzchnie z widocznymi zarysami kształtu ziaren. Gdzieniegdzie obserwowano również struktury o kształtach nieregularnych (zdj. 1).

A

B

Zdj. 1. Struktura powierzchni litej wydruków uzyskanych z urządzenia Brother MFC-L--9570CDW. Wydruk na papierze o gramaturze 80 g/m^2 – powiększenie 1280× (A), wydruk na papierze o gramaturze 199 g/m^2 – powiększenie 1160× (B).

Na obu typach papieru zostały zachowane cechy szczególne ziaren oraz powierzchni litej. Ziarna miały kształt sferyczny, a na ich powierzchni obserwowano struktury guzkowate oraz nieliczne struktury o nieregularnych kształtach. Wraz ze wzrostem grubości papieru obserwowano więcej powierzchni stopionej i litej, przy zachowaniu jednocześnie cech wewnętrznych, tzn. wszystkich cech oprócz cech zmiennych, jakimi są rozkład i wartość stosunku strefy ziarnistej do litej.

Wyniki i dyskusja

Oryginalny toner

Laserowe urządzenia drukujące firmy Brother

Na wydrukach uzyskanych z trzech modeli **monochromatycznych drukarek laserowych** zaobserwowano zarówno cechy wspólne, jak i istotne różnice w sposobie rozłożenia warstwy tonera na papierze (zakres powiększeń 100–150x). Powierzchnię tonera tworzyła głównie warstwa lita. Na wydruku uzyskanym z modelu HL-2240 (zdj. 2 A i B) obszar powierzchni litej był przerywany mniejszymi lub większymi obszarami w postaci pustych otworów (dziur), obszarów wypełnionych pojedynczymi ziarnami bądź grupami ziaren połączonych ze sobą większą lub mniejszą częścią powierzchni i tworzących aglomeraty. Warstwa lita była pofałdowana, zawierała liczne załamania i pęknięcia powierzchni mającej nieregularny kształt i ostre krawędzie. Na powierzchni litej tonera były widoczne również liczne struktury o nieregularnych kształtach i różnych wielkościach. Występowały też obszary, w których można było dostrzec zarysy ziaren wtopionych w powierzchnię tonera, głównie na granicy przejścia powierzchni litej w ziarnistą. Wydruki uzyskane z modelu HL-2250DN (zdj. 2 C i D) charakteryzowały się podobnymi cechami powierzchni litej tonera. Różnica polegała jedynie na tym, że powierzchnia lita zawierała dodatkowo obszary gładkie, czego nie zaobserwowano na wydrukach z modelu HL-2240. W przypadku wydruków uzyskanych z modelu HL-7050 (zdj. 2 E i F), w odróżnieniu od obu wcześniej opisanych modeli, powierzchnia lita tonera była przerywana nielicznymi mniejszymi lub większymi obszarami ziarnistymi. Poza tym była pofałdowana, zawierała liczne pęknięcia oraz dziury

niewypełnione ziarnami. Na powierzchni litej było widać zarysy ziaren wtopionych w powierzchnię i ściśle ze sobą połączonych, tworzących zwartą warstwę tonera.

Zdj. 2. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modeli: HL-2240 – powiększenie 112× (A), powiększenie 1150× (B); HL-2250DN – powiększenie 123× (C), powiększenie 4030× (D); HL-7050 – powiększenie 125× (E), powiększenie 906× (F).

W grupie **kolorowych laserowych urządzeń wielofunkcyjnych** analizie poddano wydruki uzyskane z dwóch modeli urządzeń drukujących: DCP-9042CDN oraz MFC-L9570CDW. Na wydrukach uzyskanych z modelu DCP-9042CDN (zdj. 3 A i B) nie zaobserwowano typowej powierzchni litej. Przypominała ona raczej powierzchnię ziarnistą, były na niej wyraźnie widoczne zarysy ziaren wtopionych w powierzchnię i ściśle ze sobą połączonych, tworzących zwartą warstwę tonera. Na wydrukach uzyskanych z modelu MFC-L9570CDW (zdj. 3 C i D) warstwę tonera tworzyły struktury: ziarnista oraz lita. Warstwa lita, przerywana licznymi mniejszymi lub większymi obszarami o strukturze ziarnistej, była pofałdowana, z licznymi wgłębieniami oraz pojedynczymi dziurami. Na powierzchni warstwy można było wyraźnie zobaczyć zarysy ziaren stopionych i połączonych ze sobą.

Zdj. 3. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modeli: DCP-9042CDN – powiększenie 103× (A), powiększenie 1840× (B); MFC-L9570CDW – powiększenie 121× (C), powiększenie 5210× (D).

Trzecią grupę badanych urządzeń drukujących stanowiły **monochromatyczne laserowe urządzenia wielofunkcyjne**. Obrazowaniu poddano wydruki z dwóch dostępnych modeli tego typu urządzeń. Na wydrukach z modelu DCP-7055W (zdj. 4 A i B) warstwę tonera tworzyły strefy lita i ziarnista. Warstwa lita była przerywana licznymi mniejszymi lub większymi obszarami powierzchni ziarnistej, a także licznymi obszarami w postaci pustych otworów (dziur), obszarów wypełnionych pojedynczymi ziarnami bądź grupami ziaren połączonych ze sobą większą lub mniejszą częścią powierzchni i tworzących aglomeraty. Powierzchnia lita była pofałdowana, z wyraźnie widocznym zarysem ziaren, stopionych i ściśle ze sobą połączonych. W przypadku wydruków uzyskanych z modelu DCP-7057E (zdj. 4 C i D) powierzchnia wydruku pojedynczej litery stanowiła głównie litą warstwę tonera. Była ona przerywana nielicznymi obszarami wypełnione pojedynczymi ziarnami lub grupami ziaren połączonych ze sobą większą bądź mniejszą częścią powierzchni. Warstwa lita była pofałdowana, występowały na niej pęknięcia powierzchni oraz dziury o powierzchni niewypełnionej ziarnami.

Zdj. 4. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modeli: DCP-7055W – powiększenie 115× (A), powiększenie 7690× (B); DCP-7057E – powiększenie 119× (C), powiększenie 2200× (D).

W części ziarnistej tonerów cechą wyróżniającą dany model urządzenia był sposób rozmieszczenia ziaren oraz ich połączenie (mniejszą lub większą ich powierzchnią), wygląd skupisk, a także to, czy występowały one licznie w środku linii wydruku, czy po jej zewnętrznych stronach.

Na wydrukach z **monochromatycznych drukarek laserowych** z modeli: HL-2240 (zdj. 5 A), HL-2250DN (zdj. 5 B) oraz HL-7050 (zdj. 5 C) powierzchnia ziarnista składała się z pojedynczych ziaren bądź grup ziaren połączonych ze sobą większą lub mniejszą częścią powierzchni. Ziarna tworzyły łańcuchy, aglomeraty. Na wydrukach uzyskanych z dwóch pierwszych modeli obserwowano nieliczne pojedyncze ziarna występujące jedynie po zewnętrznych stronach linii wydruku. Z kolei na wydrukach uzyskanych z trzeciego modelu urządzenia pojedyncze ziarna, tak samo jak na wydrukach z poprzednich modeli, występowały po zewnętrznych stronach linii wydruku, ale było ich znacznie więcej.

Na wydrukach uzyskanych z modeli DCP-9042CDN (zdj. 5 D) oraz MFC-L-9570CDW (zdj. 5 E) należących do grupy **kolorowych laserowych urządzeń wielofunkcyjnych** obserwowano liczne pojedyncze ziarna występujące głównie po zewnętrznych stronach linii wydruku pojedynczego znaku. W przypadku wydruków

z modelu DCP-9042CDN ziarna występowały zarówno pojedynczo, jak i grupami, najczęściej parami, połączone ze sobą większą lub mniejszą częścią powierzchni. Natomiast na wydrukach uzyskanych z modelu MFC-L9570CDW ziarna tworzyły aglomeraty bądź stopione skupiska.

W trzeciej grupie, którą były **monochromatyczne laserowe urządzenia wielofunkcyjne**, między badanymi wydrukami z dwóch modeli obserwowano wyraźne różnice. Na wydrukach z modelu DCP-7055W (zdj. 5 F) były widoczne bardzo liczne pojedyncze ziarna lub grupy ziaren występujące po zewnętrznych stronach linii wydruku, w modelu DCP-7057E (zdj. 5 G) natomiast zaobserwowano nieliczne pojedyncze ziarna lub całe ich grupy występujące jedynie po zewnętrznych stronach linii wydruku.

Zdj. 5. Obrazy SEM części ziarnistej tonera dla wydruków z modeli: HL-2240 – powiększenie 2640× (A), HL-2250DN – powiększenie 2540× (B), HL-7050 – powiększenie 1790× (C), DC-P-9042CDN – powiększenie 2250× (D), MFC-L9570CDW – powiększenie 1770× (E), DCP-7055W – powiększenie 2350× (F), DCP-7057E – powiększenie 4060× (G).

Analizę pojedynczych ziaren i ich struktury powierzchniowej przeprowadzono przy większych powiększeniach, tj. około 20 000–100 000×.

W przypadku wydruków uzyskanych z modeli należących do **monochromatycznych drukarek laserowych** stwierdzono różnice w kształcie pojedynczych ziaren. Dla modelu HL-2240 (zdj. 6 A i B) obserwowano ziarna o obłych wydłużonych kształtach. Na powierzchni ziaren występowały liczne niewielkie guzkowate struktury o kształcie kulistym i średnicy około 0,05 μm. Tuż pod powierzchnią ziaren były widoczne liczne struktury o nieregularnym kształcie, połączone ze sobą w łańcuchy lub tworzące aglomeraty, o średnicy około 0,02 μm. Średnica ziaren była zróżnicowana i wahała się w granicach 5–20 μm.

Na wydruku z modelu HL-2250DN (zdj. 6 C i D) obserwowano ziarna o nieregularnych kształtach. Ich powierzchnia była pofałdowana, na niektórych były widoczne wyraźne załamania powierzchni. Nielicznie występowały tu również niewielkie nieregularne struktury o średnicy do około 0,1 μm. Tuż pod powierzchnią ziaren

znajdowały się grupy struktur o nieregularnym kształcie, średnicy około 0,02 μm, połączone ze sobą w łańcuchy bądź tworzące aglomeraty, podobnie jak to obserwowano na wydrukach z modelu HL-2240. Średnica ziaren była zróżnicowana – od 4 μm do 12 μm.

W przypadku wydruków z modelu HL-7050 (zdj. 6 E i F) obserwowano dwa rodzaje ziaren. Pierwszy miał kształt obły, prawie idealnie sferyczny. Ziarna charakteryzowały się gładką powierzchnią z nielicznymi strukturami o nieregularnym kształcie na ich powierzchni. Ich średnica wynosiła od 0,02 μm do 0,1 μm. Tuż pod powierzchnią były widoczne liczne niewielkie struktury (o średnicy poniżej 0,01 μm) o nieregularnym kształcie, które tworzyły małe skupiska. Drugi rodzaj ziaren miał również kształt sferyczny. Ich powierzchnia była pofałdowana, zawierała liczne struktury guzkowate o średnicy około 0,05 μm, rozłożone po całej powierzchni ziarna, z wyjątkiem części, na której rozpościera się druga warstwa o gładkiej powierzchni. Kształtem przypominała łatę, była okrągła, lekko wydłużona, podobna do powierzchni piłeczki tenisowej. Na brzegach łaty obserwowano nieregularne struktury o ostrych krawędziach. Tuż pod jej powierzchnią znajdowały się słabo widoczne nieliczne struktury o nieregularnych kształtach i zróżnicowanych wielkościach. Średnice obu rodzajów ziaren są podobne i wynosiły około 12 μm.

W grupie **kolorowych laserowych urządzeń wielofunkcyjnych** wydruki z modelu DCP-9042CDN (zdj. 6 G i H) charakteryzowały się obecnością ziaren o obłych, lekko wydłużonych kształtach, niektóre miały kształt sferyczny. Powierzchnie tych ziaren były do siebie podobne. Występowały na nich liczne struktury o różnym kształcie i średnicy 0,05–0,1 μm. Tuż pod powierzchnią ziaren można było zauważyć liczne struktury o nieregularnym kształcie i różnej wielkości. Średnica ziaren była w niewielkim stopniu zróżnicowana i wynosiła od 6 μm do 10 μm.

Na wydrukach uzyskanych z modelu MFC-L9570CDW (zdj. 6 I i J) obserwowano obecność ziaren tonera o sferycznych kształtach. Powierzchnia ziaren była morfologicznie podobna. Były na niej widoczne drobne struktury – guzki o średnicy 0,06 μm oraz nieregularne struktury o średnicy od 0,1 do 0,2 μm. Powierzchnia ziaren była pofałdowana, a ich średnica wynosiła od 5 μm do 9 μm.

W ostatniej badanej grupie, w której były **monochromatyczne laserowe urządzenia wielofunkcyjne**, wydruki z modelu DCP-7055W (zdj. 6 K i L) charakteryzowały się obecnością ziaren w kształcie nieregularnych zwartych brył. Na powierzchniach ziaren występowały nieliczne rysy oraz nieregularne struktury o różnym kształcie i wielkości. W pozostałych miejscach powierzchnia ziaren była gładka. Tuż pod ich powierzchnią znajdowały się struktury o nieregularnym kształcie, połączone ze sobą w łańcuchy. Miały one średnicę od 0,02 μm do 0,1 μm. Średnica ziaren była zróżnicowana i wynosiła 4–10 μm.

Z kolei na wydrukach z modelu DCP-7057E (zdj. 6 Ł i M) występowały ziarna o obłych, wydłużony kształtach. Powierzchnia ziaren morfologicznie była podobna, pofałdowana. Pod ich powierzchnią obserwowano liczne struktury o nieregularnym kształcie. Średnica ziaren wynosiła od 10 μm do 12 μm.

Zdj. 6. Obrazy SEM ziaren tonerów dla wydruków wytworzonych z modeli: HL-2240 – powiększenie 27 700× (A), powiększenie 148 000× (B); HL-2250DN – powiększenie 22 600× (C), powiększenie 27 700× (D); HL-7050 – powiększenie 23 600× (E), powiększenie 59 700× (F); DCP-9042CDN – powiększenie 28 100× (G), powiększenie 52 100× (H); MFC-L9570CDW – powiększenie 40 200× (I), powiększenie 127 000× (J); DCP-7055W – powiększenie 28 300× (K), powiększenie 64 400× (L); DCP-7057E – powiększenie 29 300× (Ł), powiększenie 57 500× (M).

Laserowe urządzenia drukujące firmy Konica Minolta

Na wydruku uzyskanym z **kolorowej drukarki laserowej** model Bizhub c35 (zdj. 7) warstwa tonera tworzyła dwie strefy o powierzchni litej oraz ziarnistej. Obszar powierzchni litej był przerywany niewielkimi i nielicznymi obszarami powierzchni ziarnistej, przyjmującej postać niewielkich łat. Powierzchnia lita była gładka, z delikatnymi zarysowaniami, niewielkimi i nielicznymi zrębami lub innymi „uszkodzeniami" struktury powierzchni. Przy powiększeniu około160× zaobserwowano na niej również nieliczne struktury o nieregularnych kształtach i średnicy do około 0,2 μm. W powiększeniu ponad 11 500× uwidaczniało się, że powierzchnia strefy litej tonera była gładka

oraz że znajdowały się na niej delikatne zarysowania, niewielkie i nieliczne zręby oraz inny rodzaj struktur pod względem kształtu czy ogólnego wyglądu na powierzchni litej.

Zdj. 7. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modelu Bizhub c35 – powiększenie 158× (A), powiększenie 11 500× (B).

W przypadku wydruków uzyskanych z pięciu **kolorowych laserowych urządzeń wielofunkcyjnych** zaobserwowano istotne różnice w sposobie rozłożenia warstwy tonera już przy powiększeniu od 100× do 200×. Na wydruku uzyskanym z modelu Bizhub c25 (zdj. 8 A i B) warstwa lita była przerywana licznymi obszarami powierzchni ziarnistej. Była ona gładka, pofałdowana, z widocznymi delikatnymi zarysowaniami oraz zagłębieniami. Na jej powierzchni stwierdzono również nieliczne struktury o nieregularnych kształtach i różnych średnicach – od 0,05 μm do 0,2 μm.

W modelu Bizhub 42 (zdj. 8 C i D) część lita tonera stanowiła przeważającą część powierzchni wydruku. Powierzchnia lita była gładka, występowały w niej liczne pęknięcia i dziury. Obserwowano na niej również nieliczne struktury o nieregularnych kształtach i średnicach do około 0,2 μm.

Wydruki z modelu Bizhub c224 (zdj. 8 E i F) dały obrazy warstwy litej, przerywanej dużymi obszarami powierzchni ziarnistej. Była ona pofałdowana, występowały w niej również nieliczne pęknięcia, dziury oraz zarysowania. Na powierzchni warstwy litej można było zaobserwować liczne struktury o nieregularnych kształtach i średnicy od 0,05 μm do 0,2 μm, tworzące skupiska lub występujące pojedynczo.

Na wydruku z modelu Bizhub c552 (zdj. 8 G i H) warstwa lita była przerywana licznymi obszarami powierzchni ziarnistej, które przeważały nad częścią litą. Powierzchnia lita była nierównomierna, można było w niej zaobserwować wiele pęknięć, zrębów oraz zagłębień. Brzegi zrębów były ostre i tworzyły duże obszary, których końce nie przylegały do pozostałej powierzchni tonera. Na powierzchni warstwy litej można było dostrzec również liczne struktury o nieregularnych kształtach i średnicach od 0,05 μm do 0,5 μm.

W przypadku modelu Bizhub c754 (zdj. 8 I i J) na wydrukach było widać warstwę litą przerywaną licznymi, dużymi płatami powierzchni ziarnistej. Ta powierzchnia przeważała nad częścią litą, znacznie większą niż w modelu Bizhub c552. Powierzchnia lita była pofałdowana i w charakterystyczny sposób tworzyła okrągłe wybrzuszenia. Można było zobaczyć nieliczne pojedyncze struktury o nieregularnych kształtach i średnicach od 5 μm do 6 μm oraz drobne struktury o nieregularnych kształtach i średnicy poniżej 0,5 μm.

Zdj. 8. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modeli Bizhub c25 – powiększenie 120× (A), powiększenie 19 800× (B); Bizhub 42 – powiększenie 206× (C), powiększenie 2380× (D); Bizhub c224 – powiększenie 142× (E), powiększenie 23 000× (F); Bizhub c552 – powiększenie 157× (G), powiększenie 20 500× (H); Bizhub c754 – powiększenie 144× (I), powiększenie 7690× (J).

W grupie **monochromatycznych laserowych urządzeń wielofunkcyjnych** analizie poddano wydruki z trzech modeli urządzeń: Bizhub 283, Bizhub 501 oraz Bizhub 552. Na wszystkich wydrukach warstwa tonera tworzyła obszary powierzchni litej oraz ziarnistej. Zaobserwowano zmienność w rozkładzie powierzchni strefy ziarnistej w stosunku do powierzchni litej. Strefa lita występowała w postaci licznych obszarów łat o różnej wielkości na obszarze całej linii wydruku pojedynczego znaku.

W przypadku wydruków z modelu Bizhub 283 (zdj. 9 A i B) powierzchnia lita była pofałdowana, znajdowały się na niej rysy oraz zręby. Można było również zauważyć zarysy kształtów ziaren. Na powierzchni warstwy litej stwierdzono nieliczne struktury o nieregularnych kształtach i średnicy do 0,1 μm.

Na wydrukach uzyskanych z modelu Bizhub 501 (zdj. 9 C i D) powierzchnia lita była pofałdowana, występowały w niej liczne okrągłe dziury oraz nieliczne pęknięcia. Były widoczne zarysy kształtu ziaren. Na powierzchni oraz tuż pod powierzchnią części litej znajdowały się liczne struktury o średnicy około 0,05 μm.

Natomiast na wydrukach uzyskanych z modelu Bizhub 552 (zdj. 9 E i F) powierzchnia lita była gładka, z nielicznymi zrębami, dziurami i pęknięciami. Na powierzchni warstwy litej gdzieniegdzie zaobserwowano struktury o nieregularnych kształtach i różnych średnicach poniżej 0,1 μm.

Zdj. 9. Obrazy SEM powierzchni strefy litej tonerów dla wydruków wytworzonych z modeli Bizhub 283 – powiększenie 140× (A), powiększenie 8580× (B); Bizhub 501 – powiększenie 799× (C), powiększenie 6080× (D); Bizhub 552 – powiększenie 145× (E), powiększenie 18 600× (F).

Na wydrukach uzyskanych z **kolorowej drukarki laserowej** model Bizhub C35 (zdj.10 A) powierzchnia ziarnista była zróżnicowana. Można było zaobserwować ziarna wtopione w powierzchnię, tworzące łańcuchy lub wysepki o wyraźnie widocznych granicach ziaren. Nieliczne pojedyncze ziarna bądź grupy ziaren występowały w środkowej części oraz po zewnętrznych stronach linii wydruku.

W grupie wydruków uzyskanych z **kolorowych urządzeń wielofunkcyjnych** w modelach Bizhub c25 (zdj. 10 B), Bizhub c224 (zdj. 10 D), Bizhub c552 (zdj. 10 E) oraz Bizhub c754 (zdj. 10 F) powierzchnia ziarnista była również zróżnicowana. Ziarna były wtopione w powierzchnię i tworzyły łańcuchy bądź wysepki o wyraźnie widocznych zarysach kształtu ziaren. Liczne pojedyncze ziarna lub grupy ziaren występowały w środkowej części oraz po zewnętrznych stronach linii wydruku. Jedynie na wydrukach uzyskanych z modelu Bizhub 42 (zdj. 10 C) powierzchnia ziarnista występowała głównie po zewnętrznych stronach linii wydruku. W niektórych miejscach wchodziła głęboko w linię wydruku bądź przecinała ją na wylot. Liczne pojedyncze ziarna lub grupy ziaren połączonych ze sobą w łańcuszki występowały gównie po zewnętrznych stronach linii wydruku.

Wydruki z **monochromatycznych urządzeń wielofunkcyjnych** modeli: Bizhub 283 (zdj. 10 G), Bizhub 501 (zdj. 10 H) oraz Bizhub 552 (zdj. 10 I) charakteryzowały się obecnością aglomeratów w postaci łańcuszków i wysepek o wyraźnie widocznych zarysach ziaren, które były ze sobą połączone. Występowały również ziarna wtopione w powierzchnię, głównie na brzegach powierzchni litej przechodzącej w ziarnistą. Liczne pojedyncze ziarna lub grupy ziaren znajdowały się w środkowej części oraz po zewnętrznych stronach linii wydruku. W przypadku tych urządzeń trudno jednak było zaobserwować istotne różnice między poszczególnymi modelami.

Zdj. 10. Obrazy SEM części ziarnistej tonera dla wydruków z modeli Bizhub c35 – powiększenie 3220× (A); Bizhub c25 – powiększenie 2110× (B); Bizhub 42– powiększenie 3420× (C); Bizhub c224 – powiększenie 1720× (D); Bizhub c552 – powiększenie 1930× (E); Bizhub c754 – powiększenie 3100× (F); Bizhub 283 – powiększenie 1760× (G); Bizhub 501 – powiększenie 1320× (H); Bizhub 552 – powiększenie 2180× (I).

Analizę pojedynczych ziaren i ich struktury powierzchniowej przeprowadzono przy powiększeniach ponad 25 000×.

Z grupy **kolorowych drukarek laserowych** przeanalizowano wydruki uzyskane tylko z jednego modelu – Bizhub c35 (zdj. 11 A). Na wydrukach ziarna miały kształt obły, niektóre były lekko wydłużone, inne przypominały balonik ściągnięty w jednym końcu. Powierzchnia ziaren była grudkowata, lekko pofałdowana, z nielicznymi zagłębieniami oraz pojedynczymi przypowierzchniowymi pęknięciami. Wokół brzegów pęknięć były widoczne skupiska guzkowatych struktur mających średnicę 0,05 μm. Tego typu struktury pokrywały całą powierzchnię ziaren. Ponadto można było zaobserwować nieliczne niewielkie struktury o nieregularnych kształtach i średnicy od 0,05 μm do 0,2 μm. Średnicę ziaren oszacowano na 6–12 μm.

Wydruki uzyskane z pięciu modeli należących do grupy **kolorowych urządzeń wielofunkcyjnych** wykazały zróżnicowanie ziaren tonera pod względem strukturalnym. Toner na wydrukach uzyskanych z modelu Bizhub c25 (zdj. 11 B) charakteryzował się obecnością ziaren o kształtach obłych, jedne były bardziej sferyczne, inne lekko wydłużone. Powierzchnia ziaren była pofałdowana na brzegach, stwierdzono też nieliczne zagłębienia. Na powierzchni ziaren licznie występowały niewielkie struktury zróżnicowane pod względem kształtu i wielkości – od 0,05 μm do 0,1 μm.

Tworzyły one małe skupiska lub występowały pojedynczo. Średnica ziaren była szacowana na 5–10 μm.

Na wydrukach uzyskanych z modelu Bizhub 42 (zdj. 11 C) ziarna tonera miały kształt obły, niektóre sferyczny, a jeszcze inne – nieregularny. Powierzchnia ziaren była lekko pofałdowana z nielicznymi zagłębieniami. Na powierzchni ziaren stwierdzono występowanie licznych niewielkich struktur guzkowatych o zróżnicowanym kształcie – od bardziej sferycznych do nieregularnych, o ostrych krawędziach i średnicy od 0,05 μm do 0,2 μm. Tuż pod powierzchnią ziaren były widoczne także różne nieregularne struktury. Wielkość ziaren wynosiła od 5 μm do 8 μm.

Na wydrukach uzyskanych z modelu Bizhub c224 (zdj. 11 D) ziarna były obłe, podobnie jak w przypadku wydruków uzyskanych z modeli opisanych wcześniej. Niektóre przypominały kule, inne były bardziej wydłużone. Powierzchnia ziaren była pofałdowana w charakterystyczny sposób. Fałdy tworzyły zaokrąglone faliste wybrzuszenia i miały tendencję do układania się wokół pojedynczego ziarna. Na powierzchni ziaren występowały również nieliczne zagłębienia oraz pojedyncze przypowierzchniowe pęknięcia. Dno pęknięć było gładkie. Całą powierzchnię ziaren gęsto pokrywały niewielkie guzkowate struktury średnicy około 0,05 μm, tworzące skupiska wokół brzegów pęknięć, oraz nieliczne struktury o nieregularnym kształcie i średnicy około 0,2 μm. Wielkość ziaren wynosiła od 5 μm do 8 μm.

Toner na wydrukach uzyskanych z modelu Bizhub c552 (zdj. 11 E) zawierał ziarna o kształtach regularnych. Niektóre z nich miały kształt sferyczny. Powierzchnia ziaren była lekko pofałdowana z pojedynczymi wgłębieniami, które wyglądały jak wkłucie igły, oraz nielicznymi pęknięciami. Gęsto ją pokrywały niewielkie guzkowate struktury o średnicy około 0,05 μm, tworzące skupiska wokół brzegów pęknięć. Dno pęknięć było gładkie. Średnicę ziaren oszacowano na 5–9 μm.

Na wydrukach uzyskanych z modelu Bizhub c754 (zdj. 11 F) kształty ziaren były nieregularne. Ich powierzchnia była miejscami gładka, pofałdowana, z pojedynczymi wgłębieniami, zrębami oraz przypowierzchniowymi pęknięciami. Były widoczne również nieliczne pojedyncze struktury o średnicy około 0,4 μm lub ich skupiska. Na niektórych ziarnach można było zobaczyć wiele małych guzkowatych struktur o średnicy około 0,05 μm. Ziarna miały około 9 μm.

W grupie **monochromatycznych laserowych urządzeń wielofunkcyjnych** stwierdzono zróżnicowanie kształtu i struktury ziaren w zależności od wybranego modelu urządzenia. Na wydrukach uzyskanych z modelu Bizhub 283 (zdj. 11 G) ziarna miały kształt obły. Niektóre przypominały kule, kształt innych był nieregularny. Powierzchnia ziaren była gładka, lekko pofałdowana, z zagłębieniami. Na powierzchni ziaren, głównie w zagłębieniach, licznie występowały niewielkie skupiska struktur o zróżnicowanym kształcie – od bardziej sferycznych do nieregularnych o ostrych krawędziach i średnicy około 0,05 μm. Można było dostrzec również struktury występujące tuż pod powierzchnią ziaren. Średnica ziaren wynosiła 5–10 μm.

Na wydrukach uzyskanych z modelu Bizhub 501 (zdj. 11 H) ziarna miały kształty nieregularne. Ich powierzchnia była pofałdowana, występowały na niej zagłębienia oraz pojedyncze przypowierzchniowe pęknięcia. Wokół brzegów pęknięć znajdowały się

niewielkie guzkowate struktury o średnicy około 0,05 μm, które tworzyły skupiska. Dno pęknięć było gładkie. Na powierzchni ziaren oraz tuż pod ich powierzchnią były widoczne liczne struktury o różnych kształtach i średnicach powyżej 0,05 μm. Średnica ziaren była szacowana na około 9 μm.

Na wydrukach uzyskanych z modelu Bizhub 552 (zdj. 11 I) ziarna miały kształty nieregularne. Ich powierzchnia była pofałdowana, występowały zagłębienia oraz liczne pęknięcia. Na całej powierzchni ziaren można było zobaczyć guzkowate struktury o średnicy około 0,05 μm. Średnica ziaren wynosiła od 5 μm do 10 μm.

Zdj. 11. Obrazy SEM ziaren tonerów dla wydruków wytworzonych z modeli: Bizhub c35 – powiększenie 25 200× (A); Bizhub c25 – powiększenie 27 400× (B); Bizhub 42– powiększenie 44 900× (C); Bizhub c224 – powiększenie 29 400× (D); Bizhub c552 – powiększenie 32 400× (E); Bizhub c754 – powiększenie 33 700× (F); Bizhub 283 – powiększenie 37 600× (G); Bizhub 501 – powiększenie 35 800× (H); Bizhub 552 – powiększenie 47 100× (I).

Zamienniki

W dalszej części artykułu zostały przedstawione wyniki badań przeprowadzonych na wydrukach uzyskanych z różnych urządzeń drukujących z wykorzystaniem tonerów zastępczych, tzw. zamienników.

Laserowe urządzenia drukujące firmy Brother

Po analizie wydruków uzyskanych z laserowych urządzeń drukujących Brother stwierdzono, że warstwę tonera tworzą zarówno powierzchnia lita, jak i ziarnista. Różnica

polega na stosunku jednej warstwy do drugiej i formie ich rozmieszczenia w obszarze danego znaku, w zależności od typu urządzenia.

Ocenie poddano wydruki z dwóch **monochromatycznych drukarek laserowych**. Na wydruku uzyskanym z modelu HL-2150N (zdj. 12 A i B) obszar powierzchni litej był przerywany dużymi obszarami mającymi postać ziarnistą. Powierzchni litej było zdecydowanie mniej niż ziarnistej. Była ona pofałdowana, zawierała liczne załamania, zagłębienia, pęknięcia i dziury. Można było zaobserwować także pojedyncze struktury o nieregularnych kształtach i różnych wielkościach. Stwierdzono również obszary z zarysami ziaren, głównie na granicy przejścia powierzchni litej w ziarnistą.

Natomiast na wydrukach uzyskanych z modelu HL-2250DN (zdj. 12 C i D) obszar powierzchni litej przeważał nad ziarnistą. Część ziarnista miała postać nielicznych małych obszarów rozmieszczonych chaotycznie na powierzchni pojedynczego znaku. Powierzchnia lita była pofałdowana, zawierała wiele zagłębień i dziur. Widoczne na niej były także pojedyncze struktury o nieregularnych kształtach i różnych wielkościach. Podobnie jak w modelu HL-2150N tutaj również występowały obszary z zarysami ziaren, głównie na granicy przejścia powierzchni litej w ziarnistą.

Na wydrukach uzyskanych z modelu DCP9010CN (zdj. 12 E i F) należącego do grupy **kolorowych laserowych urządzeń wielofunkcyjnych** przeważał obszar powierzchni litej, choć przypominał on raczej powierzchnię ziarnistą. Znajdowały się tu wyraźne zarysy ziaren wtopionych w powierzchnię i ściśle ze sobą połączonych, tworzących zwartą warstwę tonera. Część ziarnista o typowej strukturze występowała w postaci nielicznych małych obszarów, głównie na brzegach linii wydruku. Na powierzchni litej tonera były widoczne pojedyncze struktury o nieregularnych kształtach i różnych wielkościach.

Zdj. 12. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modeli: HL-2150N – powiększenie 128× (A), powiększenie 2440× (B); HL-2250DN – powiększenie 131× (C), powiększenie 3920× (D); DCP9010CN – powiększenie 159× (E), powiększenie 7850× (F).

W przypadku wydruków z **monochromatycznych drukarek laserowych** z modeli: HL-2150N (zdj. 13 A) oraz HL-2250DN (zdj. 13 B) powierzchnia ziarnista składała się z pojedynczych ziaren lub grup ziaren połączonych ze sobą większą lub mniejszą częścią powierzchni. Ziarna tworzyły krótsze bądź dłuższe łańcuchy, aglomeraty. Na wydrukach uzyskanych z modelu HL-2150N pojedyncze ziarna występowały bardzo licznie w środkowej części oraz po zewnętrznych stronach linii wydruku. Natomiast na wydrukach z drugiego modelu obserwowano nieliczne pojedyncze ziarna występujące jedynie po zewnętrznych stronach linii wydruku.

Na wydrukach z modelu DCP9010CN (zdj. 13 C) należącego do grupy **kolorowych laserowych urządzeń wielofunkcyjnych** można było zauważyć liczne pojedyncze ziarna występujące głównie po zewnętrznych stronach linii wydruku badanego znaku. Były one rozmieszczone pojedynczo lub parami i połączone ze sobą większą lub mniejszą częścią powierzchni.

Zdj. 13. Obrazy SEM części ziarnistej tonera dla wydruków z modeli: HL-2150N – powiększenie 1160× (A); HL-2250DN – powiększenie 1910× (B); DCP9010CN – powiększenie 1950× (C).

Analizę pojedynczych ziaren i ich struktury powierzchniowej przeprowadzono przy powiększeniach – od około 20 000× do około 100 000×. W przypadku wydruków uzyskanych z modeli należących do **monochromatycznych drukarek laserowych** obserwowano różnice w kształcie pojedynczych ziaren. W przypadku modelu HL-2150N (zdj. 14 A i B) ziarna miały kształty nieregularne. Powierzchnia ziaren była pofałdowana, występowały na niej nieliczne, niewielkie skupiska guzkowatych struktur o kształcie kulistym, średnicy około 0,05 μm, a także inne drobne struktury o kształtach nieregularnych. Średnica ziaren była zróżnicowana i wynosiła od 5 μm do 10 μm.

Na wydruku z modelu HL-2250DN (zdj. 14 C i D) ziarna miały kształt obły, lekko wydłużony. Na powierzchni ziaren stwierdzono pofałdowania na brzegach. Występowały na niej nieliczne nieregularne struktury wyglądające jak kryształki o różnych średnicach – do około 1 μm. Znajdowały się tu również nieliczne niewielkie skupiska guzkowatych struktur mających kulisty kształt, o średnicy około 0,05 μm. Tuż pod powierzchnią ziaren występowały grupy struktur o nieregularnych kształtach i różnych średnicach. Wielkość ziaren była szacowana na około 10 μm.

Tonery na wydrukach z modelu DCP9010CN (zdj. 14 E i F), zakwalifikowanego do grupy **kolorowych laserowych urządzeń wielofunkcyjnych**, charakteryzowały się obecnością ziaren o obłych kształtach. Niektóre ziarna przypominały kule. Powierzchnia ziaren była podobna. Można było stwierdzić również pojedyncze

wgłębienia. Na ich powierzchni licznie występowały pojedyncze guzkowate struktury o kulistym kształcie i średnicy od 0,05 μm do 0,1 μm lub ich skupiska. Tuż pod powierzchnią ziaren występowały liczne struktury o nieregularnym kształcie i różnej wielkości. Średnica ziaren była w niewielkim stopniu zróżnicowana i wahała się od 4 μm do 9 μm.

Zdj. 14. Obrazy SEM ziaren tonerów dla wydruków wytworzonych z modeli: HL-2150N – powiększenie 21 700× (A), powiększenie 105 000× (B); HL-2250DN – powiększenie 26 900× (C), powiększenie 99 200× (D); DCP9010CN – powiększenie 27 600× (E), powiększenie 67 800× (F).

Laserowe urządzenia drukujące firmy Konica Minolta

W przypadku wydruków uzyskanych z laserowych urządzeń drukujących Konica Minolta analiza powierzchni tonera wykazała, że na wszystkich wydrukach warstwę tonera tworzyły powierzchnie lita oraz ziarnista. W zależności od typu urządzenia odmienny był natomiast stosunek jednej warstwy do drugiej i forma ich rozmieszczenia w obszarze danego znaku.

Na wydrukach uzyskanych z modelu Bizhub c35 (zdj. 15 A i B) należącego do grupy **kolorowych drukarek laserowych** warstwa tonera tworzyła dwie strefy o powierzchni litej oraz ziarnistej. Obszar powierzchni litej był przerywany licznymi obszarami powierzchni ziarnistej o różnych wielkościach i kształtach. Powierzchnia lita była gładka, pofałdowana, z nielicznymi dziurami oraz licznymi zagłębieniami. Te zagłębienia były wynikiem zarysu obecnych tam sieci ziaren. Powierzchnia ziarnista występowała w postaci łat.

Na wydruku uzyskanym z modelu Bizhub c25 (zdj.15 C i D), należącego do grupy **kolorowych laserowych urządzeń wielofunkcyjnych**, warstwa lita była przerywana licznymi obszarami powierzchni ziarnistej. Powierzchnia ziarnista wyglądała jak cienkie linie, które prostopadle przecinały powierzchnię litą pojedynczego znaku. Gdzieniegdzie były to niewielkie obszary o różnych kształtach i wielkościach.

Powierzchnia lita była pofałdowana, znajdowały się na niej zarysowania, zagłębienia oraz dziury, dało się zauważyć także zarysy ziaren. Na powierzchni warstwy litej były widoczne również nieliczne struktury o nieregularnych kształtach i różnych średnicach do około 0,5 μm.

Zdj. 15. Obrazy SEM powierzchni litej tonerów dla wydruków wytworzonych z modeli Bizhub c35 – powiększenie 153× (A), powiększenie 3210× (B); Bizhub c25 – powiększenie 130× (C), powiększenie 846× (D).

Analiza części ziarnistej tonerów nie wykazała istotnych różnic w obu badanych modelach. Można było zaobserwować na nich ziarna wtopione w powierzchnię, które tworzyły łańcuchy lub wysepki o wyraźnie widocznych granicach ziaren. Liczne pojedyncze ziarna lub ich grupy znajdowały się w środkowej części oraz po zewnętrznych stronach linii wydruku (zdj. 16).

Zdj. 16. Obrazy SEM części ziarnistej tonera dla wydruków z modeli: Bizhub c35 – powiększenie 6250× (A); Bizhub c25 – powiększenie 2210× (B).

Analizę pojedynczych ziaren i ich struktury powierzchniowej przeprowadzono przy powiększeniach do ponad 120 000×. W obu modelach ziarna przyjmowały kształty nieregularne, najczęściej obłe, niektóre były lekko wydłużone lub bardziej sferyczne. Powierzchnia ziaren była lekko pofałdowana, występowały na niej nieliczne zagłębienia oraz pojedyncze dziury.

W przypadku wydruków uzyskanych z modelu Bizhub c35 (zdj. 17 A i B) tuż pod powierzchnią ziaren obserwowano pojedyncze struktury o nieregularnych kształtach i różnych średnicach do około 0,2 μm. Średnica ziaren dla modelu Bizhub c35 była szacowana na 4–9 μm. Natomiast na powierzchni ziaren z wydruków uzyskanych z modelu Bizhub c25 (zdj. 17 C i D) były widoczne liczne skupiska guzkowatych struktur mających średnicę poniżej 0,05 μm oraz pojedyncze struktury o nieregularnych kształtach i średnicach również poniżej 0,05 μm. Średnica ziaren dla tego modelu wynosiła 5–10 μm.

Zdj. 17. Obrazy SEM ziaren tonerów dla wydruków wytworzonych z modeli: Bizhub c35 – powiększenie 34 300× (A), powiększenie 73 100× (B); Bizhub c25 – powiększenie 23 100× (C), powiększenie 123 000× (D).

Porównanie oryginalnego tonera i jego zamiennika

Analizę porównawczą przeprowadzono na wydrukach uzyskanych z trzech typów urządzeń drukujących: monochromatycznej drukarki laserowej Brother HL-2250DN, kolorowej drukarki laserowej Konica Minolta Bizhub c35 oraz kolorowego laserowego urządzenia wielofunkcyjnego Konica Minolta Bizhub c25. Do badań wykorzystano oryginalne tonery oraz ich zamienniki pochodzące od jednego dystrybutora.

Wydruki z monochromatycznej drukarki laserowej Brother HL-2250DN wykonane z wykorzystaniem oryginalnego tonera oraz zamiennika różniły się przede wszystkim kształtem i liczebnością ziaren. Powierzchnia ziaren w przypadku zamienników była pokryta nielicznymi drobinami struktur o nieregularnych kształtach i jasnym kontraście mikroskopowym. Wyraźnie było widać, że ziarna były wtopione w powierzchnię tonera lub papieru. Na wydrukach sporządzonych zamiennikami tonera pojedyncze ziarna występowały nielicznie, raczej tworzyły aglomeraty i można je było zobaczyć jedynie jako uwypuklenie na powierzchni papieru lub tonera.

Na wydrukach uzyskanych z kolorowej drukarki laserowej Konica Minolta Bizhub c35 różnice między wydrukami sporządzonymi przy użyciu oryginalnego tonera a zamiennika były widoczne w obrazie powierzchni litej oraz kształcie i liczebności ziaren. W oryginalnym tonerze na powierzchni litej występowały liczne pęknięcia. W zamienniku natomiast powierzchnia lita była pofałdowana, wyraźnie były widoczne również zarysy kształtu ziaren. Ziarna występowały liczniej po zewnętrznych stronach linii nadruku niż na wydrukach wykonanych z zastosowaniem oryginalnego tonera. Oryginalny toner charakteryzował się natomiast cechą, której nie obserwowano w zamiennikach, czyli kształtem ziaren, które przypominały lekko wydłużony balonik, zwężony na jednym końcu.

W przypadku wydruków uzyskanych z kolorowego laserowego urządzenia wielofunkcyjnego Konica Minolta Bizhub c25 można było stwierdzić, że różnice między oryginalnym tonerem a zamiennikiem dotyczą gównie kształtu i liczebności ziaren. Na wydrukach wykonanych zarówno oryginalnym tonerem, jak i zamiennikiem cechy powierzchni litej były podobne. Różniły się natomiast liczebnością ziaren, których więcej było na wydrukach wykonanych oryginalnym tonerem. Tutaj było także więcej ziaren, które miały kształt sferyczny, niż to obserwowano na wydrukach wykonanych zamiennikami.

W tabelach 3 i 4 przedstawiono wszystkie cechy analizowanych oryginalnych tonerów oraz zamienników naniesionych na papier za pomocą urządzeń drukujących Brother i Konica Minolta. Tabele podzielono na dwie części. W pierwszej zawarto cechy powierzchni litej, w której wyszczególniono własności powierzchni (topografia powierzchni), rodzaj i wielkość struktur występujących w tonerach, w drugiej zaś cechy powierzchni ziarnistej, z opisem topografii powierzchni ziaren, ich kształtu, rozmiaru i struktur występujących na ich powierzchniach.

Tab. 3. Ocena indywidualna tonera naniesionego na papier za pomocą urządzeń drukujących Brother oraz Konica Minolta – **oryginalny toner**. Oznaczenia: TP – topografia powierzchni, NR – nieregularne, R – regularne, X_{max} – maksymalna średnica, S – sferyczny, PP – pod powierzchnią.

Lp.	Model	Typ (rodzaj)	Powierzchnia lita			Powierzchnia ziarnista					
			TP	struktury powierzchniowe		rozłożenie w liniach nadruku	kształt powierzchni	TP ziarna	kształt ziarna	struktury na ziarnach, X_{max} [µm]	X_{max} ziarna [µm]
				NR, X_{max} [µm]	R / X_{max} [µm]						
Brother											
1.	HL-2240	monochromatyczne drukarki laserowe	pofałdowania, liczne załamania, pęknięcia	0,2–05	–	po zewnętrznych stronach, przerwy w ciągłości wydruku	nieliczne pojedyncze ziarna po zewnętrznych stronach linii wydruku, aglomeraty	pofałdowania, zagłębienia, wybrzuszenia	obły, NR, lekko wydłużony	NR, 0,2, guzki, 0,05	5–20
2.	HL-2250DN		nieliczne obszary gładkie, pofałdowania, załamania, pęknięcia, dziury	nieliczne 0,1	–	nieliczne niewielkie obszary	nieliczne pojedyncze ziarna po zewnętrznych stronach linii wydruku, aglomeraty	gładka, zręby, zagłębienia, pofałdowania	NR, wydłużony, niektóre o ostrych końcach	NR, 0,1–0,2	4–12
3.	HL-7050		pofałdowania, pęknięcia, dziury, zarys ziaren	nieliczne 0,5	–	pojedyncze mniejsze lub większe obszary	liczne pojedyncze ziarna lub grupy ziaren po zęwntrznych stronach linii wydruku, łańcuchy	pofałdowana, gładka, łaty	obły, S	guzki, 0,05, NR, 0,01–0,1	12
4.	DCP-9042CDN	kolorowe laserowe urządzenia wielofunkcyjne	pofałdowania, zarys ziaren	nieliczne 0,5	–	liczne obszary o różnych wielkościach, przerwy w ciągłości wydruku	liczne pojedyncze ziarna po zewnętrznych stronach linii wydruku	gładka	obły, lekko wydłużony, S	NR, 0,05–0,1	6–10
5.	MFC-L9570CDW		pofałdowania, zagniecenia, pęknięcia, dziury, zarys ziaren	0,8–1	guzki 0,06	po zewnętrznych stronach, przerwy w ciągłości wydruku	liczne pojedyncze ziarna po zewnętrznych stronach wydruku aglomeraty	pofałdowania, nawarstwienia	obły, S	NR, 0,1–0,2, guzki, 0,06	5–9

6.	DC 7055W	monochromatyczne laserowe urządzenia wielofunkcyjne	pofałdowania, zagłębienia, dziury, zarys ziaren	0,2–0,5	–	duże obszary (łaty), przecinające się z powierzchnią litą	liczne pojedyncze ziarna lub grupy ziaren po zewnętrznych stronach linii wydruku	gładka, miejscami rysy	NR zwarta bryła	NR, 0,02–0,1	4–10
7.	DCP 7057E		pofałdowania, pknięcia, dziury, rozerwania	0,2	–	nieliczne obszary	nieliczne pojedyncze ziarna lub grupy ziaren po zewnętrznych stronach linii wydruku	pofadowania	obły, lekko wydłużony	NR, 0,2	10–12
Konica Minolta											
8.	Bizhub c35	kolorowa drukarka laserowa	gładka, rysy, inne	0,2	–	w części środkowej, po zewnętrznych stronach nieliczne łaty	ułożenie niewarstwowe, stopione aglomeraty, nieliczne ziarna po zewnętrznych stronach linii wydruku	ziarnista, lekko pofałdowana, zagłębienia, pęknięcia	S wydłużony, balonik	NR, 0,05– 0,2, guzki. 0,05	6–12
9.	Bizhub c25	kolorowe laserowe urządzenia wielofunkcyjne	gładka, pofałdowania, zagłębienia, rysy	0,05–0,2	–	łaty, przeplatane	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren, liczne pojedyn-cze ziarna w części środ-kowej i po zewnętrznych stronach linii wydruku	gładka, lekko brzegami pofałdowana, zagłębienia	S, wydłużony	NR, 0,05–0,2	5–10
10.	Bizhub 42		gładka, dziury, liczne pęknięcia	0,2	–	głównie po zewnętrznych stronach, wchodzi głęboko w linię lub przecina ją na wylot	ułożenie niewarstwowe, liczne pojedyncze ziarna, łańcuchy	pofałdowana, nieliczne zagłębienia	S, zwarta bryła	guzki, 0,05, NR, 0,05–0,2	5–8
11.	Bizhub c224		pofałdowania, dziury, nieliczne pęknięcia	0,05–0,2	guzki 0,05	stanowi mniejszą część powierzchni	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren	pofałdowana, nieliczne zagłębienia	S, wydłużony	guzki, 0,05, NR, 0,2	5–8
12.	Bizhub c552		pofałdowania, zręby, pęknięcia i inne	0,5	guzki 0,05	stanowi większą część powierzchni	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren	gładka, lekko pofałdowana, pojedyncze wgłębienia	NR	nieliczne guzki, 0,05	5–9
13.	Bizhub c754		pofałdowania, inne	5–6	–	stanowi większą część powierzchni	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren	miejscami gładka, pofałdowana, pojedyncze duże zagłębienia, zręby i inne	NR	NR, 0,4	9

14.	Bizhub 283	monochromatyczne laserowe urządzenia wielofunkcyjne	pofałdowania, rysy, zręby, zarys ziaren	0,1	–	stanowi większą część powierzchni	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren, pojedyncze ziarna w części środkowej i po zewnętrznych stronach linii wydruku	miejscami gładka, pofałdowana, zagłębienia	obły, S, NR	sferyczne, NR, 0,05	5–10
15.	Bizhub 501		pofałdowania, nieliczne pęknięcia, okrągłe dziury, zarys ziaren	–	0,05	mniejsze i większe obszary, łaty, przeplatane	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren, pojedyncze ziarna w części środkowej i po zewnętrznych stronach linii wydruku	pofałdowana, zagłębienia, pęknięcia	NR	NR<0,05, guzki, 0,05	9
16.	Bizhub 552		gładka nieliczne dziury, pęknięcia, zręby	0,1	–	mniejsze i większe obszary, łaty, przeplatane	ułożenie warstwowe, łańcuchy, wysepki, zarys ziaren, pojedyncze ziarna w części środkowej i po zewnętrznych stronach linii wydruku	pofałdowana, zagłębienia, liczne pęknięcia	NR	guzki, 0,05	5–10

Tab. 4. Ocena indywidualna tonera naniesionego na papier za pomocą urządzeń drukujących Brother oraz Konica Minolta – **zamienniki**. Oznaczenia: TP – topografia powierzchni, NR – nieregularne, R – regularne, X_{max} – maksymalna średnica, S – sferyczny, PP – pod powierzchnią.

Lp.	Model	Typ (rodzaj)	Powierzchnia lita			Powierzchnia ziarnista					
			TP	struktury powierzchniowe		rozłożenie w lini nadruku	kształt powierzchni	TP ziarna	kształt ziarna	struktury na ziarnach, X_{max} [µm]	X_{max} ziarna [µm]
				NR, X_{max} [µm]	R, X_{max} [µm]						
Brother											
1.	HL-2150N	monochromatyczne drukarki laserowe	pofałdowana, liczne załamania, zagłębienia, dziury, pęknięcia, zarys ziaren	1	–	stanowi większość na wydruku pojedynczego znaku,	łańcuchy, aglomeraty, liczne ziarna w części środkowej, po zewnętrznych stronach linii wydruku	pofałdowana	NR	guzki, 0,05	5–10
2.	HL-2250DN		pofałdowana, liczne zagłębienia, dziury, zarys ziaren	1	–	stanowi, mniejszą część powierzchni, nieliczne, drobne obszary	łańcuchy, aglomeraty, nieliczne ziarna w części środkowej, po zewnętrznych stronach linii wydruku	brzegami pofałdowana	obły, lekko wydłużony	guzki, 0,05, NR >1, „kryształki”	10
3.	DCP-9010CN	kolorowe laserowe urządzenia wielofunkcyjne	liczne zagłębienia, zarys ziaren	1	–	typowa, stanowi mniejszość	nieliczne ziarna po zewnętrznych stronach linii wydruku	pojedyncze zagłębienia	obły, kule	guzki, 0,05–0,1	4–9
Konica Minolta											
4.	Bizhub c35	kolorowa drukarka laserowa	pofałdowana, miejscami gładka, zagłębienia, dziury, zarys ziaren	–	–	w części środkowej, po zewnętrznych stronach nieliczne łaty	łańcuchy, wysepki, zarys ziaren, liczne pojedyncze ziarna w części środkowej i po zewnętrznych stronach linii wydruku	gładka, lekko pofałdowana, zagłębienia, dziury	S, wydłużony, NR, „ziarno fasoli”	NR, 0,2	4–9
5.	Bizhub c25	kolorowe laserowe urządzenia wielofunkcyjne	pofałdowania, zagłębienia, rysy, dziury, zarys ziaren	0,5	–	obszary w kształcie łat	łańcuchy, wysepki, zarys ziaren, liczne pojedyncze ziarna w części środkowej i po zewnętrznych stronach linii wydruku	gładka, lekko brzegami pofałdowana, zagłębienia, dziury	S, wydłużony, NR	guzki, 0,05	5–10

Podsumowanie

Do przeprowadzenia analizy tonerów wykorzystano wydruki uzyskane z 21 laserowych urządzeń drukujących dwóch różnych firm. Dało to możliwość identyfikacji tego typu urządzeń dzięki zastosowaniu grupowej i indywidualnej selekcji. Do badań wykorzystano oryginalne tonery oraz zamienniki. Na podstawie wcześniej ustalonych kryteriów ocenę cech charakterystycznych danego tonera na wydrukach przeprowadzono w taki sam sposób, jak opisano w części I[6].

Na wydrukach zaobserwowano dwa rodzaje morfologiczne powierzchni tonera, tj. litą i ziarnistą. Warstwa lita była albo gładka i obejmowała całą powierzchnię nadruku, z nielicznymi pojedynczymi ziarnami widocznymi na jej linii brzegowej, albo przerywana licznymi lub pojedynczymi obszarami o różnym zagęszczeniu ziaren. Nie obserwowano powierzchni całkowicie ziarnistej.

Na żadnym badanym wydruku z obu firm nie zaobserwowano cech indywidualnych dla konkretnego tonera, takich jak pałeczki, igiełki, sześciany czy inne. Nie stwierdzono również cech charakterystycznych dla konkretnego typu urządzenia, jak na przykład nieregularnych lub kulistych struktur tuż pod powierzchnią ziarna i powierzchnią litą tonera, charakteryzujących się innym kontrastem na obrazie SEM. Tego typu struktury występowały w monochromatycznych drukarkach laserowych i monochromatycznych laserowych urządzeniach wielofunkcyjnych takich firm, jak Canon, Dell czy Lexmark[7]. Wykonano również badania oryginalnych tonerów na dwóch różnych podłożach papierowych, ale pochodzących od jednego producenta. Stwierdzono, że morfologia papieru miała wpływ na rozkład tonera na wydrukach oraz na ilość warstwy ziarnistej i litej. Nie zmieniała ona jednak cech wewnętrznych tonerów, tj. różnych struktur (guzików, struktur sferycznych, struktur nieregularnych o silnym kontraście fazowym) obecnych w samym tonerze.

Różnice między oryginalnymi tonerami a ich zamiennikami były widoczne głównie w kształtach ziaren i ich liczebności. W tym wypadku odróżnienie oryginalnego tonera od zamiennika jest dość trudne, również ze względu na zbyt małą liczbę cech szczególnych danego tonera. Dodatkowo zamienniki mogą różnić się od siebie w zależności od producenta, a nawet jeśli pochodzą od tego samego producenta. Przedstawione wyniki wstępnych badań przeprowadzonych na zamiennikach nie dają pewności co do jednoznaczności identyfikacji. Niemniej jednak badania morfologiczne oraz skład chemiczny zamienników pochodzących od różnych producentów są obecnie w fazie testów. Celem tych badań jest stworzenie bazy danych i opracowanie modelu przydatnego do klasyfikacji tonerów.

Na podstawie wykonanych badań oryginalnych kaset można stwierdzić, że tonery na wydrukach uzyskanych z urządzeń drukujących Brother i Konica Minolta charakteryzowały się dość dużym podobieństwem cech morfologicznych. Obserwacje

---

[6] Zob. A. Łasińska, *Analiza SEM czarnego tonera na wydrukach…*

[7] A. Łasińska, *Assessment of the possibility…*; taż, *Analiza SEM czarnego tonera na wydrukach…*

mikroskopowe wskazały, że charakter morfologiczny tonerów stosowanych przez obie wyżej wymienione firmy był odmienny od cech charakterystycznych tonerów stosownych przez takie firmy, jak Lexmark, Canon czy Dell[8]. W przypadku tych ostatnich obecność indywidualnych lub grupowych cech ułatwia identyfikację konkretnego modelu lub grupy urządzeń. Brak istotnych różnic między tonerami obu firm w rezultacie uniemożliwia stwierdzenie, z jakiego urządzenia lub grupy urządzeń pochodzi wydruk.

Być może dobrym rozwiązaniem trudności związanych z identyfikacją cech charakterystycznych w oryginalnych tonerach stosowanych w urządzeniach drukujących Brother i Konica Minolta jest wykorzystanie niezwykle czułej analizy metodą spektroskopii Ramana ze wzmocnieniem powierzchniowym (ang. *surface-enhanced Raman spectroscopy*, SERS). Badania składu chemicznego za pomocą tej metody są obecnie w fazie testów.

Bibliografia

Kumar R., Samkaria A., Sharma V., *On the spectroscopic cum chemometric approach for differentiation and classification of inkjet, laser and photocopier printed documents*, „Science & Justice" 2020, nr 4, s. 347–357.

Łasińska A., *Analiza SEM czarnego tonera na wydrukach. Część I*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 211–246.

Łasińska A., *Assessment of the possibility of identification of black toners on printouts in Lexmark printers using SEM method*, „Journal of Microscopy and Ultrastructure" 2018, nr 6, s. 145–159.

Verma N. i in., *On the spectroscopic examination of printed documents by using a field emission scanning electron microscope with energy-dispersive X-ray spectroscopy (FE-SEM-EDS) and chemometric methods: application in forensic science*, „Analytical and Bioanalytical Chemistry" 2019, nr 411, s. 3477–3495.

Abstrakt

Eksperci w zakresie badań dokumentów są często proszeni o określenie, czy wydruk pochodzi z określonej drukarki laserowej. Drukarkę rzadko można zidentyfikować, chyba że na wydruku są widoczne jej unikalne wady lub nieprawidłowości. W artykule przedstawiono możliwości identyfikacji i weryfikacji tonerów na wydrukach uzyskanych z różnych drukarek laserowych przy użyciu skaningowej mikroskopii elektronowej. W sumie 21 wydruków uzyskano z 21 różnych modeli maszyn drukujących

[8] Tamże.

Brother i Konica Minolta. Szesnaście wydruków uzyskano z drukarek, w których były oryginalne kasety z tonerem, a pięć z drukarek z zamiennikami. Ustalono jasne kryteria oceny indywidualnej. Na podstawie zdjęć SEM oraz tych kryteriów ujawniono szczegóły topografii struktury tonera. Na podstawie przeprowadzonych badań określono różnice lub podobieństwa tonerów na badanych wydrukach.

Słowa kluczowe: toner, Brother, Konica Minolta, skaningowa mikroskopia elektronowa, mikroanaliza rentgenowska, SEM/EDX.

SEM analysis of black toner on printouts. Part II

Abstract

Document examiners are frequently asked to determine whether or not a printout originated from a particular laser printer. The printer can rarely be identified unless some unique defects or irregularities of the printing are present on the printout. This article presents an overview of a systematic approach to characterizing and discriminating the toner of different laser printers using scanning electron microscopy. A total of twenty-one collected printouts were printed on twenty-one different Brother and Konica Minolta printing machine models. Sixteen printouts were obtained using printers with original toner cartridges while five printouts were obtained using printers with compatible cartridges. Clear criteria were established for individual assessment. Based on the SEM images and established criteria the details of topography of the toner structure were revealed. Due to this study, the differences or similarities of toners on tested printouts were determined. The SEM technique can be successfully, simply, and rapidly applied to the analysis of toners on paper documents.

Keywords: toner, Brother, Konica Minolta, scanning electron microscopy, X-ray microanalysis, SEM/EDX.

RAFAŁ JURCZAK
ORCID: 0000-0001-7850-4549

DOI: 10.4467/20801335PBW.21.007.13564

Analiza mikrośladów trinadtlenku triacetonu (TATP) w fazie gazowej z zastosowaniem TD-GC/MS

Terroryzm – na większą lub mniejszą skalę – był obecny na przestrzeni wieków. Przykładowo, w okresie rewolucji francuskiej terror stanowił „instrument zarządzania" stworzony przez państwo rewolucyjne w celu zaprowadzenia porządku w przejściowym i chaotycznym okresie niepokojów[1]. Zgodnie ze współczesną definicją, zaproponowaną w 1992 r. przez A.B. Schmidta z Wydziału Przestępczości ONZ: *Terroryzm (łac.), różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz państwowych i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych*. W dzisiejszych czasach mamy do czynienia z globalnym wymiarem terroryzmu, który swoim zasięgiem obejmuje wszystkie kontynenty.

Głównym celem ataków terrorystycznych jest zabicie jak największej liczby przypadkowych osób w celu nadania rozgłosu swoim działaniom, wywołania lęku (strachu) w społeczeństwie oraz obnażenia bezradności służb odpowiedzialnych za bezpieczeństwo społeczne[2]. Ugrupowania terrorystyczne często nie dysponują zaawansowanym technologicznie sprzętem. Dlatego, aby osiągnąć zamierzony cel swoich działań, wykorzystują (w większości przypadków) improwizowane urządzenia

---

[1] *Współczesne zagrożenia terroryzmem,* K. Jałoszyński (red. nauk.), Szczytno 2013, s. 22.

[2] C. Pawlak, J. Cichosz, *Współczesny terroryzm narzędziem działań hybrydowych i wyzwaniem dla bezpieczeństwa współczesnego świata*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, nr 1, s. 24.

wybuchowe[3] (IED[4]), skonstruowane w warunkach domowych (zdj. 1). W celu spowodowania jak największych zniszczeń są one przenoszone w specjalnych pasach, kamizelkach, walizkach, torbach przez osoby (PBIED[5]) dokonujące detonacji w określonym miejscu i czasie.

Zdj. 1. Przykłady improwizowanych urządzeń wybuchowych.

Źródło: P. Saska, F. Klimentowski, P. Kowalczyk, *Charakterystyka improwizowanych urządzeń wybuchowych stosowanych w konflikcie irackim*, „Zeszyty Naukowe. Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki" 2008, nr 1, s. 51, 54.

[3] Zgodnie z terminologią wojskową są to: urządzenia wykonane w sposób improwizowany, zawierające niszczące, śmiertelne, szkodliwe środki wybuchowe lub zapalające środki chemiczne przeznaczone do niszczenia, unieszkodliwienia, nękania lub odwracania uwagi. Mogą zawierać materiały wojskowe, ale zwykle są skonstruowane z elementów pochodzących z innych źródeł.

[4] Ang. *improvised explosive device*.

[5] Ang. *person-borne IED*.

Członkowie grup terrorystycznych wymieniają się informacjami w sieci Internet. Czerpią wiedzę m.in. z wydawanego elektronicznie magazynu „Inspire”[6] (zdj. 2).

Zdj. 2. Okładka magazynu „Inspire”.

Źródło: „Inspire” 2010, Summer 1431.

Są w nim zamieszczane teksty, w których niejednokrotnie zachęca się do przeprowadzania ataków na ludność cywilną – zarówno w formie aktów samobójczych, jak i przez spowodowanie zdalnej detonacji materiałów wybuchowych. Pomocne

[6] Magazyn internetowy publikowany przez organizację terrorystyczną Al-Kaida.

miało być zamieszczanie w Internecie m.in. dokładnych instrukcji, jak skonstruować IED[7] (zdj. 3, 4).

Make a bomb in the kitchen of your Mom

The AQ Chef

There are two types of explosions:

First: Chemical explosion. This explosion causes great pressure that would kill living beings within a certain radius. Examples are all the military grade explosives such as TNT, C4 and RDX.

Second: Mechanical explosion. This results from the burning of an inflammable material within a confined space. An example is putting gunpowder inside an iron pipe with a small opening enough only for a fuse. When the gunpowder is ignited, great pressure results from the gunpowder turning into gases and which result in the exploding of the iron pipe, turning it into shrapnel flying at high speed.

I. Preparation of the explosive device:

1. Inflammable substance
2. Decoration lamp (what is normally used for Christmas trees)
3. Iron pipe

A. Preparation of the inflammable substance

This substance is a mixture of two ingredients:
- The substance found in heads of matches
- Sugar

B. How to extract the inflammable substance:

1. Strike the head of the match softly with anything (here, we used a tube) to break up the inflammable substance.
2. Grind the substance and filter it to obtain a fine powder.
3. In the picture you will see the fine powder and you add to it sugar equivalent to ¼ its quantity.
4. Mix the two substances until they become uniform in color.

34

Zdj. 3. Instrukcja sporządzania materiału wybuchowego.

Źródło: AQ Chef, *Make a bomb in the kitchen of your Mom*, „Inspire" 2010, Summer 1431, s. 34.

[7] D. Bianchini, *Person-Borne Improvised Explosive Devices*, Montreal 2014, U.S. Department of Homeland Security, Transportation Security Administration, ICAO Symposium.

Zdj. 4. Instrukcja przygotowania IED.

Źródło: AQ Chef, *Make a bomb in the kitchen of your Mom*, „Inspire" 2010, Summer 1431, s. 35.

Należy zwrócić uwagę, że materiały wybuchowe stosowane w górnictwie i w wojsku, które są trudniejsze do pozyskania ze względu na zwiększoną ich kontrolę, są zastępowane w IED materiałami (mieszaninami) wybuchowymi domowej produkcji. Od połowy lat 90. XX w. ulubioną substancją terrorystów wykorzystywaną do przeprowadzania ataków terrorystycznych na całym świecie jest trinadtlenek triacetonu (TATP[8]). Ten materiał wybuchowy charakteryzuje się wyjątkowo wysoką zdolnością detonacji pod wpływem bodźców zewnętrznych, tj. uderzenia, tarcia, impulsu elektrycznego. TATP jest chętnie używany przez terrorystów z powodu łatwości

[8] Ang. *triacetone triperoxide.*

przygotowania z powszechnie dostępnych produktów, krótkiego czasu syntezy (która ze względu na prostotę nie wymaga wiedzy chemicznej) oraz wyjątkowo dużej siły rażenia porównywalnej z trotylem (TNT[9])[10]. Potwierdza to liczba zdarzeń o charakterze terrorystycznym z ostatnich 15 lat, w których użyto TATP przygotowanego w warunkach domowych (tab. 1).

Tab. 1. Zdarzenia o charakterze terrorystycznym z ostatnich 15 lat z użyciem TATP.

Data przeprowadzenia zamachu	Miejsce ataku	Liczba zabitych
7 lipca 2005 r.	Londyn (Wielka Brytania)	52
13 listopada 2015 r.	Paryż (Francja)	130
22 marca 2016 r.	Bruksela (Belgia)	32
22 maja 2017 r.	Manchester (Wielka Brytania)	23
20 czerwca 2017 r.	Bruksela (Belgia)	0
15 września 2017 r.	Londyn (Wielka Brytania)	29
13 maja 2018 r.	Surabaya (Indonezja)	28
Marzec 2019 r.	Sewilla (Hiszpania)	nieudana próba zamachu
21 kwietnia 2019 r.	Kolombo, Negombo, Madakalapuwa (Sri Lanka)	253

Źródło: Opracowanie własne.

Zagrożenie wywołane atakami terrorystycznymi powoduje zmiany w sferze bezpieczeństwa. To wymaga od służb odpowiedzialnych za bezpieczeństwo wykorzystania zaplecza naukowo-technicznego, aby spełnić oczekiwania społeczeństwa. Jednym z najskuteczniejszych sposobów przeciwdziałania atakom terrorystycznym jest wczesne, szybkie i skuteczne ich wykrywanie. Wymusza to jednocześnie potrzebę opracowania innowacyjnych metod analitycznych w zakresie identyfikacji materiałów wybuchowych, możliwych do wykorzystania przez służby podczas działań operacyjnych.

Najbardziej popularnymi metodami wykrywania klasycznych materiałów wybuchowych oraz nadtlenkowych materiałów wybuchowych (NMW) stosowanymi przez służby odpowiedzialne za bezpieczeństwo i porządek publiczny są:

- spektroskopowe metody analityczne – Raman i FTIR (ang. *Fourier Transform Infrared Spectroscopy*)[11],

[9] 2,4,6-trinitrotoluen.

[10] E.A. Espinosa-Fuentes i in., *A Review of Peroxide Based Homemade Explosives: Characterization and Detection*, Nova Publishers, https://www.researchgate.net/publication/259557168_A_Review_of_Peroxide_Based_Homemade_Explosives_Characterization_and_Detection [dostęp: 13 VI 2020].

[11] L. Nagli, M. Gaft, *Raman scattering spectroscopy for explosives identification,* SPIE. The international society for optics and phothonics, https://spie.org/news/0880-raman-scattering-spectroscopy-for--explosives-identification?SSO=1 [dostęp: 13 VI 2020]; M. Lopez-Lopez, C. Garcia-Ruiz, *Infrared*

- spektrometria mas (ang. *mass spectrometry*, MS)[12],
- spektrometria ruchliwości jonów (ang. *ion-mobility spectrometry*, IMS)[13].

Wychodząc naprzeciw wyzwaniom związanym z NMW, Biuro Badań Kryminalistycznych Agencji Bezpieczeństwa Wewnętrznego (dalej: BBK ABW) opracowało metody identyfikacji i próbkowania TATP z przedmiotów, co do których istnieje podejrzenie kontaktu bezpośredniego lub pośredniego[14] z tym materiałem wybuchowym (podstawą analizy jest detekcja par oraz śladów pozostawionych na powierzchni). Do badania wykorzystuje się chromatograf gazowy (GC)[15] sprzężony ze spektrometrem mas, wyposażony dodatkowo w system do desorpcji termicznej[16] (TD-GC/MS) (zdj. 5).

Zdj. 5. Sprzęt analityczny: chromatograf gazowy sprzężony ze spektrometrem mas oraz z systemem do desorpcji termicznej (widok ogólny – A; widoczny system do termodesorpcji – B); kontroler (C); butla z ciekłym azotem (D).

Źródło: Zdjęcia autora.

---

and Raman spectroscopy techniques appied to identification of explosives, „TrAC Trends in Analytical Chemistry" 2014, t. 54, s. 36–44; C.M. Hodges, J. Akhavan, *The use of Fourier Transform Raman spectroscopy in the forensic identification of illicit drugs and explosives*, „Spectrochimica Acta Part A: Molecular Spectroscopy" 1990, nr 2, s. 303–307.

12 M. Sigman, Cheng-Yu Ma, *Detection Limits for GC/MS Analysis of Organic Explosives*, „Journal of Forensic Sciences" 2001, nr 1, s. 6–11.

13 H. Koyuncu, E. Seven, A. Calimli, *Examination of Some Organic Explosives by Ion Mobility Spectrometry (IMS),* „Turkish Journal of Chemistry" 2005, nr 29, 255–264.

14 Kontrakt pośredni oznacza, że przedmiot znajdował się w bezpośrednim otoczeniu materiału wybuchowego.

15 Chromatografia gazowa (ang. *gas chromatography*, GC) – przyp. red.

16 Ang. *thermal desorption*.

Sposoby próbkowania analitów

Próbkowanie bezpośrednie polega na manualnym umieszczeniu fragmentu materiału (przedmiotu) w szklanej tubie (zdj. 6). W celu optymalizacji procesu należy zwrócić uwagę na kilka istotnych czynników. Aby uzyskać wyniki reprezentatywne dla całej próbki, materiał wprowadzany do tuby powinien mieć masę do 10 mg, być jednorodny, mieć wystarczająco dużą powierzchnię, co ułatwia dyfuzję analitów[17], np. fragment tkaniny bawełnianej o wymiarach 5 mm × 10 mm.

Zdj. 6. Aparatura do próbkowania bezpośredniego w postaci tuby pustej[18].

Źródło: Zdjęcie autora.

Próbkowanie pośrednie polega na przetłaczaniu określonej ilości gazu przez rurę adsorpcyjną zawierającą złoże TENAX TA. Do przetłoczenia gazu wykorzystuje się aspirator, który wymusza ruch powietrza i jego przetłoczenie przez rurkę (zdj. 7). Gazy atmosferyczne przechodzą przez rurę, a molekuły substancji o większej masie cząsteczkowej (tj. opary materiałów wybuchowych) zostają adsorbowane na złożu rurki.

Zdj. 7. Aparatura do próbkowania pośredniego składająca się z aspiratora oraz tuby desorpcyjnej TENAX TA[19].

Źródło: Zdjęcie autora.

---

[17] Analit – składnik próbki analitycznej podlegający oznaczaniu. Analit może być składnikiem roztworu, mieszaniny gazów lub ciała stałego, za: https://pl.wikipedia.org/wiki/Analit [dostęp: 10 XII 2020] – przyp. red.

[18] Ang. *empty thermal desorption tubes*.

[19] *Choosing the Right Adsorbent for your Thermal Desorption Gas Chromatography Applications*, Separation Science Webinar, 22 X 2013 r., https://www.sigmaaldrich.com/content/dam/sigma-aldrich/docs/Supelco/Posters/1/Adsorbent-Selection-TD-GC-Apps.pdf [dostęp: 14 VI 2020].

Mechanizm desorpcji termicznej z zastosowaniem systemów GERSTEL TDS 3 i GERSTEL CIS firmy GERSTEL

Szklana tuba z analitem[20] jest wprowadzana do pieca TDS 3. Następuje jej płukanie obojętnym gazem nośnym (helem) oraz ogrzewanie w określonych warunkach temperaturowych. Zaadsorbowane substancje na matrycy lub złożu TENAX TA ulegają desorpcji[21], a następnie przez kapilarę transferową wraz z gazem nośnym są wypłukiwane do szklanej wkładki wchodzącej w skład systemu GERSTEL CIS. Ten element, dzięki zastosowaniu zewnętrznego chłodzenia ciekłym azotem w kontrolowanych warunkach niskiej temperatury, odgrywa rolę bardzo sprawnego koncentratora analizowanych substancji (tzw. pułapki analitów). Następnie układ termodesorbera GERSTEL CIS zostaje gwałtownie ogrzany, co powoduje bezpośrednie dozowanie stężonego analitu ze szklanej wkładki do kolumny chromatograficznej (systemu GC/MS) w celu dalszej jego analizy. Połączenie GERSTEL TDS 3 oraz GERSTEL CIS (zdj. 8) tworzy bardzo sprawny system, który może działać zarówno w trybie z podziałem próbki[22], jak i bez podziału[23]. To umożliwia uzyskanie szerokiego zakresu analiz – od analiz śladowych do analiz bardzo stężonych próbek[24].

Zdj. 8. Budowa systemu GERSTEL TDS 3 oraz GERSTEL CIS.

Źródło: *Thermal Desorption System TDS*, Global Analytical Solution, Gerstel, https://www.gerstel.com/en/thermal-desorption-system-tds.htm [dostęp: 14 VI 2020].

---

[20] Analit jest próbkowany jednym z przedstawionych sposobów – pośrednim lub bezpośrednim.

[21] Zwiększenie lotności w celu odseparowania od stałej matrycy.

[22] Jedynie określona część dozowanej próbki jest wprowadzana do kolumny chromatograficznej. Podział próbki stosuje się w przypadku próbek o dużym stężeniu analitu, aby zapobiec niepożądanym zjawiskom podczas rozdziału chromatograficznego.

[23] Dozowana próbka trafia w całości do kolumny chromatograficznej (analiza śladowa).

[24] *System desorpcji termicznej TDS 3 z kontrolerem C506*; GERSTEL, podręcznik użytkownika dostarczony wraz ze sprzętem przez producenta, firmę Gerstel.

Prężność par materiałów wybuchowych

W identyfikacji materiałów wybuchowych (przeprowadzonej metodą wskazaną w artykule) decydującą rolę odgrywa właściwość fizyczna związku – prężność par. W tabeli 2 przedstawiono prężność par wybranych materiałów wybuchowych w warunkach standardowych[25].

Tab. 2. Porównanie wybranych materiałów wybuchowych i prężności ich par.

Materiał wybuchowy	Wzór strukturalny	Prężność par [mm Hg]
Trinadtlenek triacetonu (TATP)		$5{,}21 \times 10^{-2}$
Nitrogliceryna (NG)		$2{,}6 \times 10^{-6}$
Trinitrotoluen (TNT)		$1{,}1 \times 10^{-6}$
Heksogen (RDX)		$4{,}1 \times 10^{-9}$
Pentryt (PETN)		$3{,}8 \times 10^{-10}$
Oktogen (HMX)		$3{,}3 \times 10^{-14}$

Źródło: Opracowanie własne.

[25] J. Wojtas i in., *Projekt układu zatężania i dekompozycji par materiałów wybuchowych*, „Przegląd Elektrotechniczny" 2010, nr 11a, s. 225.

Analizując powyższe dane, można stwierdzić, że wysoka prężność par TATP zwiększa skuteczność wykrywania i identyfikacji tego materiału z wykorzystaniem zjawiska adsorpcji, co umożliwia wykonanie analizy nawet w ilościach śladowych. W przypadku trinitrotoluenu i nitrogliceryny znacznie mniejsza prężność par będzie wpływała na obniżenie progu wykrywania tych substancji, a w przypadku oktogenu, pentrytu i heksogenu prężność par jest znikoma, co wręcz uniemożliwi przeprowadzenie analizy metodą opisaną w artykule.

Duży wpływ na intensywność parowania materiałów wybuchowych mają warunki oraz sposób ich przechowywania, tj. tworzywo, z którego opakowanie jest wykonane, szczelność opakowania, temperatura oraz wilgotność powietrza podczas przechowywania.

Synteza TATP

W celu wykonywania testów próbki TATP były przygotowywane w warunkach laboratoryjnych zgodnie z przepisem: do mieszaniny acetonu oraz nadtlenku wodoru 60%, chłodzonej lodem, dodano kwas solny 36%, a następnie w celu dokonania całkowitej krystalizacji odstawiono na 24 godziny do lodówki. Wytrącone kryształy przemyto wodą oraz 5% roztworem węglanu sodu do uzyskania pH neutralnego (pH około 7)[26]. Reakcję chemiczną przestawiono na schemacie 1.

Schemat 1. Synteza TATP. W celach terrorystycznych do syntezy są używane produkty powszechnie dostępne, których zakup oraz posiadanie nie są w żaden sposób kontrolowane.

Źródło: https://pl.wikipedia.org/wiki/Nadtlenek_acetonu [dostęp: 14 VI 2020].

Na schemacie 2 oraz na zdj. 9 zaprezentowano substraty potrzebne do syntezy TATP.

[26] Sposób syntezy zaczerpnięty z projektu Narodowego Centrum Badań i Rozwoju pt. „Projektowanie badań empirycznych i analizy materiałów dotyczących specyfiki metod kryminalistyki w pracy służb specjalnych służb porządku publicznego", projekt nr 0023/R/ID3/2012/02 z 30 lipca 2012 r.

Schemat 2. Substraty powszechnego użytku wykorzystywane w syntezie TATP.

Źródło: Opracowanie własne na podstawie: www.vmc.org.pl; R. Matyáš, J. Šelešovský, T. Musil, *Study of TATP: Mass Loss and Friction Sensitivity During Ageing*, „Central European Journal of Energetic Materials" 2012, nr 3, s. 255; Karty charakterystyk substancji chemicznych – acetonu, nadtleneku wodoru, kwasu siarkowego (VI), kwasu azotowego, kwasu solnego, węglanu sodu, CEMPUR, www.chempur.pl/katalog/karty-charakterystyk/ [dostęp: 14 VI 2020].

Wykonanie: Aleksandra Bednarczyk.

Zdj. 9. Postać handlowa produktów służących do syntezy TATP: aceton techniczny, nadtlenek wodoru, elektrolit (kwas siarkowy), soda oczyszczona, woda destylowana.

Źródło: Zdjęcie autora.

W środkach masowego przekazu, m.in. w Internecie, istnieją liczne fora hobbystów (entuzjastów) materiałów wybuchowych, których użytkownicy wymieniają się podstawowymi informacjami, np. skąd pozyskać surowce do syntezy, jak można zastąpić sprzęt laboratoryjny sprzętem używanym w domu, jakie środki bezpieczeństwa należy zachować, jak również dokładnymi opisami syntezy (zdj. 10–14). W swoich wypowiedziach podpierają się literaturą naukową oraz własnymi doświadczeniami. Łatwość zdobycia tych informacji powoduje stałe zagrożenie bezpieczeństwa publicznego w każdym rejonie świata.

A

B

C

D

Zdj. 10. Synteza TATP w warunkach domowych: suszenie TATP na podłodze w pokoju (A); synteza TATP (B); produkt syntezy TATP w formie proszku (granulek) (C) lub splastyfikowanej[27] (D).

Źródło: *First Responders Toolbox*, NCTC ID 10-19, 1 X 2019, s. 1.

[27] Plastyfikacja – zmiękczanie, nadanie elastyczności, za: sjp.pwn.pl/sjp.plastyfikacja;2571678 [dostęp: 10 X 2020] – przyp. red.

OSJ SPECIAL MAKING THE HIDDEN BOMB

A.3 Sulfuric Acid

Also known as clear battery acid. In this process, we are going to use it directly while it's dilute: without concentrating it.

B MAKING THE DETONATING MATERIAL

I. Assemble all materials and tools needed in this process.

NOTE

When preparing the detonating material, **DO NOT USE METALLIC** utensils. Rely on plastic or glass. Use medical syringe taking measurements and stirring.

82 | INSPIRE | Al-Malahem Media | 2014

Zdj. 11. Instrukcja syntezy TATP w warunkach domowych – niezbędne odczynniki i akcesoria.

Źródło: AQ Chef, *Making the hidden bomb*, „Inspire" 2014, Winter 1436, s. 82.

OSJ SPECIAL: MAKING THE HIDDEN BOMB.

II. Pour 20 ml of acetone and 20 ml of hydrogen peroxide in a glass. Stir well.

SAFETY

It is better to cool the mixture before adding the acid.

NOTE

In our experiments, we used home-made acetone by following the procedure in pg 99.

III. Add 6 ml of clear battery acid in quick drops as you stir quickly.

IV. Wait for 1 - 2 hours in room temperature (20°C - 30°C). You will see a white precipitate (solid) forming.

V. Transfer the mixture into another glass, the white solid will float.

BEFORE

AFTER

83

Zdj. 12. Instrukcja syntezy TATP w warunkach domowych – instrukcja mieszania składników.

Źródło: AQ Chef, *Making the hidden bomb*, „Inspire" 2014, Winter 1436, s. 83.

Zdj. 13. Instrukcja syntezy TATP w warunkach domowych – otrzymanie produktu końcowego.

Źródło: AQ Chef, *Making the hidden bomb*, „Inspire" 2014, Winter 1436, s. 84.

Zdj. 14. Instrukcja przygotowania detonatora.

Źródło: AQ Chef, *Making the hidden bomb*, „Inspire" 2014, Winter 1436, s. 85.

Sprawdzenie skuteczności zastosowanej metody przez wyznaczenie granicy wykrywalności

Granica wykrywalności (ang. *detection limit*, DL) jest to najmniejsze wykrywalne stężenie analitu w próbce generujące sygnał, który jest możliwy do odróżnienia od sygnału

pochodzącego ze ślepej próby (tła)[28]. Przyjmuje się, że granica wykrywalności powinna wynosić ~ ≥ 3 w stosunku do sygnału pochodzącego od szumu (wyrażone symbolem S/N). Na wykresach 1–3 zaprezentowano uzyskane wyniki.

Wykres 1. Chromatogram otrzymany z TD-GC/MS w trybie skanowania mas SCAN[29]. Pik przy czasie retencji 13,78 odpowiada TATP. Granica wykrywalności została wyznaczona na poziomie 1 ppb[30].

Źródło: Opracowanie własne.

Wykres 2. Chromatogram otrzymany z TD-GC/MS w trybie skanowania mas SIM[31] (43, 58, 75 m/z). Pik przy czasie retencji 13,74 odpowiada TATP. Granica wykrywalności została wyznaczona na poziomie 1 ppt[32].

Źródło: Opracowanie własne.

---

28 W. Szczepaniak, *Metody instrumentalne w analizie chemicznej*, Warszawa 2007, s. 39–40.

29 Tryb pełnego skanowania w zakresie wskazanych mas. Typowy zakres skanowania mas wynosi od 35 do 500 m/z (stosunek masy do ładunku jonów – dop. red.). Tryb pełnego skanowania jest szczególnie przydatny przy identyfikacji związków w próbce nieznanego pochodzenia.

30 Ang. *parts per bilion* (10^{-9}).

31 Ang. *selected ion monitoring*. Charakteryzuje się on rejestrowaniem mas charakterystycznych dla danego związku. Dzięki zmniejszeniu szumu tła oraz zwiększeniu sygnału właściwego piku zwiększa się znacznie selektywność i obniża limit detekcji podczas pomiaru.

32 Ang. *parts per trillion* (10^{-12}).

Wykres 3. Widmo masowe TATP (syntezowanego zgodnie instrukcją przedstawioną na zdjęciach 10–14), uzyskane z chromatografu gazowego sprzężonego ze spektrometrem mas.

Źródło: Opracowanie własne.

Przygotowanie próbek rzeczywistych

W BBK ABW wykonano doświadczenia z materiałami wybuchowymi. Zostały one przeprowadzone według trzech scenariuszy.

Doświadczenie 1. Analiza słuchawki telefonu stacjonarnego po wybuchu. Z przygotowanego przez BBK ABW materiału wybuchowego TATP wykonano improwizowane urządzenia wybuchowe, umieszczając nadtlenkowy materiał wybuchowy w słuchawce telefonu stacjonarnego (zdj. 15). Następnie zainicjowano wybuch za pomocą lontu wolnopalnego. Zabezpieczony materiał powybuchowy poddano analizie z zastosowaniem chromatografii gazowej sprzężonej ze spektrometrem mas wyposażonym w system do termodesorpcji (TD-GC/MS).

A

B

Zdj. 15. Słuchawka telefonu stacjonarnego, w której umieszczono improwizowany materiał wybuchowy (15 g TATP flegmatyzowanego[33] 7,5 g celulozy) (A); zabezpieczony materiał powybuchowy (B).

Źródło: Zdjęcie autora.

[33] Flegmatyzacja – dodanie do materiału wybuchowego substancji obniżającej jego wrażliwość na bodźce mechaniczne, za: pl.wikipedia.org/wiki/Flegmatyzacja [dostęp: 10 XII 2020] – przyp. red.

Doświadczenie 2. Analiza kabla telefonu stacjonarnego z doświadczenia 1 pod kątem identyfikacji śladowych ilości materiału wybuchowego rozrzuconych w wyniku wybuchu. Kabel telefonu z doświadczenia 1 nie miał bezpośredniego kontaktu z materiałem wybuchowym umieszczonym w słuchawce telefonu.

Zdj. 16. Kabel od telefonu stacjonarnego użytego w doświadczeniu 1.

Źródło: Zdjęcie autora.

Doświadczenie 3. Analiza myszki komputerowej po wybuchu. Z przygotowanego przez BBK ABW materiału wybuchowego TATP wykonano improwizowane urządzenia wybuchowe przez umieszczenie nadtlenkowego materiału wybuchowego w myszce komputerowej, a następnie zainicjowano wybuch za pomocą lontu wolnopalnego. Zabezpieczony materiał powybuchowy poddano analizie z zastosowaniem chromatografii gazowej sprzężonej ze spektrometrem mas wyposażonym w system do termodesorpcji (TD-GC/MS).

A

B

Zdj. 17. Improwizowany materiał wybuchowy (10 g TATP flegmatyzowanego 5 g celulozy) umieszczony w myszce komputerowej (A); zabezpieczony materiał powybuchowy (B).

Źródło: Zdjęcie autora.

W tabeli 3 zestawiono wyniki przeprowadzonych doświadczeń 1–3 przy uwzględnieniu najważniejszych parametrów próbkowania i analitycznych.

Tab. 3. Wyniki doświadczeń 1–3.

Parametry próbkowania i analityczne	Opis
Systemy próbkowania	pośredni – zasysanie analitu z atmosfery opakowania zewnętrznego (torebka plastikowa z zamknięciem strunowym) zawierającego materiał powybuchowy na złoże TENAX TA
Prędkość przepływu gazów podczas próbkowania	100 ml/min
Całkowita objętość pobranych gazów podczas próbkowania	500 ml
Systemy desorpcji termicznej	desorpcja termiczna ze złoża TENAX TA
Tryb pracy spektrometru mas	SCAN
Wynik identyfikacyjny	potwierdzono wykorzystanie TATP w badanych improwizowanych materiałach wybuchowych

Źródło: Opracowanie własne.

Doświadczenie 4. Badanie zabezpieczonych rękawiczek nitrylowych wykorzystywanych przez osobę wykonującą syntezę 300 g TATP (zdj. 18). Materiał dowodowy nie miał bezpośredniego kontaktu z NMW.

Zdj. 18. Materiał dowodowy (rękawiczki nitrylowe) umieszczone w torebce foliowej z zamknięciem strunowym.

Doświadczenie 5. Analiza powietrza na wysokości 50 cm od miejsca syntezy 300 g TATP (zdj. 19).

Zdj. 19. Aparatura do pobierania próbki powietrza w miejscu wytwarzania TATP.

Źródło: Zdjęcie autora.

W tabeli 4 zestawiono wyniki przeprowadzonych doświadczeń 4 i 5 przy uwzględnieniu najważniejszych parametrów próbkowania i analitycznych.

Tab. 4. Wyniki doświadczeń 4–5.

Parametry próbkowania i analityczne	Opis
Systemy próbkowania	pośredni – zasysanie analitu z atmosfery opakowania zewnętrznego oraz atmosfery w pomieszczeniu na złoże TENAX TA
Prędkość przepływu podczas próbkowania	100 ml/min
Całkowita objętość pobranych gazów podczas próbkowania	doświadczenie 4: 500 ml
	doświadczenie 5: 1500 ml
Systemy desorpcji termicznej	desorpcja termiczna ze złoża TENAX TA
Tryb pracy spektrometru mas	SIM
Wynik identyfikacyjny	potwierdzono TATP w badanej próbce, która nie miała bezpośredniego kontaktu z materiałem wybuchowym (doświadczenie 4) oraz zidentyfikowano TATP w postaci oparów w pomieszczeniu (doświadczenie 5)

Źródło: Opracowanie własne.

Doświadczenie 6. Analiza materiałów wystawionych na ekspozycję oparów TATP. Zbitek włosów ludzkich oraz kawałek tkaniny bawełnianej umieszczono w otwartym eksykatorze bezpośrednio nad próbką 10 mg TATP, pozostawiając na ekspozycję par na 24 godziny (zdj. 20). Po tym czasie materiały usunięto z eksykatora i przechowywano w warunkach pokojowych (temp. 20°C) przez 36 dni, a następnie poddano analizie identyfikacyjnej (zdj. 21).

Zdj. 20. Przygotowanie próbek do przeprowadzenia doświadczenia 6.

Zdj. 21. Bezpośrednie próbkowanie analitów z materiałów przygotowanych w doświadczeniu 6 (włosy ludzkie oraz tkanina bawełniana).

W tabeli 5 zestawiono wyniki przeprowadzonego doświadczenia 6 przy uwzględnieniu najważniejszych parametrów próbkowania i analitycznych.

Tab. 5. Wyniki doświadczenia 6.

Parametry próbkowania i analityczne	Opis
Systemy próbkowania	bezpośredni – umieszczenie materiału w szklanej tubie
Prędkość przepływu podczas próbkowania	nie dotyczy
Całkowita objętość pobranych gazów podczas próbkowania	nie dotyczy
Systemy desorpcji termicznej	desorpcja termiczna bezpośrednio z materiału dowodowego
Tryb pracy spektrometru mas	SIM
Wynik identyfikacyjny	po 36 dniach przechowywania w warunkach pokojowych zidentyfikowano TATP

Podsumowanie

Wykonane optymalizacje parametrów chromatograficznych, spektroskopowych i termodesorpcyjnych pozwoliły na stworzenie metody badawczej do identyfikacji śladowych ilości TATP z przedmiotów, które miały bezpośredni kontakt lub znajdowały się w bezpośrednim otoczeniu materiału wybuchowego. Do tego celu wykorzystano chromatografię gazową sprzężoną ze spektrometrią mas wyposażoną w system do termodesorpcji (TD-GC/MS). Wskazana metodyka przedstawia nowatorskie wykorzystanie sprzętu TD-GC/MS w identyfikacji materiałów wybuchowych z grupy nadtlenków.

Należy zwrócić uwagę również na zastosowane sposoby próbkowania. W próbkowaniu pośrednim nie ma bezpośredniego kontaktu między sprzętem próbkującym a matrycą[34], co powoduje, że nie ma ingerencji w materiał dowodowy. Jest to szczególnie istotne podczas prowadzenia czynności w sposób niejawny, maksymalnie konspirujący zainteresowanie służb. Jednocześnie sposób próbkowania bezpośredniego w zestawieniu z bardzo czułym sprzętem analitycznym TD-GC/MS (dzięki zastosowaniu przekierowanej desorpcji termicznej[35]) umożliwia identyfikację nadtlenku już nawet w nanogramowych ilościach[36]. W toku przeprowadzonych badań wyznaczono granicę wykrywalności dla TATP w trybie skanowania mas SCAN na poziomie 1 ppb oraz w trybie skanowania mas SIM na poziomie 1 ppt.

Rozwiązanie analityczno-sprzętowe przedstawione w niniejszej pracy jest podstawą do stworzenia bardziej zaawansowanych koncepcji w zakresie sposobu próbkowania, a także rozwoju metodyki analitycznej powiększonej o nowo dodane związki. Należy jednak pamiętać o jednym podstawowym ograniczeniu – opisane metody można

[34] Może nią być: ubranie, ziemia, przedmioty.

[35] Odgrywająca rolę koncentratora analitów „zimna pułapka".

[36] Inaczej – nanoślady (zawartość składników w próbce 10^{-11} – 10^{-14} %; Wojtas J. i in., *Projekt układu zatężania*… s. 225–226.

stosować jedynie do klasycznych materiałów wybuchowych oraz NMW charakteryzujących się odpowiednio wysokim poziomem prężności par[37]. Im większa wartość tego parametru, tym lepsza skuteczność wykrywania danego związku.

Bibliografia

AQ Chef, *Make a bomb in the kitchen of your Mom*, „Inspire" 2010, Summer 1431.

AQ Chef, *Making the hidden bomb*, „Inspire" 2014, Winter 1436.

Bianchini D., *Person-Borne Improvised Explosive Devices*, Montreal 2014, U.S. Department of Homeland Security, Transportation Security Administration, ICAO Symposium.

Hodges C.M., Akhavan J., *The use of Fourier Transform Raman spectroscopy in the forensic identification of illicit drugs and explosives*, „Spectrochimica Acta, Part A: Molecular Spectroscopy" 1990, nr 2, s. 303–307.

Koyuncu H., Seven E., Calimli A., *Examination of Some Organic Explosives by Ion Mobility Spectrometry (IMS)*, „Turkish Journal of Chemistry" 2005, nr 29, s. 255–264.

Lopez-Lopez M., Garcia-Ruiz C., *Infrared and Raman spectroscopy techniques appied to identification of explosives,* „TrAC Trends in Analytical Chemistry" 2013, t. 54, s. 36–44.

Matyáš R., Šelešovský J., Musil T., *Study of TATP: Mass Loss and Friction Sensitivity During Ageing*, „Central European Journal of Energetic Materials" 2012, nr 3, s. 251–260.

Pawlak C., Cichosz J., *Współczesny terroryzm narzędziem działań hybrydowych i wyzwaniem dla bezpieczeństwa współczesnego świata*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, nr 1, s. 23–35.

Projektowanie badań empirycznych i analizy materiałów dotyczących specyfiki metod kryminalistyki w pracy służb specjalnych służb porządku publicznego, Narodowe Centrum Badań i Rozwoju, projekt nr 0023/R/ID3/2012/02 z 30 lipca 2012 r.

Saska P., Klimentowski F., Kowalczyk P., *Charakterystyka improwizowanych urządzeń wybuchowych stosowanych w konflikcie irackim*, „Zeszyty Naukowe. Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki" 2008, nr 1, s. 41–57.

Sigman M., Ma Cheng-Yu, *Detection Limits for GC/MS Analysis of Organic Explosives*, „Journal of Forensic Sciences" 2001, nr 1, s. 6–11.

Szczepaniak W. *Metody instrumentalne w analizie chemicznej*, Warszawa 2007, Wydawnictwo Naukowe PWN.

[37] J. Bokszczanin, T. Ludwikowski, A. Wawro, *Detektor MO-2M jako urządzenie do wykrywania materiałów wybuchowych,* http://www.konferencja.home.pl/materialy2/11.pdf [dostęp: 14 VI 2020].

Wojtas J. i in., *Projekt układu zatężania i dekompozycji par materiałów wybuchowych*, „Przegląd Elektrotechniczny" 2010, nr 11a, s. 225–228.

Współczesne zagrożenia terroryzmem, K. Jałoszyński (red. nauk.), Szczytno 2013, Wydawnictwo Wyższej Szkoły Policji w Szczytnie.

Źródła internetowe

Bokszczanin J., Ludwikowski T., Wawro A., *Detektor MO-2M jako urządzenie do wykrywania materiałów wybuchowych*, http://www.konferencja.home.pl/materialy2/11.pdf [dostęp: 13 VI 2020].

Espinosa-Fuentes E.A. i in., *A Review of Peroxide Based Homemade Explosives: Characterization and Detection*, Nova Publishers, https://www.researchgate.net/publication/259557168_A_Review_of_Peroxide_Based_Homemade_Explosives_Characterization_and_Detection [dostęp: 13 VI 2020].

Nagli L., Gaft M., *Raman scattering spectroscopy for explosives identification,* SPIE. The international society for optics and phothonics, https://spie.org/news/0880-raman-scattering--spectroscopy-for-explosives-identification?SSO=1 [dostęp: 13 VI 2020].

Thermal Desorption System TDS, Global Analytical Solution, Gerstel, https://www.gerstel.com/en/thermal-desorption-system-tds.htm [dostęp: 13 VI 2020].

Triacetone Triperoxide (TATP): Indicators of Acquisition and Manufacture, and Considerations for Response, https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/78--NCTC-DHS-FBI---Triacetone-Triperoxide-(TATP)-.pdf [dostęp: 13 VI 2020].

Abstrakt

W artykule opisano metodykę wykrywania trinadtleneku triacetonu (TATP) w postaci par oraz śladów powierzchniowych z wykorzystaniem chromatografi gazowej sprzężonej ze spektrometrią mas wyposażoną w system do termodesorpcji (TD-GC/MS). Rozwiązania techniczne aparatury analitycznej umożliwiają wybór jednej z dwóch metod wprowadzenia par analitu w celu identyfikacji – pośrednio ze złoża TENAX TA lub bezpośrednio z obiektów badań. Dodatkowo zastosowanie elementu GERSTEL CIS odgrywającego rolę koncentratora substancji powoduje, że jest możliwa identyfikacja już nawet nanośladowych ilości TATP. W artykule przedstawiono schemat działania termodesorpcji w TD-GC/MS z jednoczesnym zwróceniem uwagi na cechy fizyczne substancji warunkujące osiągnięcie zadowalających wyników.

Słowa kluczowe: identyfikacja, TATP, prężność par, termodesorpcja, terroryzm.

Micro-traces analysis of triacetone triperoxide (TATP) in the form of vapours using TD-GC/MS

Abstract

The article discusses the method of detecting triacetone triperoxide (TATP) in the form of vapours and surface traces using gas chromatography with a thermal desorption system of mass spectrometry (TD-GC/MS). The technical solutions of analytical equipment make it possible to choose one or two methods for introducing analyte vapour for identification – indirectly from the TENAX TA deposit or directly from the research objects. In addition, the use of the GERSTEL CIS element as a substance concentrator renders identification of even nano-trace amounts of TATP possible. The article presents the experimental procedure of the thermal desorption TD-GC/MS and simultaneously draws attention to physical properties of the substance determining the achievement of satisfactory results.

Keywords: identification, TATP, vapour pressure, thermal desorption, terrorism.

TOMASZ SZCZEPAŃSKI
ORCID: 0000-0002-0157-6293

URSZULA WIĘCKIEWICZ
ORCID: 0000-0002-6993-0869

BARBARA KONIOR
ORCID: 0000-0003-2492-7276

PATRYK PUCUŁEK
ORCID: 0000-0003-3644-6541

DOI: 10.4467/20801335PBW.21.008.13565

Wpływ dezynfekcji pomieszczeń ozonem na skuteczność ujawniania śladów daktyloskopijnych na powierzchni papieru metodą DFO w dobie pandemii SARS-CoV-2

Obserwowany od początku 2020 r. gwałtowny wzrost zachorowań na COVID-19 wywołanych zakażeniem koronawirusem SARS-CoV-2 (ang. *Severe acute respiratory syndrome coronavirus 2*) oraz ogłoszenie w marcu ubiegłego roku przez WHO stanu pandemii spowodowały zwiększenie zainteresowania technikami dezynfekcji niszczącymi przede wszystkim wirusy. Jedną z takich metod jest ozonowanie. Niebezpieczeństwo zakażenia może wynikać z kontaktu materiału, np. przesyłki pocztowej, z nosicielem wirusa, szczególnie asymptomatycznym. Możliwe jest także intencjonalne skierowanie skażonego listu w celu wywołania zagrożenia. Wymusza to wypracowanie skutecznej metody dezynfekcji, która zapewni względne bezpieczeństwo odbiorcom. Jednocześnie aby umożliwić ewentualną identyfikację nadawcy, w tym m.in. na podstawie śladów daktyloskopijnych, niezwykle istotne jest stosowanie takich technik dezynfekcji, które nie zniszczą śladów kryminalistycznych. Ponadto, z punktu widzenia czynności wykrywczych, jest ważne ustalenie, czy ślady daktyloskopijne pozostawione na podłożu papierowym (np. list, koperta, dokument) poddanym ozonowaniu nie ulegają zniszczeniu.

W czasie pandemii i realnego zagrożenia infekcją wirusem SARS-CoV-2 warto przytoczyć kilka faktów. Koronawirusy, a dokładnie cztery serotypy HCoV (ang. *human coronavirus*): HCoV-229E, HCoV-OC43, HCoV-NL63, HCoV-UKU1, są od lat

odpowiedzialne za przeziębienia i infekcje grypopodobne u ludzi[1]. Szacuje się, że powodują 2–10 proc. zimowych lub wczesnowiosennych przeziębień z pojawiającymi się co dwa–cztery lata epidemiami[2]. Będący przyczyną obecnej pandemii SARS-CoV-2 jest siódmym znanym wirusem infekującym człowieka należącym do rodziny *Coronaviridae*. Pierwszy ludzki koronawirus powodujący zagrażającą życiu infekcję dolnych dróg oddechowych – ostrą niewydolność oddechową, oznaczony jako SARS-CoV, pojawił się w Chinach w 2002 r.[3] Równie groźny okazał się kolejny koronawirus MERS-CoV (ang. *Middle East respiratory syndrome coronavirus*), który tym razem pojawił się na Półwyspie Arabskim w 2012 r. Jednak zarówno SARS-CoV, jak i MERS-CoV nie spowodowały pandemii, mimo że przypadki infekcji odnotowano w wielu krajach na różnych kontynentach.

Ludzkie koronawirusy (HCoV) są w stanie zachować infekcyjność w temperaturze pokojowej na różnych powierzchniach nawet do 9 dni[4]. Badania dotyczące obecności koronawirusa SARS-CoV-2 na konkretnych podłożach wskazują na jego większą stabilność na powierzchni plastiku i stali nierdzewnej niż na miedzi i tekturze. Wirus w formie umożliwiającej zakażenie był wykrywany na plastiku do 72 godzin w temperaturze 21–22°C, przy wilgotności 40 proc. RH[5], przy czym znacząco zmniejszała się jego ilość w czasie. Na tekturze, w podobnych warunkach, wirus zdolny do wywołania infekcji był wykrywany do 24 godzin[6]. Kolejne badania dotyczyły określenia wpływu temperatury na stabilność SARS-CoV-2 na różnych powierzchniach. Należy podkreślić, że w trakcie tych badań wyeliminowano wpływ promieniowania UV; próbki przechowywano w ciemności, przy stałej wilgotności 50 proc. RH. W temperaturze 20°C na szkle, polimerowych i papierowych banknotach, stali nierdzewnej oraz tworzywie sztucznym (winylu) SARS-CoV-2 był wykrywany nawet przez 28 dni od momentu naniesienia. Na bawełnianej tkaninie SARS-CoV-2 nie był wykrywany już po 14 dniach. Wzrost temperatury o 10°C skracał czas obecności SARS-CoV-2 na stali nierdzewnej, polimerowych banknotach i szkle do 7 dni, natomiast na winylu i bawełnianej tkaninie do 3 dni. Przy tej temperaturze SARS-CoV-2 na powierzchni papierowych banknotów był wykrywany nawet do 21 dni od momentu naniesienia. Znaczną redukcję obecności wirusa SARS-CoV-2 na badanych powierzchniach notowano przy 40°C: na bawełnianej tkaninie nie stwierdzono jego obecności już

---

1 M.G. Hemida. M.M. Ba Abduallah, *The SARS-CoV-2 outbreak from a one health perspective*, „One Health" 2020, t. 10, https://doi.org/10.1016/j.onehlt.2020.100127 [dostęp: 16 III 2020].

2 L. Collier, J. Oxford, *Wirusologia. Podręcznik dla studentów medycyny, stomatologii i mikrobiologii*, M. Łuczak (red.), tłum. M.M. Krajewska, Warszawa 1996, s. 134–135.

3 W. Irving, D. Ala'Aldeen, T. Boswell, *Mikrobiologia medyczna*, Warszawa 2008, s. 90.

4 G. Kampfi i in., *Persistence of coronaviruses on inanimate surfaces and their inactivation with biocidal agents*, „Journal of Hospital Infection" 2020, t. 104, s. 246–251.

5 Ang. *Relative Humidity* – dopuszczalna względna wilgotność otoczenia (przyp. red.).

6 N. van Doremalen i in., *Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS-CoV-1*, „The New England Journal Medicine" 2020, nr 16, s. 1564–1567, https://www.nejm.org/doi10.1056/NEJMc2004973 [dostęp: 13 X 2020].

po 24 godzinach, a na pozostałych badanych podłożach – po 48 godzinach[7]. Badania przeprowadzone przez kanadyjskich naukowców wykazały obecność wirusa SARS-CoV-2: na plastiku – 21 dni od momentu naniesienia, na stali nierdzewnej – 14 dni od momentu naniesienia, na nitrylowych rękawiczkach – 7 dni od momentu naniesienia, na chemoodpornych rękawiczkach – 4 dni od momentu naniesienia, na maskach filtracyjnych typu N-95 i N-100 – 21 dni od momentu naniesienia, na kombinezonie Tyvek® – 14 dni od momentu naniesienia. W przypadku bawełny SARS-CoV-2 nie był wykrywany po 24 godzinach od pozostawienia. Należy nadmienić, że te podłoża przechowywano w temperaturze 20°C i wilgotności 40 proc. RH[8].

Przytoczone dane dotyczące między innymi tworzyw sztucznych i tektury nie zostały wybrane przypadkowo. Obiektami badań daktyloskopijnych są często paczki oraz różnego rodzaju przesyłki. Paczki są wykonane powszechnie z tektury, miejscami oklejonej taśmą z tworzywa sztucznego. Przesyłki listowe to zazwyczaj papierowa koperta, która zawiera czasem okienko z przezroczystego tworzywa sztucznego. Niezależnie od pandemii wywołanej wirusem SARS-CoV-2 zagrożeniem mogą być także inne niebezpieczne patogeny, szczególnie te powodujące infekcje o wysokiej śmiertelności, jak wąglik, dżuma, ospa, wirus gorączki krwotocznej.

Konieczność dezynfekcji wszystkich dotykanych powierzchni, zwłaszcza w dobie pandemii, potwierdzają badania przeprowadzone w Singapurze. Wykryto RNA koronawirusa SARS-CoV-2 na większości powierzchni w pomieszczeniu, w którym przebywał pacjent z symptomami choroby COVID-19. Próbki pobierano przed rutynową procedurą dezynfekcji powierzchni przy wykorzystaniu dichlorocyjanouranu sodu w stężeniu 5000 ppm (ang. *parts per million*, pol. liczba cząstek na milion). Próbki z powierzchni pobierano także w dwóch innych pomieszczeniach, w których również przebywali pacjenci z objawami tej choroby, jednak zrobiono to po dezynfekcji przeprowadzonej tam dwa razy w ciągu dnia. W tym przypadku nie stwierdzono RNA koronawirusa. Należy jednak podkreślić, że w takich okolicznościach samo wykrycie RNA koronawirusa SARS-CoV-2 nie oznacza obecności cząsteczek wirusa o zdolnościach infekcyjnych[9].

Ozon (O_3) jest uważany za efektywny środek dezynfekujący stosowany między innymi do uzdatniania wody. Przewyższa on skutecznością inne środki chemiczne, takie jak chlor, chloramina, dwutlenek chloru. Jako naturalny składnik stratosfery ozon powstaje na wysokości ok. 30 km w wyniku oddziaływania promieniowania UV na tlen, w niższych warstwach atmosfery może powstawać natomiast na skutek wyładowań

---

[7] S. Riddell i in., *The effect of temperature on persistence of SARS-CoV-2 on common surfaces*, „Virology Journal" 2020, nr 17, https://doi.org/10.1186/s12985-020-01418-7 [dostęp: 13 X 2020].

[8] S.B. Kasloff i in., *Stability of SARS-CoV-2 on critical personal protective equipment*, MedRxiv, https://doi.org/10.1101/2020.06.11.20128884 [dostęp: 13 X 2020].

[9] Sean Wei Xiang Ong i in., *Air, Surface Environmental, and Personal Protective Equipment Contamination by Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) from a Symptomatic Patient*, „Journal of the American Medical Association" 2020, nr 16, s. 1610–1612.

atmosferycznych[10]. W troposferze ozon powstaje w dużej mierze z gazów pochodzących ze źródeł antropogenicznych, w wyniku reakcji fotochemicznych w obecności światła słonecznego i zanieczyszczeń prekursorowych[11].

Cząsteczka ozonu składa się z trzech atomów tlenu i jest drugą odmianą alotropową tlenu występującą w biosferze. Czysty gaz ma ostry, gryzący zapach, jest łatwopalny i toksyczny. Otrzymuje się go w wyniku cichych wyładowań elektrycznych, które powodują częściową przemianę tlenu w ozon. W ten sposób można uzyskać stężenie nieprzekraczające 10 proc. Większe stężenia ozonu lub czysty ozon uzyskuje się podczas procesu frakcyjnej kondensacji mieszaniny tlenu i ozonu. Ozon w krótkim czasie przechodzi z powrotem w tlen. Czysty ciekły O_3 może mieć właściwości wybuchowe, gdyż reakcja jego rozkładu na tlen, katalizowana przez wiele materiałów, jest silnie egzotermiczna. Jest on silnym utleniaczem, reaguje szybciej niż tlen, a zdolnością utleniania ustępuje tylko fluorowi[12]. Ozon jest bardzo reaktywny z substancjami organicznymi. W trakcie ozonolizy rozkłada się do niestałego ozonku, degradując następnie do karbonylu i jonu obojnaczego, który reaguje m.in. z wolnymi aminokwasami, grupami sulfohydrolowymi, aldehydami, alkoholami, estrami lub wodą, tworząc nadtlenki. Ozon szczególnie szybko reaguje z nienasyconymi kwasami tłuszczowymi, niszcząc wiązania podwójne i tworząc wiązania peroksydowe[13].

Ze względu na swoje właściwości utleniające ozon stał się jednym ze sposobów skutecznego eliminowania zagrożenia przenoszenia infekcji za pośrednictwem dotykanych powierzchni. Jednak, jak podaje Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny, istnieją pewne niejasności dotyczące skuteczności wirusobójczego działania ozonu w stanie gazowym, które jest słabiej udokumentowane i zależy w dużej mierze od stężenia ozonu w powietrzu pomieszczenia oraz od czasu jego działania[14]. Podobną opinię zawiera komunikat Centralnego Instytutu Ochrony Pracy – Państwowego Instytutu Badawczego[15]. Badania przeprowadzone przez Jamesa B. Hudsona i in. (2009 r.) wykazały, że maksymalne właściwości wirusobójcze ozonu występują po osiągnięciu szczytowego stężenia gazowego ozonu o wartości 20–25 ppm

---

[10] J. Szaflik, *Ozon – wróg czy przyjaciel?*, „Biuletyn Informacyjny Stowarzyszenia nRetina AMD Polska", http://idn.org.pl/psrp/ozon.html [dostęp: 20 VII 2020].

[11] M. Amann i in., *Health risks of ozone from long-range transboundary air pollution*, WHO 2008, s. 21, https://www.euro.who.int/__data/assets/pdf_file/0005/78647/E91843.pdf [dostęp: 5 VIII 2020].

[12] J.D. Lee, *Zwięzła chemia nieorganiczna*, Warszawa 1997, s. 241.

[13] J. Szaflik, *Ozon – wróg czy przyjaciel?…*

[14] *Opinia NIZP-PZH z dn. 2.04.2020 r. dot. dezynfekcji pomieszczeń biurowych poprzez ozonowanie i skuteczności powyższej metody w zwalczaniu SARS-CoV-2 oraz kwestii związanych z bezpieczeństwem jej stosowania*, http://wsse.waw.pl/aktualnosci-i-komunikaty/komunikaty/opinia-nizp-pzh-z-dn-2-04-2020-r-dot-dezynfekcji-pomieszczen-biurowych-poprzez-ozonowanie-i-skutecznosci-powyzszej-metody-w-zwal [dostęp: 5 VIII 2020].

[15] *Komunikat nr 4. Ozonowanie jako metoda przeciwdziałająca skażeniu wirusem SARS-CoV-2*, 27 III 2020 r., Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, https://www.ciop.pl/CIOPPortalWAR/file/89653/2020033104228&Komunikat-4-Stanowisko-NC-ozonowanie.pdf [dostęp: 5 VIII 2020].

(39–49 mg/m^3) i wymagają krótkiego okresu wysokiej wilgotności (powyżej 90 proc. RH). Eksperyment przeprowadzano w pomieszczeniu laboratoryjnym o kubaturze 65 m^3, wykorzystano trzy generatory rozmieszczone w różnych miejscach, które doprowadzały stężenie ozonu do wartości 25 ppm w ciągu 15 minut i utrzymywały takie stężenie przez 10 minut, po czym gwałtownie zwiększano wilgotność do ponad 95 proc. RH. Badania obejmowały przedstawicieli różnych rodzin wirusów, a uzyskane rezultaty wskazywały stopień inaktywacji przekraczający wartość 3 $\log_{10}$ (99,9 proc.)[16].

Z punktu widzenia badań daktyloskopijnych istotny jest wpływ ozonu na najważniejsze komponenty substancji potowo-tłuszczowej: aminokwasy i tłuszcze. Ozon jako jeden z najsilniejszych znanych utleniaczy reaguje ze związkami organicznymi, doprowadzając do ich utlenienia. Reakcji ulegają tłuszcze występujące na zewnętrznych powierzchniach skóry człowieka, tj. estry woskowe (reaguje 22 proc.), triacyloglicerole (reaguje 25 proc.), di- i monoacyloglicerole (reaguje 10 proc.) oraz nienasycone kwasy tłuszczowe (reaguje 25 proc.). W przybliżeniu w połowie z tych substancji są obecne nienasycone wiązania węgiel–węgiel, które łatwo wchodzą w interakcje z ozonem. Spośród wszystkich nienasyconych związków występujących na powierzchni warstwy rogowej naskórka najbardziej reaktywny jest skwalen. Końcowymi produktami peroksydacji (utleniania – przyp red.) lipidów są aldehydy, węglowodory oraz związki resztkowe, głównie dialdehyd malonowy. Ozon równie dobrze reaguje z aminokwasami, szczególnie z aminokwasami zawierającymi grupę tiolową[17] .

Materiały i metody

W Pracowni Badań Daktyloskopijnych Biura Badań Kryminalistycznych Agencji Bezpieczeństwa Wewnętrznego (dalej: Pracownia Badań Daktyloskopijnych BBK ABW) przeprowadzono badania w celu określenia wpływu ozonu wykorzystywanego do dezynfekcji pomieszczeń na skuteczność ujawniania śladów linii papilarnych na podłożach papierowych metodą DFO. W eksperymencie wykorzystano podłoża w postaci arkuszy papieru kserograficznego, na których pozostawiano ślady linii papilarnych naniesione naturalną substancją potową i potowo-tłuszczową oraz sztuczną substancją śladotwórczą pochodzącą ze specjalistycznych poduszek daktyloskopijnych nasączonych aminokwasami i tłuszczami (rys. 1).

---

[16] J.B. Hudson, M. Sharma, S. Vimalanathan, *Development of Practical Method of Using Ozone Gas as a Virus Decontaminating Agent*, „Ozone: Science & Engineering" 2009, t. 31, s. 216–223.

[17] A. Wisthaler, Ch.J. Weschler, *Reaction of ozone with human skin lipids: Sources of carbonyls, dicarbonyls and hydroxycarbonyls in indoor air*, „Proceedings of the National Academy Sciences" 2010, nr 15, s. 6568–6575; J. Szaflik, *Ozon – wróg czy przyjaciel?…*; H. Zieliński, *Ozon – jego znaczenie i toksyczność*, „Medycyna Weterynaryjna" 1997, nr 6, s. 325.

Rys. 1. Przykładowy arkusz, na który nanoszono ślady linii papilarnych[18].

[18] Wszystkie materiały ikonograficzne zostały opracowane przez autorów (przyp. red.).

Naturalną substancję potową na skórze palców uzyskiwano po kilkunastominutowym noszeniu jednorazowych rękawiczek, a naturalną substancję potowo-tłuszczową pozyskano dzieki potarciu opuszkami palców czoła, którego skóra jest pokryta naturalną wydzieliną w formie emulsji potowo-tłuszczowej.

Badaniami objęto opisane wcześniej ślady linii papilarnych i podłoże, na którym się znajdowały. Podzielono je na trzy grupy (oznaczone literami A, B, C) w zależności od czasu, jaki upływał od momentu pozostawienia śladów do ich ujawnienia (rys. 2).

Rys. 2. Schemat przeprowadzenia eksperymentu w trzech przedziałach czasowych (grupa A – 11 dni, grupa B – 7 dni, grupa C – 2 dni).

W poszczególnych grupach pozostawiono określoną liczbę śladów:

- grupa A (ślady 11-dniowe) – cztery osoby pozostawiły po 24 ślady linii papilarnych, naniesione czterema rodzajami substancji śladotwórczej,
- grupa B (ślady 7-dniowe) – trzy osoby pozostawiły po 12 śladów linii papilarnych, naniesione czterema rodzajami substancji śladotwórczej,
- grupa C (ślady 2-dniowe) – trzy osoby pozostawiły po 24 ślady linii papilarnych, naniesione czterema rodzajami substancji śladotwórczej.

W sumie badania obejmowały 816 śladów linii papilarnych.

Przygotowane podłoża rozcięto w miejscach pozostawienia śladów linii papilarnych w taki sposób, że każdy ślad podzielono na dwie części: pierwszą umieszczono w pomieszczeniu, które poddano ozonowaniu, drugą określono jako referencyjną i nie poddano jej takiej procedurze (zob. rys. 1). Ozonowanie przeprowadzono w pomieszczeniach o kubaturze ok. 20 m^3. W tym celu wykorzystano generator ozonu Airclean7G firmy Ulsonix, który pracując przez jedną godzinę, wytworzył, zgodnie z danymi odczytanymi z czujnika umieszczonego w pobliżu próbek, maksymalne stężenie 10 ppm. Następnie próbki pozostawały w pomieszczeniach przez kolejne dwie godziny, w których dochodziło do rozkładu ozonu i stopniowego spadku jego stężenia. Po tym czasie pomieszczenia były dokładnie wietrzone. W dalszej kolejności podzielone arkusze poddawano procedurze ujawniania śladów linii papilarnych metodą DFO, zgodnie z metodyką przyjętą w Pracowni Badań Daktyloskopijnych BBK ABW[19]. W metodzie DFO jest wykorzystywany odczynnik reagujący z aminokwasami obecnymi

[19] H.L. Bandey, i in., *Fingermark Visualisation Manual*, (b.m.w.) 2014, s. 5. DFO.1-13.

w substancji śladotwórczej. Produkt reakcji wykazuje fluorescencję przy maksimum wzbudzenia (długość fali 560 nm) i maksimum emisji (575 nm)[20]. W badaniach wykorzystano metodę DFO także do ujawniania śladów naniesionych sztuczną substancją tłuszczową, zakładając, że będzie ona również skuteczna, ale w mniejszym zakresie. Takie założenie wynika z istnienia dużego prawdopodobieństwa kontaminacji (skażenia – przyp. red.) poduszki tłuszczowej aminokwasami, która zachodzi w trakcie wielokrotnego i powtarzającego się kontaktu palców pokrytych naturalną warstwą substancji potowej stale tworzącą się na skórze ze wspomnianą poduszką.

Po ujawnieniu śladów rozcięte arkusze zestawiano ze sobą i porównywano m.in. ich czytelność, rozmycie linii, poziom fluorescencji. Należy podkreślić, że ocena śladów nie obejmowała określenia liczby minucji[21], a co za tym idzie – przydatności do identyfikacji poszczególnych połówek. Celem tego porównania było znalezienie właściwości i cech badanych obiektów wspólnych dla nich lub je różniących, w tym przypadku rozdzielonych śladów linii papilarnych[22]. Zestawienie nie obejmowało cech i właściwości wynikających z morfologii linii papilarnych. Na tej podstawie wywnioskowano o negatywnym lub obojętnym wpływie ozonowania pomieszczenia na próbki poddane badaniom. W badaniach nie zakładano możliwości pozytywnego wpływu ozonowania na proces ujawniania śladów linii papilarnych. Rozdzielonym połówkom przypisywano jedną z dwóch wartości: 0 (ślad linii papilarnych słabej jakości) albo 1 (ślad linii papilarnych dobrej jakości). Przypisywanie jednej z tych wartości i porównywanie podzielonych wcześniej śladów zależało od osoby dokonującej oceny i dlatego charakteryzowało się dużym subiektywizmem. Aby zwiększyć obiektywność otrzymanych wyników badań, wszystkie ślady porównywały niezależnie od siebie cztery osoby. Na koniec wyniki zestawiono i przy użyciu programu Microsoft Excel obliczono średnią arytmetyczną uzyskanych ocen. W przypadku gdy obie połowy śladu oceniono jako słabej jakości, zestawiony cały ślad otrzymywał ocenę 0-0, a gdy dwie połowy śladu oceniono jako dobrej jakości, zestawiony cały ślad otrzymywał ocenę 1-1. Jeżeli stwierdzono, że połowa śladu poddana ozonowaniu otrzymała ocenę „słaba jakość", a połowa referencyjna otrzymała ocenę „dobra jakość", zestawiony cały ślad otrzymywał ocenę 0-1. W sytuacji odwrotnej zestawiony cały ślad otrzymywał ocenę 1-0. Wyniki badań wszystkich porównywanych śladów zsumowano i zestawiono w formie wykresów (wykresy 1–8).

---

[20] Ch. Champod, Ch. Lennard, P. Margot, M. Stoilovic, *Fingerprint and Other Ridge Skin Impressions*, Boca Raton–London–New York–Washington 2016, s. 201.

[21] Charakterystyczne elementy budowy linii papilarnych tworzące różne układy linii ciągłych, ich początków i zakończeń oraz odcinków i kropek. Za: J. Moszczyński, *Daktyloskopia. Zarys teorii i praktyki*, Warszawa 1997, s. 22.

[22] J. Apanowicz, *Metodologiczne uwarunkowania pracy naukowej. Prace doktorskie. Prace habilitacyjne*, Warszawa 2005, s. 30.

Wykres 1. Wynik porównania jakości 2-dniowych śladów linii papilarnych (grupa C) poddanych ozonowaniu w dniu pozostawienia z niepoddanymi ozonowaniu, wyrażony w procentach.

Wykres 2. Wynik porównania jakości 2-dniowych śladów linii papilarnych (grupa C) poddanych ozonowaniu w dniu pozostawienia z niepoddanymi ozonowaniu, wyrażony w liczbach.

Wykres 3. Wynik porównania jakości 7-dniowych śladów linii papilarnych (grupa B) poddanych ozonowaniu po jednym dniu od pozostawienia z niepoddanymi ozonowaniu, wyrażony w procentach.

Wykres 4. Wynik porównania jakości 7-dniowych śladów linii papilarnych (grupa B) poddanych ozonowaniu po jednym dniu od pozostawienia z niepoddanymi ozonowaniu, wyrażony w liczbach.

Wykres 5. Wynik porównania jakości 11-dniowych śladów linii papilarnych (grupa A) poddanych ozonowaniu po piątym dniu od pozostawienia z niepoddanymi ozonowaniu, wyrażony w procentach.

Wykres 6. Wynik porównania jakości 11-dniowych śladów linii papilarnych (grupa A) poddanych ozonowaniu po piątym dniu od pozostawienia z niepoddanymi ozonowaniu, wyrażony w liczbach.

Wykres 7. Suma wyników porównania jakości 816 śladów linii papilarnych poddanych ozonowaniu z niepoddanymi ozonowaniu, wyrażony w procentach.

Wykres 8. Suma wyników porównania jakości 816 śladów linii papilarnych poddanych ozonowaniu z niepoddanymi ozonowaniu, wyrażony w liczbach.

W celu określenia wpływu gazowego ozonu na aminokwasy w badaniach wykorzystano także materiał wzorcowy w postaci gotowych do użycia pasków testowych z podłoża papierowego przypominającego bibułę filtracyjną, na którym były cztery pola reakcyjne o zmniejszającym się wykładniczo stężeniu aminokwasów[23]. Paski podzielono na dwie grupy, z których jedną poddano ozonowaniu. Następnie paski

[23] T. Szczepański, U. Więckiewicz, K. Klemczak, *Paski testowe do sprawdzania reaktywności metod wizualizacji śladów daktyloskopijnych na podłożach chłonnych z aminokwasami*, „Problemy Kryminalistyki" 2015, nr 288, s. 50–53.

poddano działaniu DFO i porównano efekty wizualizacji przez zestawienie pasków (zdjęcie poniżej).

Zdjęcie. Papierowe paski testowe firmy SEMA nasączone aminokwasami o zmniejszającym się wykładniczo stężeniu (paski poddane ozonowaniu oznaczono niebieskim długopisem bezpośrednio na pasku symbolem O_3), widok we fluorescencji: wzbudzenie – światło niebieskozielone, filtr pomarańczowy (A), widok w białym świetle (B).

Wyniki i dyskusja

Po przeanalizowaniu otrzymanych wyników w poszczególnych grupach stwierdzono pogorszenie jakości próbek poddanych ozonowaniu w przypadku śladów linii papilarnych naniesionych sztuczną substancją tłuszczową: 7-dniowych o 16 punktów procentowych i 11-dniowych o 26 punktów procentowych oraz naturalną substancją potowo-tłuszczową w przypadku śladów 11-dniowych (o 13 punktów procentowych). Jakość połówek 7-dniowych śladów naniesionych naturalną substancją potowo-tłuszczową nie różniła się. Natomiast w przypadku substancji śladotwórczej zawierającej głównie aminokwasy stwierdzono, że różnice jakości śladów we wszystkich badanych okresach nie przekraczały 4 punktów procentowych (wykresy 1–6).

Po podsumowaniu wszystkich otrzymanych danych stwierdzono pogorszenie jakości ujawnionych śladów – w przypadku śladów linii papilarnych naniesionych sztuczną substancją tłuszczową o 16 punktów procentowych, a naturalną substancją potowo-tłuszczową o 6 punktów procentowych. W przypadku substancji śladotwórczej zawierającej głównie aminokwasy pogorszenie jakości śladów poddanych ozonowaniu nie przekraczało 2 punktów procentowych (wykresy 7 i 8).

Nie ma możliwości ustalenia, czy stwierdzone różnice w jakości śladów naniesionych substancją śladotwórczą zawierającą większą ilość tłuszczowych składników mogły powstać na skutek m.in. utleniania składników pod wpływem ozonowania, co mogło spowodować reakcję aminokwasów z odczynnikiem DFO, czy też te różnice mogą być wynikiem przeprowadzonej procedury ujawniania. Badania obejmowały dużą liczbę próbek, a technika zastosowania metody DFO (zanurzeniowa) i wynikające z niej

stałe odparowywanie z roztworu roboczego rozpuszczalnika HFE7100 mogły spowodować zmiany jego stężenia. To zjawisko mogło lekko rozmywać ślady i pogorszyć ich jakość przez częściowe rozpuszczenie emulsji śladotwórczej, która zawiera składniki tłuszczowe. Badania materiału referencyjnego w postaci pasków testowych nasączonych aminokwasami również nie potwierdziły negatywnego wpływu gazowego ozonu na reakcję aminokwasy–DFO, co jest widoczne na zamieszczonym zdjęciu.

Wyniki przeprowadzonej analizy porównawczej zsumowanych danych oraz charakterystyka DFO reagującego z aminokwasami obecnymi w substancji śladotwórczej wskazują, że ozonowanie pomieszczeń przy wykorzystaniu typowego generatora ozonu zapewniającego stężenie nieprzekraczające 10 ppm nie wpływa istotnie na możliwość ujawnienia śladów linii pozostawionych na papierze kserograficznym. Należy podkreślić, że wykonane badania dotyczą stężeń gazowego ozonu nieprzekraczających w pomieszczeniach wartości 10 ppm, a zalecana dezynfekcja o udokumentowanym działaniu wirusobójczym powinna zostać przeprowadzona przy urzyciu ozonu w stężeniu przekraczającym 20 ppm, przy znacznie podwyższonej wilgotności.

W przyszłości warto podjąć badania w celu ustalenia, w jakim stopniu stężenia gazowego ozonu przekraczające wartość 10 ppm mogą wpływać na ślady daktyloskopijne i warunkować możliwość ich skutecznego ujawniania.

Podsumowanie

Dane dotyczące skuteczności dezynfekcji wirusobójczej ozonem w stanie gazowym nie są obszerne, a odnalezione informacje wskazują, że wymagane do inaktywacji wirusów stężenie zapewniające względne bezpieczeństwo jest określane na ok. 25 ppm, przy czym konieczne jest szybkie uzyskanie wilgotności do ponad 90 proc. RH. Przeprowadzone badania z wykorzystaniem niższych stężeń gazowego ozonu, o wartości nieprzekraczającej 10 ppm bez podwyższania wilgotności potwierdziły, że ślady linii papilarnych pozostawione na papierze kserograficznym umieszczonym w pomieszczeniu, w którym panują takie warunki, nie ulegają zniszczeniu i z powodzeniem mogą być ujawnione metodą DFO. Należy podkreślić, że potwierdzono skuteczność ujawniania śladów metodą DFO standardowo stosowaną na podłożach chłonnych (m.in. papier), ukierunkowaną wyłącznie na aminokwasy zawarte w substancji śladotwórczej, w tym obecne w emulsji tworzącej ślady potowo-tłuszczowe. Badania nie obejmowały metod ujawniania śladów linii papilarnych reagujących z substancją zawierającą składniki tłuszczowe.

Autorzy dziękują dr Magdalenie Białas, ekspertowi z zakresu badań pisma, za cenne uwagi przy opracowaniu publikacji oraz ekspertom z zakresu badań chemicznych Biura Badań Kryminalistycznych Agencji Bezpieczeństwa Wewnętrznego za pomoc w przeprowadzeniu procesu ozonowania próbek.

Bibliografia

Apanowicz J., *Metodologiczne uwarunkowania pracy naukowej. Prace doktorskie. Prace habilitacyjne*, Warszawa 2005, Difin.

Bandey H.L. i in., *Fingermark Visualisation Manual*, 2014, Home Office Centre for Applied Science and Technology (CAST).

Champod Ch., Lennard Ch., Margot P., Stoilovic M., *Fingerprint and Other Ridge Skin Impressions*, Boca Raton–London–New York–Washington 2016, CRC Press.

Collier L., Oxford J., *Wirusologia. Podręcznik dla studentów medycyny, stomatologii i mikrobiologii*, M. Łuczak (red.), tłum. M.M. Krajewska, Warszawa 1996, Wydawnictwo Lekarskie PZWL.

Hudson J.B., Sharma M., Vimalanathan S., *Development of Practical Method of Using Ozone Gas as a Virus Decontaminating Agent*, „Ozone: Science & Engineering" 2009, t. 31, s. 216–223.

Irving W., Ala'Aldeen D., Boswell T., *Mikrobiologia medyczna*, Warszawa 2008, PWN.

Kampf G., Todt D., Pfaender S., Steinmann E., *Persistence of coronaviruses on inanimate surfaces and their inactivation with biocidal agents*, „Journal of Hospital Infection" 2020, nr 3, s. 246–251.

Lee J.D., *Zwięzła chemia nieorganiczna*, Warszawa 1997, PWN.

Moszczyński J., *Daktyloskopia. Zarys teorii i praktyki*, Warszawa 1997, CLK KGP.

Sean Wei Xiang Ong i in., *Air, Surface Environmental, and Personal Protective Equipment Contamination by Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) from a Symptomatic Patient*, „JAMA" 2020, nr 16, s. 1610–1612.

Szczepański T., Więckiewicz U., Klemczak K., *Paski testowe do sprawdzania reaktywności metod wizualizacji śladów daktyloskopijnych na podłożach chłonnych z aminokwasami*, „Problemy Kryminalistyki" 2015, nr 288, s. 50–53.

Wisthaler A., Weschler Ch.J., *Reaction of ozone with human skin lipids: Sources of carbonyls, dicarbonyls and hydroxycarbonyls in indoor air*, „Proceedings of the National Academy Sciences" 2010, nr 15, s. 6568–6575.

Zieliński H., *Ozon – jego znaczenie i toksyczność*, „Medycyna Weterynaryjna" 1997, nr 6, s. 325.

Źródła internetowe

Amann M. i in., *Health risks of ozone from long-range transboundary air pollution*, WHO 2008, https://www.euro.who.int/__data/assets/pdf_file/0005/78647/E91843.pdf [dostęp: 5 VIII 2020].

N. van Doremalen i in., *Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS-CoV-1*, „The New England Journal Medicine" 2020, nr 382 (16), s. 1564–1567, https://www.nejm.org/doi/full/10.1056/nejmc2004973 [dostęp: 13 X 2020].

Hemida M.G., Ba Abduallah M.M., *The SARS-CoV-2 outbreak from a one health perspective*, „One Health" 2020, t. 10, https://doi.org/10.1016/j.onehlt.2020.100127 [dostęp: 16 III 2020].

Kasloff S.B., i in., *Stability of SARS-CoV-2 on critical personal protective equipment*, MedRxiv, https://doi.org/10.1101/2020.06.11.20128884 [dostęp: 13 X 2020].

Komunikat nr 4. Ozonowanie jako metoda przeciwdziałająca skażeniu wirusem SARS-CoV-2, 27 III 2020 r., Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, https://www.ciop.pl/CIOPPortalWAR/file/89653/2020033104228&Komunikat-4-Stanowisko-NC-ozonowanie.pdf [dostęp: 5 VIII 2020].

Opinia NIZP-PZH z dn. 2.04.2020 r. dot. dezynfekcji pomieszczeń biurowych poprzez ozonowanie i skuteczności powyższej metody w zwalczaniu SARS-CoV-2 oraz kwestii związanych z bezpieczeństwem jej stosowania, http://wsse.waw.pl/aktualnosci-i-komunikaty/komunikaty/opinia-nizp-pzh-z-dn-2-04-2020-r-dot-dezynfekcji-pomieszczen-biurowych-poprzez-ozonowanie-i-skutecznosci-powyzszej-metody-w-zwal [dostęp: 5 VIII 2020].

Riddell S. i in., *The effect of temperature on persistence of SARS-CoV-2 on common surfaces*, „Virology Journal" 2020, nr 17, https://doi.org/10.1186/s12985-020-01418-7 [dostęp: 13 X 2020].

Szaflik J., *Ozon – wróg czy przyjaciel?*, „Biuletyn Informacyjny Stowarzyszenia nRetina AMD Polska", http://idn.org.pl/psrp/ozon.html [dostęp: 20 VII 2020].

Abstrakt

W artykule przedstawiono wyniki badań, których celem było określenie, w jakim stopniu ozon wykorzystywany do dezynfekcji pomieszczeń wpływa na możliwość ujawnienia metodą DFO śladów linii papilarnych na podłożach papierowych. Gwałtowny wzrost zachorowań na COVID-19 skierował uwagę na dezynfekcję pomieszczeń technikami, które zapewniają bezpieczeństwo ich użytkownikom. Istotne staje się także zapewnienie bezpieczeństwa osobom otrzymującym przesyłki, na których mogą się znajdować patogeny. Ich inaktywacja powinna być dokonana w taki sposób, aby można było przeprowadzić badania pozwalające na identyfikację nadawcy, co jest istotne z punktu

widzenia kryminalistyki. Ozonowanie jest techniką dezynfekcji wykorzystywaną od wielu lat, szczególnie do uzdatniania wody, w przemyśle spożywczym. Eksperymenty wykonano w pomieszczeniach o kubaturze ok. 20 m^3 przy urzyciu generatora ozonu dostępnego na rynku. Uzyskiwane stężenie gazowego ozonu nie przekraczało 10 ppm. Przeprowadzone badania potwierdziły, że ślady linii papilarnych pozostawione na papierze kserograficznym umieszczonym w pomieszczeniu poddanym ozonowaniu w stężeniu nieprzekraczającym 10 ppm nie ulegają zniszczeniu i z powodzeniem mogą być ujawnione metodą DFO.

Słowa kluczowe: ślady linii papilarnych, daktyloskopia, DFO, ozon, papier, dezynfekcja, kryminalistyka.

The effect of ozone disinfection of rooms on the efficacy of revealing dactyloscopic traces on the surface of the paper using the DFO method during the SARS-CoV-2 pandemic

Abstract

The article presents the results of research aimed at determining the extent to which ozone used for disinfecting rooms affects the possibility of developing fingerprints on paper using the DFO method. A sudden increase in COVID-19 cases has placed the focus on disinfection techniques for user safety. It is also becoming important to ensure the safety of parcels addressed to various recipients by inactivating pathogens, while maintaining the possibility of examination that can identify the sender, which is important from the point of view of forensics. Ozonation is a disinfection technique that has been used for many years, in particular for water treatment or in the food industry. The experiments were carried out in rooms with a cubature of approx. 20 m3 using an ozone generator available on the market. The obtained ozone gas concentration did not exceed 10 ppm. The conducted research confirmed that the traces of fingerprints left on xerographic paper placed in a room subjected to ozonation in a concentration not exceeding 10 ppm are not damaged and can be successfully developed with the DFO method.

Keywords: fingerprints, dactyloscopy, DFO, ozone, paper, disinfection, forensics.

III

RECENZJE

REVIEWS

KRZYSZTOF IZAK
ORCID: 0000-0001-9815-6035

DOI: 10.4467/20801335PBW.21.013.13570

Gérard Chaliand, Arnaud Blin, *Historia terroryzmu. Od starożytności do Da'isz*[1]

W 2020 r. na polskim rynku księgarskim ukazała się publikacja, o której w krótkiej recenzji zamieszczonej na tylnej stronie okładki wydawca pisze:

> *Historia terroryzmu. Od starożytności do Da'isz* – wynik współpracy międzynarodowego zespołu specjalistów pod redakcją Gérarda Chalianda i Arnauda Blina – jest pierwszą na światowym rynku tak ambitną i szeroko zakrojoną pracą przedstawiającą historię i naturę terroryzmu. Za sprawą interdyscyplinarnego podejścia autorów, dzieło to pozwala na analizę zarówno samego zjawiska, jak i ewolucji jego postrzegania. Badacze śledzą skrupulatnie wszystkie przejawy i formy terroryzmu na przestrzeni dziejów – od zelotów i asasynów, poprzez XIX-wiecznych anarchistów, terror rosyjski w służbie państwa, współczesne formy wyrosłe po roku 1968, aż po radykalny fundamentalizm muzułmański bojowników Al-Ka'idy i Państwa Islamskiego. Wykład historyczny został uzupełniony obszernym wyborem tekstów źródłowych – wystąpień, manifestów i pism teoretycznych – od Michała Bakunina po Usamę Ibn Ladena i Ajmana az-Zawahiriego – co czyni z tej pracy prawdziwą wielką encyklopedię terroryzmu.

Po przeczytaniu tej notki można by właściwie przejść do szczegółowej recenzji, gdyby nie konieczność sprostowania. Nie jest to (…) *pierwsza na światowym rynku tak ambitna i szeroko zakrojona praca przedstawiająca historię i naturę terroryzmu*, w 2004 r. bowiem ci sami autorzy opublikowali *Historię terroryzmu od starożytności do Al-Kaidy.* Ich druga książka jest zatem aktualizacją pierwszej publikacji, która liczyła 660 stron. Poza tym nie mniej monumentalnym dziełem jest *Encyklopedia terroryzmu*

---

[1] G. Chaliand, A. Blin, *Historia terroryzmu. Od starożytności do Da'isz,* Warszawa 2020, PIW, 584 s. Książka pod oryginalnym tytułem *Histoire du terrorisme: de l'Antiquité à Daech* ukazała się we Francji w 2015 r. nakładem znanego paryskiego wydawnictwa Fayard.

pod redakcją Marthy Crenshaw i Johna Pimlotta wydana w 2004 r. przez Muzę SA i Bellonę S.A., również opisująca zjawisko terroryzmu od starożytności, w tym okresie nawet bardziej szczegółowo niż recenzowana książka. Należy też wymienić przekrojową publikację Jarosława Tomasiewicza pt. *Terroryzm na tle przemocy politycznej (zarys encyklopedyczny)*, wydaną w 2000 r. w Katowicach. Istnieje więc możliwość porównania i szerszej oceny.

Historia terroryzmu. Od starożytności do Da'isz ukazała się nakładem Państwowego Instytutu Wydawniczego w słynnej „serii ceramowskiej", co z pewnością podnosi jej walor czytelniczy i kolekcjonerski[2]. Obniża go natomiast brak ilustracji, ponieważ wspomniana seria ma z reguły bogatą szatę graficzną. Był to prawdopodobnie świadomy wybór wydawcy w celu obniżenia kosztów i zmniejszenia objętości książki, która we francuskojęzycznym oryginale liczy aż 840 stron.

Publikacja składa się z czterech części i dwudziestu jeden rozdziałów, które zachowują ciągłość numeracji od części pierwszej. Rozdziały wraz z podrozdziałami są wymienione aż na sześciu stronach spisu treści. Nie każdy z nich ma jednakową wartość poznawczą. Już na początku recenzji trzeba przyznać, że zawartość książki rozczarowuje. W spisie treści zwraca uwagę tytuł części pierwszej: *Prehistoria terroryzmu*. Wypadałoby więc, aby część druga dotyczyła starożytności, ale nic podobnego – nosi ona tytuł *Okres współczesny: od 1789 do 1968 roku*. Jest to więc całkowite przekłamanie dziejów ludzkości. Prehistoria to okres przed pojawieniem się pisma i jest domeną badań archeologów. Nie było wówczas żadnych źródeł pisanych, które potwierdzałyby istnienie zjawiska terroryzmu. Autor recenzji zna poglądy archeologów pochodzących z różnych krajów, którzy potwierdzają istnienie brutalnej przemocy niezwiązanej z działaniami o charakterze wojennym, ale autorzy części pierwszej – Gérard Chaliand i Arnaud Blin – w ogóle o tym nie wspominają. Dla nich prehistoria terroryzmu zaczyna się w I wieku n.e. działalnością żydowskich zelotów i asasynów. Oba ruchy dzieli tysiąc lat historii, również wypełnionych licznymi aktami terrorystycznymi, ale o nich autorzy nie wspominają. Braku ich wiedzy historycznej dowodzą również inne przykłady. Chaliand i Blin we wprowadzeniu piszą:

> W 1979 r. radykalny fundamentalizm muzułmański pojawił się gwałtownie w wersji szyickiej w Iranie. W tym samym roku wojna w Afganistanie, za sprawą Stanów Zjednoczonych, Arabii Saudyjskiej i Pakistanu, doprowadziła do apogeum radykalny fundamentalizm sunnicki. Ten nurt, do którego należą elementy wywodzące się z różnych państw sunnickich z wyjątkiem Afryki Czarnej, po wycofaniu się ZSRR z Afganistanu zwrócił się przeciwko Stanom Zjednoczonym (s. 21).

[2] Nazwa pochodzi od C.W. Cerama (pseudonim literacki Kurta Wilhelma Marka). Ceram jest ananimem, czyli pseudonimem utworzonym przez odwrócenie kolejności liter w nazwisku autora książki pt. *Bogowie, groby i uczeni. Powieść o archeologii*, będącej pierwszą publikacją wydaną w serii Rodowody Cywilizacji. Do tej pory ukazało się sto kilkadziesiąt tytułów w ramach serii „dużego Cerama" i „małego Cerama" (formaty serii).

Nie można w pełni się zgodzić z tymi twierdzeniami, ponieważ już w XIX w. idee dżihadu doprowadziły do powstania niezależnych państw muzułmańskich w Czarnej Afryce. W 1809 r. imam Usman dan Fodio utworzył sułtanat (kalifat) Sokoto (północna Nigeria). W Afryce Zachodniej natomiast powstało państwo Samoriego. W latach 1851–1864 istniał dżihad ludu Tukulerów, kierowany przez Hadżiego Umara Talla. Sukcesy militarne Tukulerów zahamowały zwycięski pochód dżihadu sufickiego, ekstatycznego bractwa kadirijja, które utraciło swoje pierwotne pozycje na rzecz bractwa tidżanijja w Gwinei, kraju Hausa (sułtanat Sokoto) i na obszarze obecnego Kamerunu. Ponadto w niektórych państwach Czarnej Afryki antyamerykańskość też była widoczna. Należy tu wymienić bitwę stoczoną w dniach 3–4 października 1993 r. przez wojsko USA z siłami Muhammada Faraha Aidida w Mogadiszu, w wyniku której zginęło 18 amerykańskich żołnierzy, a 73 zostało rannych. Na skutek decyzji Waszyngtonu Amerykanie wycofali się wówczas z Somalii.

Wstęp do omawianej publikacji napisał Ariel Merari, izraelski politolog kierujący Wydziałem Badań nad Przemocą Polityczną Uniwersytetu w Tel Awiwie. Stara się on roboczo zdefiniować terroryzm. I tu dość duża niespodzianka: autor pod pojęciem terroryzm rozumie każdą przemoc polityczną, również tę stosowaną przez państwo wobec własnych obywateli. W naszej literaturze przedmiotu jest ona określana pojęciem terror, Merari natomiast nazywa ją terroryzmem państwowym. Zatarł więc różnice między opresyjną polityką państwa a rzeczywistymi działaniami terrorystycznymi wspieranymi przez państwo (np. ZSRR, Iran, Syrię, Libię, Arabię Saudyjską czy Pakistan). Istnieją przecież także inne formy przemocy politycznej, które trudno zaliczyć do terroryzmu, m.in. bojówkarstwo (manifestacje, przemoc, walki uliczne) i bandytyzm polityczny (blokady dróg, rozboje, pobicia, akty wandalizmu). Autor dokonuje rozróżnienia między terroryzmem i partyzantką, choć niektóre twierdzenia są mało przekonujące, np.: *Najważniejsza różnica jest taka, że inaczej niż w przypadku terroryzmu partyzantka próbuje narzucić swoją fizyczną kontrolę na danym terytorium* (s. 27) czy: *Strategia terrorystyczna nie ma na celu materialnej kontroli nad terytorium* (s. 28). Wiele organizacji terrorystycznych dąży przecież do sprawowania kontroli nad określonym terytorium (Hamas, Hezbollah, Harakat asz-Szabab al-Mudżahidin, Boko Haram, talibowie, Państwo Islamskie). Zacytowane wypowiedzi siłą rzeczy doprowadziły do kolejnego nieprawdziwego stwierdzenia: *Ponieważ terroryści, w przeciwieństwie do partyzantów, nie mają bazy terytorialnej, muszą wmieszać się w ludność cywilną, aby uniknąć natychmiastowego namierzenia* (s. 28). Przecież członkowie Abu Sajaf, Boko Haram, Harakat asz-Szabab al-Mudżahidin, Hezbollahu czy Państwa Islamskiego nosili lub nadal noszą mundury. Trudno również się zgodzić z następującymi wypowiedziami: *Sami terroryści działają w bardzo małych jednostkach, wahających się na ogół od samotnego zabójcy lub pojedynczej osoby, która tworzy i podkłada wykonany rzemieślniczo ładunek wybuchowy, do pięcioosobowej grupy biorącej zakładników. Ważniejsze grupy liczą od czterdziestu do pięćdziesięciu osób. Jednakże jest to bardzo rzadkie* (s. 28). Ten opis pasuje do XIX-wiecznych terrorystów – rewolucjonistów – i nie pokrywa się

z funkcjonowaniem wielu współczesnych organizacji terrorystycznych. Ponadto Państwo Islamskie (Da'isz) podniosło terroryzm do rangi operacji wojennych.

Podobne kontrowersje mogą wzbudzać inne fragmenty *Wstępu*. W jego dalszej części Merari przedstawia zjawisko terroryzmu jako strategię powstańczą. Próbuje odpowiedzieć na pytanie, do jakiego stopnia terroryzm może odnieść sukces. Na koniec prowadzi rozważania na temat mieszanej formy buntów – wymienia m.in. ruchy partyzanckie w okresie II wojny światowej, ale nie wspomina o polskiej Armii Krajowej, której działalność powinna być znana chociażby z publikacji historyka Normana Daviesa. W *Historii terroryzmu*… nie ma jednak odniesienia do żadnej z jego prac.

Interesujące są rozważania zawarte w podrozdziale *Terroryzm i moralność*, dotyczące skali „zabijalności", tj. tego, kiedy, kogo i w jakich warunkach można zabijać. Merari odwołuje się do Michaela Walzera, który zanalizował moralność, uwzględniając to, czy ma ona charakter religijny (pochodzi od Boga), czy też uniwersalny pod względem psychologicznym. Historia pokazuje, że „zabijalność" w ciągu wieków się zmieniała, gdyż inną moralność dyktuje czas pokoju, a inną czas wojny. W publikacji zabrakło, niestety, odniesień do monumentalnego opracowania Karen Armstrong pt. *Fields of Blood. Religion and the History of Violence*[3]. Autorka opisuje w nim, w jaki sposób na przestrzeni dziejów władza świecka była powiązana z religijną, i znajduje religijne, a więc moralne, uzasadnienie wojen i masakr. Badaczka podkreśla, że religia była narzędziem ucisku nie ze swej istoty, lecz dlatego, że była wpisana w określony porządek społeczny zbudowany na przemocy i wyzysku.

Część pierwsza książki, zatytułowana – jak już wspomniano – *Prehistoria terroryzmu*, powinna zdaniem autora recenzji nosić bardziej poprawny tytuł *Terroryzm w okresie starożytnym i w średniowieczu*. Treść tej części należałoby rozszerzyć o wydarzenia, które nastąpiły przed pierwszym wiekiem naszej ery, od którego zaczynają swoją opowieść Chaliand i Blin. Najkorzystniej byłoby się cofnąć do VI w. p.n.e., a dokładniej do roku 514 p.n.e. Jest to jedna z najważniejszych dat w historii starożytnej Grecji. W tym bowiem roku ateńscy arystokraci Aristogejton i Harmodios zamordowali tyrana Aten Hipparcha i jego brata Hippiasza. Sami zginęli, ale wdzięczny lud Aten ufundował im pomnik nazwany Grupą Tyranobójców, który został wystawiony na Agorze (pomnik jest znany z rzymskiej kopii). Jest to o tyle istotne, że fragment rozdziału drugiego jest poświęcony teoretycznym rozważaniom nad tyranobójstwem. Są one zresztą potraktowane dość wybiórczo w porównaniu z 18 stronami opisu działalności wspomnianych asasynów (która także została potraktowana w sposób dość chaotyczny) i przerywane porównaniami do terroryzmu w ostatnich dwóch stuleciach. Ponadto informacje o asasynach znajdują się również na stronach 239–240.

---

[3] Polski przekład książki, zatytułowany *Pola krwi. Religia i przemoc*, ukazał się w 2017 r. nakładem Grupy Wydawniczej Foksal. Przy uzupełnianiu tych informacji nie sposób pominąć filozofii Friedricha Nietzchego (1844–1900), który spoglądając wstecz, doszedł do wniosku, że Zaratustra (VI w. p.n.e.) stworzył najbardziej złowieszcze pojęcie – m o r a l n o ś ć. Tę myśl rozwinął w książce *To rzekł Zaratustra* (Warszawa 2005). Taki sam tytuł nadał Richard Strauss (1864–1949) swojemu poematowi muzycznemu.

W rozdziale drugim, liczącym zaledwie 21 stron, autorzy dokonują przeglądu przejawów terroryzmu na przestrzeni stuleci, zaczynając od wspomnianego powyżej tyranobójstwa (*Tyranobójstwo* to tytuł pierwszego podrozdziału). Wymieniają w nim starożytnych i średniowiecznych autorów, którzy poświęcili temu tematowi swoje prace. Nie znajdzie się tu jednak żadnych informacji o zabójstwie Cezara w 44 r. p.n.e., o podpaleniu świątyni Artemidy w Efezie przez Herostratesa w 356 r. n.e. czy skrytobójstwach na dworze cesarzy rzymskich i bizantyjskich oraz we włoskich rodach Medyceuszy i Sforzów.

Podrozdział drugi tego rozdziału nosi tytuł *U początków terroryzmu państwowego: podbój mongolski*. Terroryzm (zdaniem recenzenta właściwsze byłoby używanie słowa „terror") był praktykowany przez Tatarów. Okrutny terror pozwalał im na zrekompensowanie mniejszej liczebności w porównaniu z liczebnością ludów, które podbijali. Z kolei element zaskoczenia i lęk, jaki wywoływali, były atutami umożliwiającymi odnoszenie zwycięstw w walkach. Rekordy okrucieństwa pobił Tamerlan. Po splądrowaniu miast, które atakował, wznosił piramidy ze ściętymi głowami ku przestrodze tych, którzy wzniecali bunty.

Kolejny podrozdział nosi tytuł *Terror w wojnie: wojna trzydziestoletnia*. W ten sposób pominięto tak ważne wydarzenia w historii Europy, naznaczone przemocą polityczną i religijną, jak reformacja i walki między katolikami i protestantami przed wybuchem wojny trzydziestoletniej w 1618 r. Nie ulega wątpliwości, że pokój westfalski w 1648 r., kończący tę wojnę, był wielkim zwycięstwem Francji w jej wielowiekowej rywalizacji z dynastią Habsburgów - ugruntował rozbicie Niemiec i umocnił pozycję Szwecji na Morzu Bałtyckim. Należy jednak podkreślić, że książka jest historią terroryzmu, a nie jego dziejami w Europie Zachodniej. W wiekach XVI i XVII w Europie Wschodniej i na Bałkanach również zaistniały istotne wydarzenia, które autorzy mogliby włączyć do katalogu zdarzeń o charakterze terrorystycznym. Podobnie działo się w Hiszpanii po zakończeniu rekonkwisty, nie wspominając już o Azji i obu Amerykach. W książce nie ma o tym ani słowa.

Część druga publikacji obejmuje okres współczesny – od 1789 r. do 1968 r. Rozpoczyna ją rozdział trzeci zatytułowany *Pojawienie się nowoczesnego terroru*. Czytelnikowi należy się wyjaśnienie. W historiografii francuskiej za początek okresu współczesnego uznaje się wybuch rewolucji w 1789 r., w polskiej natomiast ten okres, mimo że jest nazywany „historią najnowszą", przyjęło się datować od trzeciego rozbioru Polski w 1795 r. Anglosaska szkoła historyczna nie wprowadziła tej nomenklatury, gdyż uznała czasy współczesne za część nowożytności.

Autorami rozdziału trzeciego również są Gérard Chaliand i Arnaud Blin, którzy bagatelizując chronologię, już na początku rozdziału przechodzą do krótkiego omówienia znaczenia rewolucji francuskiej dla rozwoju terroryzmu w XIX i XX w., a dopiero potem przedstawiają problematykę, której ten rozdział dotyczy. Pojęć „terror" i „terroryzm" używają zamiennie. Według nich: *Ogólnie terror jest rozumiany raczej jako okres rewolucji niż „forma polityki rewolucyjnej", co można by zdefiniować jako „wykorzystanie przymusu i przemocy w celach politycznych wobec milczenia prawa"*

(s. 90). Następnie rozwijają tę tezę i przytaczają interpretacje pojęcia „terror", dokonywane przez historyków francuskich. Te same czynniki jednak, tj. (…) *wykorzystanie przymusu i przemocy w celach politycznych wobec milczenia prawa*, występują w postrewolucyjnych państwach autorytarnych, w których stosuje się przemoc, i autorzy nazywają ją – jak już wspomniano – „terroryzmem państwowym", a nie „terrorem". Pobieżnie omawiają wydarzenia z XIX i XX w., aby wrócić do zdarzeń, które nastąpiły po 1789 r. Według tych autorów: *Z punktu historycznego terror rozpoczął się 5 września 1793 r. w Konwencie Narodowym i zakończył 27 lipca 1794 r. wraz z upadkiem Robespierre'a (9 thermidora), czyli trwał niecały rok*. W polskiej literaturze wymienia się natomiast datę 13 lipca 1793 r., kiedy to żyrondystka Charlotte Corday zasztyletowała jakobińskiego trybuna Jeana-Paula Marata w proteście przeciwko terrorowi jakobinów (lewicowe stronnictwo polityczne rewolucji powstałe w 1789 r.) wymierzonemu w żyrondystów (prawicowy klub polityczny rewolucji) i kler. Z tego wynika, że terror pojawił się wcześniej niż wyznaczają go obie daty. Najbardziej krwawy przebieg miał w Wandei, gdzie w latach 1793‑1796 toczyło się rojalistyczne powstanie. Pomijając te uwagi, należy podkreślić, że to właśnie Francja podczas rewolucji wynalazła ten rodzaj przemocy państwowej, który znacznie się rozwinął i udoskonalił w krajach autorytarnych w XX w., czyli terror lub ‑ jak piszą autorzy ‑ „terroryzm państwowy".

Autorem rozdziału czwartego pt. *Terroryści anarchistyczni w XIX wieku* jest Olivier Hubac-Occhipinti, specjalista w zakresie konfliktów zbrojnych i aktów piractwa. W XIX w. terroryzm był cechą charakteryzującą różne grupy ideologiczne (anarchistów, nihilistów, populistów, marksistów i rasistów). Nihilizm i populizm były źródłami rosyjskiego terroryzmu wymierzonego w carski reżim. Aktywiści tych grup tworzyli pierwsze organizacje, a w niektórych z nich głosowano nad tym, czy używać przemocy, czy też nie. Autor w sposób zwięzły i przejrzysty wprowadza czytelników w problem terroryzmu anarchistycznego. Omawia jego kontekst historyczny, który sprzyjał ukształtowaniu i rozpowszechnianiu idei anarchistycznych, a także definiuje anarchizm, wymienia czołowych teoretyków tego ruchu oraz regionalnych anarchistycznych terrorystów, kolejno: włoskich, hiszpańskich, z Ameryki Północnej (w tym Leona Czołgosza, anarchistę polskiego pochodzenia, który we wrześniu 1901 r. zabił prezydenta Williama McKinleya) i francuskich. Od tego rozdziału daje się zauważyć małą dbałość o spójną redakcję dalszej części książki. Te same nazwiska pojawiają się na bliższych i dalszych stronach, w cząstkowych opisach działalności danej osoby. Aby uzyskać komplet informacji na czyjś na temat, często trzeba korzystać z indeksu nazwisk.

W osobnym rozdziale historyk Yves Ternon, specjalista od historii najnowszej, scharakteryzował terroryzm rosyjski, cechujący się dużym udziałem kobiet. Umieścił go w latach 1878‑1908. Te granice czasowe zostały nakreślone sztucznie i zdaniem recenzenta niepotrzebnie, ponieważ Ternon rozpoczyna narrację od lat 40. XIX w., a kończy na roku 1917. Dla wyjaśnienia, rok 1878 to data powstania organizacji Ziemia i Wola, której poprzedniczką była organizacja Ziemia i Wolność, istniejąca od 1863 r. Następczynią Ziemi i Woli była z kolei Wola Ludu (ros. Народная Воля, pis. fon. Narodnaja Wola) utworzona w 1879 r., stąd nazwa jej członków – narodnicy. W 1900 r. powołano

Partię Socjalistów-Rewolucjonistów, której członkowie byli nazywani eserowcami. Narodnicy i eserowcy byli wprawdzie specyficznym zjawiskiem rosyjskim, ale ich wpływ wykraczał poza granice Rosji. W tym rozdziale zawarto kilka polskich wątków, w tym informacje o zamachu na cara Aleksandra II, przeprowadzonym w marcu 1881 r. przez Polaka Ignacego Hryniewieckiego. Pod datą 1908 r. autor umieszcza zlikwidowanie siatek terrorystycznych w Rosji i nieudany zamach na cara Mikołaja II.

Rozdział szósty Gérard Chaliand i Arnaud Blin zatytułowali *Belle époque terroryzmu*. Jest to okres od zakończenia wojny francusko-pruskiej w 1871 r. do wybuchu I wojny światowej w 1914 r., uznawany za czas spokoju, rozwoju i postępu. Postęp ujawnił się tu w użyciu nowej broni i udoskonalonej technologii produkcji materiałów wybuchowych wykorzystywanych do przeprowadzania ataków terrorystycznych, które pociągały za sobą coraz więcej ofiar. Wydarzenia w omawianym okresie są częściowo powtórzeniem tego, co przedstawiono w rozdziale poprzednim, ale poruszono tu także nową problematykę – początki terroryzmu w Irlandii, w Indiach, na Bałkanach i w Armenii. Jednak wbrew tytułowi rozdziału autorzy wykraczają poza datę końcową, tj. 1914 r., komentują wydarzenia rozgrywające się w okresie międzywojennym, a ponadto porównują działalność chorwackich ustaszy do działalności Al-Kaidy. Powoduje to duży chaos zarówno w tej części publikacji, jak i w następnych. Całkowicie pominięto problem terroru w okresie I wojny światowej (lub Wielkiej Wojny, jak ją nazywają Francuzi). Używano wówczas gazów bojowych i dopuszczano się zbrodni na ludności cywilnej. Niezwykle skrótowo potraktowano zagadnienie terroryzmu skrajnej prawicy w okresie międzywojennym, ale ze szczegółami opisano przygotowania i przebieg zamachu na króla Jugosławii Aleksandra I Karadżiordżiewicza w październiku 1934 r. w Marsylii. Nie wspomniano natomiast o zamachu na pierwszego prezydenta Polski Gabriela Narutowicza w grudniu 1922 r. ani o terrorystycznej działalności Organizacji Ukraińskich Nacjonalistów, o której w międzywojniu było głośno za granicą.

Ci sami autorzy napisali rozdział siódmy - *Lenin, Stalin i terroryzm państwowy*, oraz ósmy - *Terroryzm w czasie wojny, od II wojny światowej do wojen o wyzwolenie narodowe*, tj. ostatni w części drugiej. Brakuje w nim jednak omówienia terroryzmu w czasie wojny. Jedyny problem, któremu poświęcono nieco uwagi, dotyczy ruchu syjonistycznego w Palestynie. Na przedstawienie tak ważnego okresu, obejmującego - przynajmniej w założeniu - lata 1939-1967, poświęcono zaledwie osiem stron (s. 184-192), nieproporcjonalnie mało w porównaniu na przykład z opisem działalności asasynów (18 stron).

Część trzecia, najobszerniejsza (ponad 240 stron), nosi tytuł *Terroryzm współczesny od 1968 roku do dzisiaj*. Składa się na nią dziewięć rozdziałów napisanych przez pięciu autorów. Oprócz wcześniej wymienianych są to: Philippe Migaux – wykładowca w paryskim Instytucie Nauk Politycznych (pełna nazwa: Institut d'études politiques, ale w literaturze, prasie i rozmowach używa się ogólnie przyjętego synonimu: Sciences Po), autor i współautor książek na temat terroryzmu i Al-Kaidy; Francois Géré – historyk i specjalista od geostrategii, założyciel Francuskiego Instytutu Analiz Strategicznych; Rohan Gunaratna – najbardziej znany w Polsce, analityk ds. politycznych

specjalizujący się w zakresie terroryzmu międzynarodowego, autor kilkunastu książek poświęconych m.in. Al-Kaidzie i globalnemu ruchowi islamskiego dżihadu (kierował Międzynarodowym Centrum Badań nad Przemocą Polityczną i Terroryzmem w Singapurze). Niezwykle trudno zrecenzować na kilku stronach tę część publikacji, która mogłaby stanowić odrębną książkę. Czytelnik musi tu zachować dużą uwagę, aby połączyć tę samą problematykę porozrzucaną po różnych rozdziałach. Dotyczy to źródeł terroryzmu (uwarunkowania społeczno-polityczne i religijne), organizacji terrorystycznych, nazwisk i wydarzeń.

Pierwszy rozdział części trzeciej publikacji (dziewiąty w kolejności) nosi tytuł *Od 1968 roku do radykalnego fundamentalizmu* i dotyczy wydarzeń z tego okresu. Chaliand i Blin wymieniają cztery daty mające największe znaczenie dla współczesnego terroryzmu (s. 195), tj.:

- rok 1968 – początek strategii partyzantki miejskiej w Ameryce Łacińskiej i umiędzynarodowienie terroryzmu palestyńskiego;
- rok 1979 – zwycięstwo rewolucji islamskiej w Iranie, wyznaczającej początek fundamentalizmu szyickiego, oraz wkroczenie armii ZSRR do Afganistanu, skutkujące ukształtowaniem się ruchu dżihadu z pomocą USA, Arabii Saudyjskiej i Pakistanu;
- lata 1991–1993 – wyjście dżihadu poza Afganistan;
- 11 września 2001 r. – data wyznaczająca ostatni etap klasycznego terroryzmu, ale też symbolicznie najważniejszej operacji w ramach działań kontrterrorystycznych.

W opisie wydarzeń z przełomowego 1968 r. pominięto protesty i rozruchy studenckie, które przetoczyły się latem tegoż roku w Europie Zachodniej i które przyczyniły się do powstania lewackich organizacji terrorystycznych: Frakcji Czerwonej Armii w Niemczech i Czerwonych Brygad we Włoszech. Informacje na ten temat można znaleźć dopiero na stronie 208, rozpoczynającej krótki przegląd grup i ruchów europejskich oraz śródziemnomorskich. Poprzedzają go podrozdziały *Różne oblicza terroryzmu* (s. 199–200) i *Typologia rodzajów terroryzmu* (s. 200–204). W tym drugim znajduje się krótka wzmianka o Demokratycznej Partii Kurdystanu (DPK) z irańskiego Kurdystanu. Poprawna nazwa to Demokratyczna Partia Irańskiego Kurdystanu. DPK zaś to skrótowiec od nazwy organizacji działającej w Iraku. Abdullah Öcalan nie został aresztowany w 1998 r., lecz w lutym 1999 r., po porwaniu go z Kenii przez żołnierzy elitarnej jednostki tureckiej przy pomocy izraelskich i amerykańskich służb specjalnych. Na stronie 202 czytamy: *Bez wątpienia w chwili pisania tych słów najskuteczniejsza na świecie organizacja terrorystyczna to LTTE (Liberation Tigers of Tamil Eelam), czyli Tamilskie Tygrysy*. Te słowa opisywały rzeczywistość w okresie, w którym autorzy pracowali nad pierwszą wersją książki opublikowaną w 2004 r. Tymczasem, gdy ukazało się jej drugie wydanie (w 2015 r.), LTTE nie działała już od sześciu lat, rozbita przez siły rządowe Sri Lanki. Podobnie straciło na aktualności stwierdzenie znajdujące się na końcu tej samej strony: *Można do tego dorzucić* [treść odnosi się do walczących islamskich fundamentalistów – dop. aut.] *długą listę organizacji fundamentalistycznych*

liczących od kilkudziesięciu do nawet ponad tysiąca członków. Krajem pochodzenia tych ruchów są niemal zawsze kraje muzułmańskie – z wyjątkiem Afryki Subsaharyjskiej. Kilka lat przed 2015 r. Unia Trybunałów Islamskich i Boko Haram, ugrupowania liczące po kilka tysięcy bojowników, prowadziły w swoich krajach, tj. w Somalii i w Nigerii, a więc w państwach Afryki Subsaharyjskiej, działania zakrojone na szeroką skalę. Dwa ostatnie podrozdziały zatytułowane *Ruchy mniejszościowe i religijne* oraz *Terroryzm religijny* poprzedza podrozdział pt. *Organizowanie odpowiedzi na terroryzm*, chociaż bardziej logiczne wydaje się przeniesienie tego ostatniego na koniec rozdziału. Ponadto znacznie korzystniejsza byłaby inna konstrukcja rozdziału, polegająca na rozdzieleniu organizacji europejskich i śródziemnomorskich. Te pierwsze należałoby umieścić na jego początku, a następnie omówić problematykę terroryzmu (partyzantki) latynoamerykańskiego. Wszystkie kwestie dotyczące terroryzmu palestyńskiego, Afganistanu oraz Iranu powinno się połączyć w jeden podrozdział pt. *Grupy śródziemnomorskie*, choć bardziej prawidłowy byłby tytuł *Grupy bliskowschodnie*, ponieważ z tym terenem są związane.

W ten sposób zostałaby zachowana ciągłość narracji z rozdziałem dziesiątym, zatytułowanym *Korzenie radykalnego fundamentalizmu muzułmańskiego*. Jego autorem, podobnie jak dwóch pozostałych, jest Philippe Migaux. Uwagę zwraca tu całkiem odmienny warsztat naukowy autora, który konsekwentnie, trzymając się chronologii zdarzeń, wprowadza czytelnika w problematykę islamskiego radykalizmu. Migaux zadedykował tekst 58 francuskim komandosom z „drakkaru" oraz siedmiu mnichom z Tibhirine, którzy przybyli na ziemię islamu, aby na swój sposób czynić pokój[4]. Na początku uwagę zwraca poprawność polityczna autora, który stosując słowną ekwilibrystkę, stara się pomniejszyć związek współczesnego terroryzmu z islamem i tzw. dżihad miecza przypisuje (…) *spaczonej wizji jednej ze szkół myśli fundamentalistycznej*. Zdaniem Migaux'a wyrażenie „dżihad miecza" zostało utworzone (…) *przez radykalnych myślicieli, którzy przywłaszczyli sobie koraniczną alegorię „raju w cieniu miecza"* (s. 229). Tymczasem „raj w cieniu miecza" nie jest koraniczną alegorią, lecz hadisem ze zbioru *Sahih al-Muslim* autorstwa Abu al-Husajna Muslima (zm. w 875 r.)[5]. To Allah gwarantuje muzułmanom, że ci, którzy zginą w jego imię, trafią do raju. Miecz (lub szable) znajduje się w symbolice wielu organizacji muzułmańskich i na fladze Arabii Saudyjskiej, a wyroki śmierci w tym państwie wykonuje się właśnie mieczem. Migaux dokonuje

[4] W dniu 23 X 1983 r. Hezbollah przeprowadził w Bejrucie jednocześnie dwa zamachy terrorystyczne – na koszary amerykańskich marines (zginęło 241 żołnierzy) oraz na budynek zwany „drakkarem" (od nazwy łodzi wikingów), w którym skoszarowano francuskich komandosów. Pamięć o mnichach dotyczy zdarzeń z nocy z 26 na 27 III 1996 r. Wtedy to terroryści z islamskiej grupy zbrojnej uprowadzili z klasztoru trapistów w Tibhirine, niedaleko Medei, siedmiu mnichów, którym następnie obcięli głowy.

[5] Mahomet powiedział: „»Zaprawdę, bramy raju leżą w cieniu mieczy«. Nędznie wyglądający mężczyzna wstał i zapytał Abu Musę, czy słyszał, jak Mahomet wypowiedział te słowa. »Tak« odpowiedział [Abu Musa]. Nędznik wrócił wówczas do swych przyjaciół i pożegnał się z nimi. Następnie dobył swego miecza, wyrzucił jego pochwę, ruszył na wroga i walczył, aż do swej śmierci". Zob. B. Warner, *Hadisy. Sunna Mahometa*, Brno 2016, s. 22.

gradacji fundamentalizmu na: umiarkowany, polityczny, radykalny, aktywistyczny (walczący) i na końcu - dżihadyzm. Posługując się sformułowaniem: *Ideologiczne początki radykalnego islamu: ograniczająca i mylna interpretacja islamu dokonana przez rygorystycznych i marginalnych egzegetów* (s. 231) i treściami zawartymi w następującym po nim rozwinięciu, stara się wyrobić w czytelniku przekonanie, że to mylna interpretacja źródeł islamu sprowadziła część jego wyznawców na drogę walki i terroryzmu. Tymczasem islam po roku 622, czyli roku hidżry, był przepełniony przemocą. Koran jest bezdyskusyjnie księgą sprzeczności. Można się w niej doszukiwać walorów pokojowego i tolerancyjnego islamu, zawartego w objawieniach z epoki przedislamskiej (sury mekkańskie), jednak sury medyńskie i zbiory hadisów (czyli sunna) nie pozostawiają wątpliwości co do jego agresywnego charakteru. Islam jest religią poddania i zniewolenia. Nie pozostawia też prawdziwemu, bogobojnemu muzułmaninowi wyboru – musi się on poddać woli Allaha i podążać drogą wskazaną przez niego i jego posłańca Muhammada. Islam jest jednocześnie pokojowy i nacechowany przemocą. Nie można pozbawić go elementu agresji. Jedyny właściwy pogląd to ten, który uwzględnia islam w jego pełni. Polityczna doktryna islamu zawsze pozostawia dwie możliwości, które są równoprawne. Polityczny islam jest w swej naturze dualistyczny i nie sposób tego zmienić. Można zreformować muzułmanów, ale nie da się zreformować islamu. Migaux daje skrócony wykład na temat teoretyków islamskiego fundamentalizmu, reformizmu, salafizmu i dżihadu, a także dokonuje przeglądu organizacji i ruchów fundamentalistycznych oraz terrorystycznych. Najwięcej miejsca poświęca algierskiemu dżihadowi i jego konsekwencjom dla Europy.

Omawiany rozdział, podobnie jak i dwa następne autorstwa Migaux, został napisany w sposób czytelny i bez zbędnych powtórzeń. Autor nie uniknął jednak kontrowersyjnych sformułowań i rażących błędów. Niektóre z nich recenzent postara się wymienić. Po pierwsze, Mekka nie została zajęta przez proroka Muhammada w 632 r. (s. 232), tylko dwa lata wcześniej, Muawija nie należał do rodu proroka (Haszim), lecz do rodu Szams (s. 235). Na s. 236 Migaux pisze: *Około 850 roku krystalizuje się termin „dżihad"*… (s. 236). Nie wiadomo, skąd ta data, ponieważ to określenie było już od lat wykrystalizowane. Słowo „dżihad" wcześniej występowało w tekstach islamu (Koran, hadisy, siry). Malik ibn Anas (zm. w 795 r.), arabski teoretyk państwa i prawa (szkoła malikicka), rozbudował idee dżihadu jako walki zbrojnej. Opisywał, jak powinien działać bojownik islamski, jak dzielić łupy i jak interpretować śmierć w boju. W 797 r. Abdallah ibn al-Mubarak napisał *Kitab al-Dżihad* (*Księgę dżihadu*). Migaux popełnił błąd w tekście dotyczącym pierwszej wyprawy krzyżowej (1096-1099). Wyprawę kierowaną przez Piotra Pustelnika (tzw. ludową), zakończoną klęską, nazwał pierwszą, a drugą według niego była krucjata rycerska, zakończona w 1099 r. zdobyciem Jerozolimy (s. 238). Tymczasem wszystko to działo się podczas pierwszej wyprawy. Do drugiej krucjaty doszło natomiast w latach 1147-1149. Na s. 242 Migaux pisze: *Kilka lat zajęło egipskim Mamelukom* [sic!] *zwalczenie tych nowych zdobywców* (mowa o wahhabitach na Półwyspie Arabskim). Tymczasem kampanię przeciwko wahhabitom w Arabii prowadziły w latach 1811-1818 wojska Muhammada Alego dowodzone przez jego syna

Ibrahima, ale bez udziału mameluków (zostali oni całkowicie wyniszczeni w 1811 r. przez Muhammada Alego). Na s. 258 czytamy: *Nowy przywódca Egiptu, generał Husni Mubarak, zrozumiał, że represje, chociaż prowadzone żelazną ręką, nie są wystarczające, tym bardziej że w 1982 roku trzeba było wysłać czternaście tysięcy żołnierzy, aby przez sześć tygodni szturmowali slumsy Imbaba w Górnym Egipcie, które ogłosiły się Republiką Islamu*. Cytowane wydarzenia rozegrały się w 1992 r. w Imbabie, która jest robotniczą dzielnicą Gizy na przedmieściach Kairu, a więc w Dolnym Egipcie.

W rozdziale jedenastym pt. *Al-Kaida i polityka zjednoczenia ruchu mudżahedinów* również nie uniknięto kilku błędów. Autor pisze: *Rohan Gunaratna uznaje pułapkę w samochodzie Azzama, bardzo nowoczesną pod względem techniki terrorystycznej (mechanizm wybuchowy uruchamiany na odległość), za dzieło Egipcjan z Al-Dżihadu, kierowanych przez nowego mentora, Usamę Ibn Ladena* (s. 280). Do zamachu na Abdullaha Azzama doszło 24 listopada 1989 r. Najprawdopodobniej stał za nim Ajman az-Zawahiri, który kierował Egipskim Islamskim Dżihadem, a nie Osama bin Laden. W czerwcu 2001 r. Al-Kaida połączyła się z Egipskim Islamskim Dżihadem w Al-Kaida al-Dżihad. Hasan at Turabi nie był sekretarzem generalnym Ludowej Konferencji Arabskiej i Islamskiej, jak pisze Migaux na s. 282, lecz Islamskiego Frontu Narodowego (Al-Dżabha al-Islamijja al-Kawmujja) utworzonego w 1985 r. w Sudanie. Z jego inicjatywy w kwietniu 1991 r. w Chartumie odbyła się Konferencja Narodów Arabskich i Muzułmańskich, której przewodniczył Turabi. Uczestniczyli w niej przedstawiciele organizacji fundamentalistycznych z 55 krajów. Słynna fatwa skierowana do wszystkich muzułmanów z apelem o zabijanie Amerykanów została ogłoszona przez bin Ladena 23 lutego 1998 r., a nie 2 lutego 1998 r. (s. 286). W tym samym akapicie znajduje się stwierdzenie, że sygnatariuszem deklaracji powołującej Światowy Front Islamski na rzecz Dżihadu przeciwko Żydom i Krzyżowcom był m.in. pakistański Ruch Towarzyszy Proroka (Harakat ul-Ansar). Tymczasem podpisał ją Mir Hamzah, który w tamtym czasie przewodził Stowarzyszeniu Ulemów Pakistanu (Dżamiat Ulema-e Pakistan). Na następnej stronie jest kolejny błąd w dacie. Do słynnej bitwy w Mogadiszu, w której zginęło 18 amerykańskich żołnierzy, doszło nie 18 sierpnia 1993 r., lecz 3–4 października tego samego roku. Do ataków na ambasady USA w Kenii i Tanzanii, o których czytamy na stronie 288, doszło nie 8 sierpnia, lecz 7 sierpnia 1998 r. i wśród 224 zabitych było 12 Amerykanów, a nie 7, jak stwierdza autor. Recenzent ma wątpliwości również co do istnienia w Jordanii organizacji Miecz Mahometa (Sajf al-Muhammad), rozbitej 3 grudnia 1999 r., a przede wszystkim co do sprawowania nad nią przywództwa przez Palestyńczyka Muhammada al-Makdisiego. Tą grupą mogła być natomiast Dżund asz-Szam (Armia Lewantu), zrzeszająca jordańskich ochotników walczących w Afganistanie. Na jej czele stał Abu Musab az-Zarkawi, a nie Abu Muhammad al-Makdisi. Przygotowywała ona zamach millenijny na hotel Radisson w Ammanie.

W rozdziale dwunastym, zatytułowanym *Przyszłość ruchu fundamentalistycznego*, Migaux analizuje kilka problemów związanych z lokalnymi grupami dżihadystycznymi, możliwościami wykorzystania przez nie broni masowego rażenia, terroryzmem

morskim i współpracą między islamskimi organizacjami terrorystycznymi. Pomimo krytycznych uwag trzy ostatnie rozdziały czyta się najlepiej. Jednak brak przypisów w tych tekstach całkowicie pozbawia je waloru naukowości. Wydawałoby się, że po ich lekturze, zgodnie z logiką i porządkiem chronologicznym, będzie kontynuowany wątek muzułmańskiego terroryzmu. Tymczasem czytelnik ma przed sobą rozdział pt. *Akcje samobójcze: między wojną a terroryzmem*, poświęcony wyłącznie terroryzmowi samobójczemu. Jego autor, François Géré, powraca do starożytności, a następnie – przez średniowiecze do czasów współczesnych – dokonuje przeglądu przypadków poświęcania się dla Boga i sprawy. Zbyt mało miejsca, niestety, przeznaczył na wyjaśnienie problemu męczeństwa w islamie. W przypisach brakuje odniesień do podstawowej pracy dotyczącej tego zagadnienia, czyli do książki Davida Cooka *Martyrdom in Islam*, wydanej w 2007 r. przez Uniwersytet Cambridge.

W rozdziale czternastym uwaga czytelnika zostaje skierowana w jeszcze inną stronę, a mianowicie na problematykę podejścia Stanów Zjednoczonych do terroryzmu. Na wstępie Arnaud Blin wyjaśnia, dlaczego odrębny rozdział poświęca USA. Autor dokonuje szybkiego przeglądu zjawiska terroryzmu w Stanach Zjednoczonych od XIX w. do czasu wkroczenia wojsk amerykańskich i brytyjskich do Iraku wiosną 2003 r. Wskazuje to na przeniesienie tekstu z pierwszego wydania książki w 2004 r., bez najmniejszej próby jego aktualizacji. Blin nie wspomniał tu o takich istotnych wydarzeniach, jak powstanie i rozwój fundamentalizmu protestanckiego, ruchów millenarystycznych, terroryzmu w sektach, terroryzmu aborcyjnego i terroryzmu obrońców środowiska. Także Rohan Gunaratna, autor następnego rozdziału, zatytułowanego *Nowy wizerunek Al-Kaidy: zagrożenie muzułmańskim terroryzmem po 11 września*, nie wykracza poza rok 2003. O tym, że tekst ma charakter historyczny, świadczy zdanie: *Obecnie Al-Kaida jest w okresie przejściowym*, zamieszczone na początku rozdziału (s. 375). Omawiany rozdział również jest pozbawiony przypisów, podobnie jak rozdział szesnasty pt. *Panorama sytuacji po 2004 r.*, autorstwa Philippe'a Migaux, Autor dokonuje w nim geograficznego przeglądu zdarzeń o charakterze terrorystycznym w sposób niezwykle skrótowy i chaotyczny, nie wychodząc poza rok 2005 (tylko w dwóch przypadkach zahacza o rok 2006). Zaczyna od Europy, choć właściwsze byłoby określenie „od Unii Europejskiej". Omawiając sytuację w krajach Afryki, wymienia Algierię, ale nie wspomina o powstaniu i działalności Organizacji Al-Kaidy w Krajach Islamskiego Maghrebu (Tanzim Al-Kaida bi Bilad al-Maghrib al-Islami). W przypadku Tunezji pisze: *Od zamachu na Dżerbie w Tunezji nie doszło do żadnego innego, poza groźbami wysuwanymi pod adresem zachodnich ambasad przez nieznaną organizację Dżihadi Dżund al-Islam (Dżihad Bojowników Islamu)* (s. 398). Przecież od zamachów na Dżerbie 11 kwietnia 2002 r. do czasu wydania tej książki w 2015 r. w Tunezji doszło do całej serii zamachów terrorystycznych. O Somalii, Nigerii i Kenii autor nawet nie wspomniał, podobnie jak o Jemenie w przypadku Bliskiego Wschodu czy Azji Południowo-Wschodniej. Za to poświęcił półtorej strony na omówienie terroryzmu morskiego, który dokładnie opisał sto stron wcześniej, w rozdziale dwunastym.

Rozdział siedemnasty, zamykający trzecią część książki, nosi tytuł *Dżihadyzm w czasach Da'isz*. Został napisany przez Gérarda Chalianda, który także nie uniknął poważnych błędów. Pisząc na stronie 428 o Abu Bakrze al-Bagdadim, stwierdza: *W 2006 roku utworzył on Państwo Islamskie Iraku, początkowo kierowane przez niejakiego Abu Umara*. Jednak to nie Abu Bakr al-Bagdadi utworzył Państwo Islamskie w Iraku. Powołała je 15 października 2006 r. koalicja sunnickich ugrupowań na czele z Al-Kaidą w Iraku. Ze stwierdzenia, że było ono kierowane przez „niejakiego" Abu Omara, można wnioskować, że była to osoba bliżej nieznana. Jest to przekaz niezgodny z prawdą, chodzi bowiem o Abu Omara al-Baghdadiego, czyli Hamida Dawuda Muhammada Khalila az-Zawiego, byłego oficera armii irackiej, który kierował nową strukturą wraz z Abu Hamzą al-Muhadżirem (Abu Ajjub al-Masri). Dopiero po ich śmierci, która nastąpiła 18 kwietnia 2010 r., przywódcą Islamskiego Państwa w Iraku został Abu Bakr al-Bagdadi. W tym rozdziale można przeczytać także: *Po wyjściu oddziałów amerykańskich w 2011 roku Państwo Islamskie schroniło się w Syrii, zależne od Al-Kaidy, ale zyskujące coraz większą autonomię*. To twierdzenie również jest fałszywe, ponieważ po opuszczeniu Iraku przez wojska USA z końcem 2011 r. Państwo Islamskie przystąpiło do intensywnych działań w tym kraju, ogłaszając m.in. kampanię pod nazwą „Rozbicie murów". W dalszej części rozdziału autor podaje nieprawdziwe informacje dotyczące liczby mieszkańców Mosulu (s. 429) i partii irackich Kurdów walczących z Da'isz. Zamiast DPK (Demokratycznej Partii Kurdystanu) wymienia PPK, czyli turecką Partię Pracujących Kurdystanu (s. 429). Mylące są także informacje dotyczące podziału Państwa Islamskiego na trzy prowincje w Syrii i czwartą w Iraku (s. 430) – w rzeczywistości początkowo utworzono ich aż 17. Nie ma plemienia Abu Nima, jest Al-Bu Nimr (na tej samej stronie). To tylko niektóre przykłady informacji wprowadzających czytelnika w błąd. Nieprawdziwe informacje występują również w dalszej części rozdziału. Dotyczą one dat i nazw organizacji, co znacznie obniża wartość opracowania. Zdaniem autora recenzji, w celu zachowania ciągłości narracji, o ile w ogóle taką można by uzyskać, rozdziały od 15. do 17. powinny być umieszczone po rozdziale 12., a rozdziały 13. i 14. powinny być przesunięte na koniec części trzeciej książki.

Część czwarta składa się z czterech rozdziałów (18.–21.), przy czym pierwszy i ostatni są pozbawione przypisów. W pierwszym, zatytułowanym *Literatura i terroryzm*, zamieszczono fragmenty różnych utworów literackich odnoszące się do terroryzmu, autorstwa m.in. Jeana-Paula Sartre'a, Alberta Camusa i Fiodora Dostojewskiego. Trzy kolejne rozdziały są poświęcone tekstom źródłowym autorstwa XIX-wiecznych teoretyków terroryzmu anarchistycznego (rozdział 19.), manifestom i odezwom XX-wiecznych autorów reprezentujących różne organizacje terrorystyczne oraz działaniom antyterrorystycznym (rozdział 20.). W ostatnim rozdziale zaprezentowano zbiór tekstów źródłowych autorstwa muzułmańskich fundamentalistów: od Hasana al-Banny do Ajmana az-Zawahiriego. Wszystkie opublikowano nie później niż w 2002 r. Zostały więc przeniesione z pierwszego wydania książki, a redaktorzy pracujący nad jej drugim wydaniem nie dołożyli starań, aby załączyć wybór najnowszych tekstów, mających zasadnicze znaczenie m.in. dla zrozumienia rozwoju ruchu dżihadystycznego.

Wystarczy wspomnieć chociażby następujących autorów i ich dzieła: Abdel Aziz Issa al-Mukrin – *Praktyczny kurs wojny partyzanckiej* (2003 r.); Abu Bakr an-Nadżi – *Zarządzanie barbarzyństwem* (2004 r.); Mustafa Setmarian Nasar, znany bardziej jako Abu Musab as-Suri – *Wezwanie do światowego muzułmańskiego oporu* (2005 r.) i *Odpowiedzialność ludu jemeńskiego uczestniczącego w dżihadzie na Półwyspie Arabskim* (2007 r.); Fuad Hussein – *Az-Zarkawi: Druga generacja Al-Kaidy* (2005 r.).

W podsumowaniu należy stwierdzić, że zawartość książki nie odpowiada opinii wydawcy, który określił ją jako (…) *ambitną i szeroko zakrojoną pracę*. Publikacja z pewnością nie jest też (…) *prawdziwą wielką encyklopedią terroryzmu*. Być może taką była w 2004 r., kiedy ukazało się jej pierwsze wydanie pt. *Histoire du terrorisme: de l'Antiquité à al-Qaida* (*Historia terroryzmu od starożytności do Al-Kaidy*). Dostrzega się w niej braki w zachowaniu chronologii, a przede wszystkim powtórzenia wynikające z poruszania tej samej problematyki w różnych rozdziałach. Znacznie właściwiej byłoby – zdaniem autora recenzji – podzielić opisywane przejawy terroryzmu po 1968 r. (jeśli chce się utrzymać tę datę jako cezurę) na terroryzm skrajnie prawicowy, lewacki, separatystyczny, palestyński – świecki, ekologiczny (tej tematyki nie opracowano), fundamentalistyczny we wszystkich religiach, z tym że muzułmański na końcu. Uniknięto by wówczas chaosu, z jakim mamy do czynienia. Według autora recenzji książkę czyta się bardziej jako zbiór luźno ze sobą powiązanych artykułów niż jedną spójną publikację. Autorzy poszczególnych rozdziałów często nawiązują do historycznych źródeł wielu zdarzeń, powtarzając te same tematy.

W publikacji jest wiele skrótów myślowych, które dla czytelników o niewielkiej wiedzy na temat np. działalności lewackich organizacji terrorystycznych w Europie i Ameryce Łacińskiej mogą być mało zrozumiałe. Uwagi krytyczne nie pozwalają recenzentowi na zachęcenie potencjalnych czytelników do lektury omawianej książki. Można przy tym żałować, że ambitne opracowanie, na które autorzy poświęcili tyle pracy przy jego pierwszym wydaniu, 11 lat później okazało się nieco wzbogaconą w treści kopią pierwowzoru. Nie o to chyba chodziło.

ROBERT BORKOWSKI
ORCID: 0000-0001-7086-9455

DOI: 10.4467/20801335PBW.21.012.13569

Peter Warren Singer, Emerson T. Brooking, *Nowy rodzaj wojny: media społecznościowe jako broń*[1]

Analiza przebiegu wojen, konfliktów czy rewolucji to żmudne zadanie, gdyż niejednokrotnie trudno znaleźć wyjaśnienie, dlaczego niektóre procesy przebiegają błyskawicznie i w sposób nieoczekiwany, a inne toczą się powoli, co umożliwia przewidywanie rozwoju sytuacji. Jest to *de facto* poszukiwanie odpowiedzi na pytanie o skuteczność działań, dzięki którym osiąga się przewagę nad przeciwnikiem. Zarówno dla historyków wojskowości, jak i dla strategów jednym z najważniejszych problemów badawczych jest zidentyfikowanie czynników, które przyczyniły się do osiągnięcia sukcesów w wojnach błyskawicznych, takich jak mongolskie podboje w średniowieczu, ofensywa islamu za czasów pierwszych kalifów, niemiecki blitzkrieg, obalenie Saddama Husajna w wyniku amerykańsko-brytyjskiej inwazji czy ofensywa ISIS w Syrii i Iraku.

Próbę refleksji nad naturą współczesnych konfliktów podjęło dwóch specjalistów, którzy od dawna pełnią funkcje doradcze w wielu amerykańskich instytucjach, w tym w służbach wywiadowczych. Doktor Peter Warren Singer jest autorem cenionych publikacji poświęconych wojnom i wojskowości, a politolog Emerson T. Brooking jest ekspertem z zakresu wojny informacyjnej i byłym pracownikiem Krajowej Rady Bezpieczeństwa. Sam tytuł ich wspólnej książki może wzbudzić ciekawość, jakkolwiek wykorzystywanie mediów społecznościowych do celów politycznych ma już bogatą historię. Z jednej strony aktywiści ruchów protestu szybko zrozumieli, jaki potencjał mobilizacji społecznej można uruchomić za pomocą nowych sposobów komunikowania się (co było widoczne chociażby podczas wydarzeń związanych z Arabską Wiosną), z drugiej – z internetowych narzędzi korzystają rządzący, służby specjalne i siły zbrojne w celu manipulowania postawami i nastrojami społecznymi. Zdaniem autorów

[1] P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny: media społecznościowe jako broń* (tytuł oryginału: *Like War. The Weaponization of Social Media*), tłum. S. Baranowski, Kraków 2019, Vis-á-vis Etiuda, 296 s.

skonfliktowane strony przygotowują się do starć na Twitterze w takim samym stopniu, jak do bezpośrednich, fizycznych konfrontacji, co dowodzi znaczenia psychologicznych i medialnych aspektów dyskursu politycznego. Próby cenzurowania informacji zamieszczanych w sieci i ograniczania swobody dostępu do niej podejmowane przez totalitarne i autorytarne reżimy polityczne nie powinny więc dziwić. Najsilniejsze mechanizmy kontroli stworzyły władze Chin, czym dały przykład reżimom na całym świecie. Chiny cenzurują Internet przez stosowanie embarga na pewne treści i umieszczanie określonych słów kluczowych na liście prohibitów. Wykorzystują także aplikacje instalowane w smartfonach w celu obserwowania aktywności półtora miliarda swoich obywateli. Kolejne państwa wprowadzają, m.in. pod pretekstem monitorowania rozprzestrzeniania się pandemii SARS-CoV-2, różnego rodzaju aplikacje szpiegowskie, których można używać do kontrolowania zachowań ludzi. Z kolei w Syrii z chwilą wybuchu fali protestów społecznych w 2011 r. rząd zdecydował o wyłączaniu Internetu w piątki, gdyż w ten dzień Syryjczycy organizowali demonstracje przy okazji spotkań w meczetach (s. 126).

W początkowych partiach książki Singer i Brooking skupili się na omówieniu propagandowych działań dżihadystów z ISIS, przede wszystkim na znaczeniu hasztagu #AllEyesOnISIS. Przez rozpowszechnianie filmów ukazujących egzekucje islamscy terroryści osiągnęli cel, którym było wywołanie powszechnego przerażenia i destabilizowanie sił rządowych. Autorzy opisują działalność czołowego dżihadysty internetowego Junaida Hussaina, którego aktywność w sieci okazała się dla Ameryki zagrożeniem równie poważnym jak działania zbrojnych dżihadystów. Na skutek agresywnej propagandy ISIS upowszechniło się przekonanie o sile i omnipotencji terrorystów (s. 202). Dziś prawie każdy akt przemocy lub przestępstwo z udziałem muzułmanina jest w środkach masowego przekazu określane, często niesłusznie, jako terroryzm, co z kolei prowadzi do podsycania paniki moralnej. Zrozumienie niebywałej skuteczności przesyconych okrucieństwem komunikatów ISIS jest możliwe, jeśli uzmysłowimy sobie statystyki dostępu do sieci w irackim społeczeństwie. Do chwili obalenia Saddama Husajna dostęp do Internetu i telefonii komórkowej był ściśle reglamentowany przez reżim. Tylko w ciągu roku od momentu amerykańskiej inwazji liczba abonentów sieci komórkowych wzrosła ze 150 tys. do 4 mln, a więc prawie 27-krotnie (s. 12–13). Warto zwrócić uwagę, że zadziałał tam, o czym autorzy książki nie wspominają, efekt nowości środka komunikowania i przypisywania wiarygodności nowym mediom przez społeczeństwo, które doświadczyło dyktatury i nie potrafiło podejść sceptycznie do wolnorynkowych reguł gry na rynku medialnym. Tego rodzaju brak krytycyzmu, silne reakcje emocjonalne i masowa naiwność stały się udziałem również polskiego społeczeństwa w początkowym okresie transformacji, na potwierdzenie czego wystarczy przypomnieć błyskawiczną karierę Stana Tymińskiego w 1991 r. Wybuch emocji wśród Polaków poszukujących przywódcy był jednak nieporównanie mniejszy niż w irackim społeczeństwie zagrożonym krwawą ofensywą partyzantów ISIS.

Singer i Brooking słusznie podkreślają, że to wszystko to nic nowego, nowe są jedynie środki komunikacji. Schemat wojennej ofensywy propagandowej pozostaje taki

sam jak chociażby podczas niemieckiej ofensywy we Francji w 1940 r. O szybkim tempie można w tym przypadku mówić nie tylko w odniesieniu do ruchu niemieckich czołgów, lecz także do rozpowszechniania przez stacje radiowe wiadomości o kolejnych porażkach francuskich oddziałów. Duże zintensyfikowanie tych komunikatów wpłynęło demoralizująco i demobilizująco na francuskich żołnierzy i przyczyniło się do ich klęski, wywołując, jak napisał Marc Bloch, „gorączkę ucieczki" (s. 16). W piśmiennictwie naukowym wielokrotnie zwracano uwagę, że wykorzystanie radia umożliwiło Hitlerowi dojście do władzy. Autorzy książki także podkreślają pozytywny wpływ propagandy radiowej na osiąganie celów taktycznych w trakcie działań wojennych Wehrmachtu. Szkoda, że w pracy nie przytoczono innego przykładu z Bliskiego Wschodu pokazującego podatność arabskich społeczeństw na panikę. Otóż podczas walk arabsko-żydowskich w 1948 r., w izraelskiej historiografii zwanych wojną o niepodległość, palestyńscy przywódcy w komunikatach emitowanych przez radio wzywali Palestyńczyków do ucieczki przed rzekomym zagrożeniem czystką i krwawymi rzeziami ze strony okrutnych żołnierzy izraelskich, a jednocześnie zapewniali o rychłym arabskim zwycięstwie. Ten przekaz propagandowy okazał się jednym z najbardziej skutecznych w historii radia – wzbudził wśród Palestyńczyków masową panikę i spowodował exodus. Historia potoczyła się jednak inaczej niż zapowiadano, a brak wyobraźni arabskich liderów wpłynął na los 6 mln mieszkańców Autonomii Palestyńskiej.

Ofensywa medialna ISIS w Iraku jest jednym z kilku przykładów opisanych przez autorów książki. Dużo uwagi poświęcają oni również wykorzystaniu mediów społecznościowych przez strony walczące w Donbasie (s. 18–19). Stwierdzają, że (…) *fizyczne i cyfrowe pole walki znajdowały się niesamowicie blisko siebie* (s. 20). Stawiają pytanie o to, jak należy pojmować dziś wojnę w sensie działań zbrojnych, skoro za pomocą środków cyfrowej komunikacji można zmienić przebieg bitwy czy nawet wyeliminować jej potrzebę (s. 21). Można odnieść wrażenie, że w tym dylemacie pobrzmiewają echa rozważań teoretyków sztuki wojennej Sun Tzu i Carla von Clausevitza, szczególnie że autorzy przytaczają później wypowiedź gen. Walerego Gierasimowa o wzroście roli (…) *środków niemilitarnych w dążeniu do osiągnięcia celów politycznych i strategicznych. W wielu przypadkach mają one przewagę nad bronią i jej skutecznością* (s. 151).

W kolejnych rozdziałach autorzy podejmują rozważania o tym, czym w ogóle jest Internet i w jaki sposób zmienił on świat społeczny. Interesuje ich zwłaszcza to, jak pierwsze wyobrażenia społeczne o roli Internetu rozminęły się z rzeczywistością. Formułują kilka tez na temat rozwoju sieci, wskazując, że Internet wyszedł już z „wieku dojrzewania". Obecnie stał się m.in. polem walki, które przeobraża się w czasie trwania konfliktu, a ta walka zmienia sens słowa „wojna", wszyscy bowiem jesteśmy jej uczestnikami (s. 36–37). W innym miejscu autorzy konstatują jednak, że pod wieloma względami Internet przeszedł taką samą ewolucję jak wszystkie wcześniejsze środki komunikacji (s. 77). Takich sprzeczności jest w tej książce więcej, być może Singer i Brooking nie do końca przedyskutowali swoje poglądy. Kilkadziesiąt stron książki nie wnosi nic nowego do historii Internetu. Dobrze jednak, że przypomniano o amerykańskich specjalistach w dziedzinie informatyki – Josephie Carlu Robnetcie

Lickliderze i Robercie Wiliamie Taylorze. W 1968 r. przewidzieli oni, że komputery staną się narzędziem powszechnej komunikacji oraz że pojawi się wielka sieć komputerowa (już rok później powstał ARPANet). Singer i Brooking piszą o współczesnej cyberwojnie oraz o wojnie sieciowej, przypominając jednocześnie o amerykańskich politologach Johnie Arquilli i Davidzie Ronfeldcie, których pierwsze prognozy (z 1990 r.) Pentagon utajnił i dopiero trzy lata później mogli oni opublikować artykuł na temat nowych zagrożeń i łamania zabezpieczeń w sieci (s. 227).

Omawiając działania rosyjskiej Agencji Badań Internetowych (ang. Internet Research Agency) w Petersburgu, w polskich mediach powszechnie określanej „fabryką trolli", autorzy nie nazywają pracowników tej agencji „trollami z Olgino[2]" a „pacynkami". Uznają, że boty, *fake newsy* czy szerzenie teorii spiskowych to narzędzia powszechnie wykorzystywane we współczesnej komunikacji sieciowej.

Singer i Brooking wyjaśniają nie tylko, w jaki sposób rozwija się nowe środowisko informacyjne, lecz także to, dlaczego jesteśmy tak podatni na manipulacje. Autorzy wskazują również, że właściciele mediów społecznościowych nie kwapią się do usuwania nawet ewidentnie fałszywych kont (s. 187). Wyjaśniają mechanizmy homofilii[3] i tzw. efektu potwierdzenia[4] (s. 173), które sprzyjają powstawaniu grup siejących nienawiść. Jako przykład podają teorię spiskową zwaną Pizzagate, w ramach której współpracownicy Donalda Trumpa przeprowadzili kampanię oczerniającą Hillary Clinton. Autorzy twierdzą, że chociaż Facebook, Microsoft, Twitter i Google od dawna zdawały sobie sprawę, w jaki sposób ich produkty i usługi są wykorzystywane do wzniecania nienawiści i rozpowszechniania fałszywych informacji, to dopiero w 2016 r. postanowiły podjąć działania zapobiegające najpoważniejszym wykroczeniom, tj. szerzeniu w sieci terrorystycznej propagandy, nienawiści i pornografii dziecięcej (s. 268). Tym samym pojawił się problem cenzury Internetu. Autorzy książki podkreślają hipokryzję Marka Zuckerberga, który odmawia usuwania nienawistnych wpisów Donalda Trumpa, motywując to względami biznesowymi, czyli groźbą utraty konserwatywnych użytkowników i obniżenia zysków (s. 272).

Kolejny aspekt rozwoju mediów społecznościowych, na który zwracają uwagę obaj analitycy, to możliwość penetrowania zasobów Internetu i analizy ogromnej ilości danych przez użytkowników sieci. Mamy więc do czynienia z zupełnie nową formułą OSINT[5]. W książce opisano wyniki śledztwa brytyjskiego dziennikarza Eliota Higginsa i witryny dziennikarstwa śledczego Bellingcat dotyczącego zestrzelenia w 2014 r.

---

[2] W Olgino na przedmieściach Petersburga mieści się biuro Agencji Badań Internetowych (przyp. red.).

[3] Homofilia – upodobanie do podobieństwa, skłonność do akceptacji poglądów osób podobnych, reprezentujących tę samą grupę społeczną i podobny styl życia (przyp. aut.).

[4] Efekt potwierdzenia – tendencja do preferowania informacji, które potwierdzają wcześniejsze oczekiwania i hipotezy, niezależnie od tego, czy te informacje są prawdziwe. Za: Wikipedia [dostęp: 8 XII 2020] – przyp. red.

[5] *Open-source intelligence* (OSINT) – gromadzenie informacji pochodzących z ogólnodostępnych źródeł, biały wywiad (przyp. red.).

samolotu MH17 nad Ukrainą (s. 108). Obywatelskie śledztwo potwierdziło informacje posiadane przez służby specjalne kilku państw zainteresowanych sprawą. Tym samym wiele zagadnień, które kiedyś były objęte klauzulą tajności, współcześnie staje się *de facto* publiczną informacją. Dotyczy to także zagadnień militarnych, takich jak dyslokacje wojsk, przygotowywanie operacji militarnych czy udział określonych jednostek wojskowych w danych działaniach. Autorzy przytaczają opinię amerykańskiego generała Marka Mallory'ego, który stwierdził, że (…) *po raz pierwszy w historii jest rzeczą prawie niemożliwą nie być obserwowanym* (s. 86). Rozdział książki poświęcony tej tematyce jest jednym z najciekawszych.

Singer i Brooking wyjaśniają również, na czym polega skuteczność w polityce oraz siła propagandowego oddziaływania. Podkreślają, że warunkiem sukcesu jest stworzenie i narzucenie własnej narracji, którą muszą cechować prostota, rezonans i nowość (s. 205–208). Prostota to zrozumiałość przekazu dla szerokich mas odbiorców. Rezonans to nośność haseł i pozytywna reakcja na treści, które trafiają do przekonania dużej liczbie odbiorców. Walor nowości oznacza, że narrator tak dobrał werbalne instrumenty komunikacyjne oraz środki wyrazu, że udaje mu się stworzyć wrażenie przedstawiania całkowicie nowych idei. To chyba najbardziej interesująca część rozważań autorów, dlatego szkoda, że nie została bardziej rozbudowana.

Wykorzystanie mediów społecznościowych jest, jak twierdzą Singer i Brooking, rodzajem nowej broni w arsenale środków wojny psychologicznej. Cechą relacji między procesami kumulowania i dystrybucji informacji w Internecie a polityką i wojną jest, co oczywiste, sprzężenie zwrotne. Terroryści planują zamachy i nierzadko je transmitują na żywo, „wojny twitterowe" są źródłem ofiar w rzeczywistym świecie, a rozprzestrzeniające się błyskawicznie dezinformacje nie tylko zmieniają wyniki starć zbrojnych, lecz także mogą przesądzić o losach całych narodów. W rezultacie polityka i wojna rozgrywają się w znacznej mierze na smartfonach i w ten sposób wszyscy jesteśmy częścią walki, która toczy się w Internecie (s. 282–283). Autorzy podają wiele informacji na temat ćwiczeń US Army w kompleksie o nazwie Kirsham Social Media Environment and Internet Replication (SMEIR), które są mało znane. W SMEIR przeprowadza się symulacje zarówno działań zbrojnych, jak i ataków w formie kampanii w mediach społecznościowych (s. 281).

Konkludując swoje rozważania, Singer i Brooking proponują nową perspektywę poznawczą, która umożliwia lepsze zrozumienie zagrożeń w sieciocentrycznym porządku świata i podjęcie skutecznej obrony przed nimi. Model tego, co powinniśmy zrealizować, pochodzi, jak piszą autorzy, z krajów, które odeszły od reorganizacji militarnej na rzecz edukacji swojego społeczeństwa na temat zagrożeń informacyjnych. Nieprzypadkowo wśród krajów, które uczyniły to jako pierwsze, są Finlandia, Estonia, Szwecja, Litwa i Łotwa. Jak wiadomo, poziom powszechnego nauczania jest w nich bardzo wysoki, a metody nauki nowoczesne i nastawione na kształtowanie krytycyzmu, racjonalizmu i samodzielności w myśleniu. Trudno oprzeć się wrażeniu, że w polskim systemie szkolnictwa wdrożenie tego rodzaju propozycji byłoby niemożliwe.

W tekście, znakomicie zresztą przetłumaczonym, rażą hipostazy bezustannie stosowane przez autorów, polegające na przypisywaniu realnego atrybutu rzeczom abstrakcyjnym. Autorom zabrakło ponadto konsekwencji w przedstawianiu kolejnych wątków tematycznych – układ treści książki nie jest uporządkowany ani chronologicznie, ani pod względem rangi omawianych problemów. Zważywszy na profesję autorów, można by było oczekiwać większej precyzji w narracji i bardziej pogłębionej refleksji. Pewnym wytłumaczeniem mogą być względy rynkowe, które zdecydowały zapewne o opublikowaniu książki łatwej w odbiorze kosztem pewnych uproszczeń. Niemniej *Nowy rodzaj wojny*… można polecić każdemu, kogo interesuje kondycja współczesnego świata i rosnący wpływ mediów społecznościowych na różne sfery życia. Jej lektura pozwala na przypomnienie i uporządkowanie wiedzy na temat zjawisk tworzących nowy ład w społeczeństwie informacyjnym, który jest w istocie bezustanną walką o panowanie nad umysłami.

MAŁGORZATA KUDZIN-BORKOWSKA
ORCID: 0000-0002-5816-3676

DOI: 10.4467/20801335PBW.21.014.13571

Marek Górka, *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*[1]

Marek Górka w pionierskiej monografii na temat bezpieczeństwa cybernetycznego państw Grupy Wyszehradzkiej (dalej: Grupa V4) podjął rozważania nad wieloma ważnymi problemami informacyjnego i informatycznego ładu naszych czasów. Autor określił ramy chronologiczne swoich dociekań na lata 2013–2017, jednak w wielu miejscach wykracza poza wyznaczoną cezurę czasową z uwagi na konieczność dogłębnego wyjaśnienia przyczyn wybranych zjawisk, wydarzeń i ich konsekwencji. Praca ma charakter interdyscyplinarny, obejmuje obszar polityczny, społeczny i gospodarczy funkcjonowania Grupy V4. Monografia składa się ze wstępu oraz pięciu rozdziałów poświęconych kolejno: cyberbezpieczeństwu NATO i Unii Europejskiej, bezpieczeństwu państw członkowskich Grupy V4, cyberzagrożeniom, technologiom informacyjnym oraz perspektywom polityki cyberbezpieczeństwa państw Grupy V4. Całości pracy dopełniają obszerna bibliografia, wykaz stosowanych skrótów i zbiór aneksów z danymi tabelarycznymi.

Książka liczy 340 stron. Objętość dwóch pierwszych rozdziałów jest zbliżona (67 i 68 stron), podobnie trzeciego i czwartego (47 i 43 strony), ostatni rozdział jest najkrótszy (29 stron). Zakończenie liczy siedem stron. Bibliografia jest podzielona właściwie, złożona z 26 stron, a aneksy z 22 stron, co razem stanowi 12 proc. objętości książki. W bibliografii zaskakuje brak wartościowych pozycji autorstwa Wojciecha Gizickiego i Iwony Pawlikowskiej. Pojawia się też błędny zapis niektórych pozycji, np. monografii nr 25.

We wstępie liczącym niemal 14 stron autor uznaje, że Grupa V4 jest najbardziej dynamiczną organizacją w subregionie Europy Środkowej. Podkreśla zasadniczy cel współpracy państw członkowskich Grupy V4, którym jest założenie, że sąsiedztwo

[1] M. Górka, *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*, Warszawa 2019, 340 s.

geograficzne powinno stanowić podstawę do zbliżonego postrzegania bezpieczeństwa i wspólnego, solidarnego działania na jego rzecz. Zmiany gospodarcze, polityczne i społeczne, które zachodzą w państwach Grupy V4, są postrzegane przez opinię międzynarodową jako wzorowy przykład transformacji w Europie Środkowo-Wschodniej. Cyberprzestrzeń jest niezbędna do prawidłowego funkcjonowania państwa i społeczeństwa. Z uwagi na globalny zasięg Internetu niektóre podmioty polityczne usiłują wykorzystywać cyberprzestrzeń do osiągania własnych celów.

Zdaniem Marka Górki wykorzystanie cybertechnologii wzrosło w pierwszej dekadzie XXI w., a nabierający tempa proces cyberrewolucji powoduje konieczność wprowadzenia zmian w zarządzaniu bezpieczeństwem państwa. W 2014 r. pojawiła się potrzeba określenia nowego kierunku współpracy Polski, Słowacji, Czech i Węgier m.in. na płaszczyźnie polityki bezpieczeństwa cybernetycznego. Wszystkie państwa członkowskie Grupy V4 podkreślają ogromne znaczenie cyberbezpieczeństwa, czemu dają wyraz w dokumentach i programach strategicznych. Autor w zdecydowany sposób stawia tezę, że mimo deklaracji współpracy poszczególne państwa różnie postrzegają zagrożenia płynące z cyberprzestrzeni, a tym samym ich zaangażowanie w rozwój technologiczny jest odmienne.

Autor podkreśla we wstępie, że obszar badań podjętych w monografii jest złożony i interdyscyplinarny. Jako główny cel pracy wskazuje analizę różnych aspektów polityki cyberbezpieczeństwa państw członkowskich Grupy V4, z uwzględnieniem ich funkcjonowania w ramach NATO i Unii Europejskiej. Ponadto wyodrębnia cztery dodatkowe cele badawcze, które są *de facto* problemami szczegółowymi. Jeden z nich dotyczy różnic i podobieństw w definiowaniu i prowadzeniu polityki cyberbezpieczeństwa w Grupie V4. Marek Górka podjął próbę weryfikacji pięciu hipotez badawczych, które dotyczą cyberbezpieczeństwa, cyberzagrożeń i wyzwań dla polityki w Europie Środkowej, a szczególnie w Grupie V4.

Rozdział pierwszy jest złożony z dwóch części, które dotyczą polityki bezpieczeństwa cybernetycznego NATO i UE. Jego treść obejmuje opis i ocenę starań instytucjonalno-prawnych tych organizacji w celu włączenia bezpieczeństwa cybernetycznego do głównego kierunku ich działań. Autor wyraźnie wskazuje etapy ewolucji cyberbezpieczeństwa, które weryfikowały sprawność instytucjonalną obu organizacji wobec nowych wyzwań, jakie stanowią cyberzagrożenia.

W rozdziale drugim, pt. *Uwarunkowania cybernetyczne i pozacybernetyczne państw Grupy Wyszehradzkiej,* Górka prezentuje politykę Grupy V4, poczynając od jej genezy i uwarunkowań historycznych. Przedstawia klasyfikację polityki państw Grupy V4 i charakteryzuje ich aktywności w kontekście celów formułowanych podczas poszczególnych prezydencji. Górka wyodrębnia najważniejsze inicjatywy międzynarodowe, które miały odzwierciedlenie w publikowanych dokumentach stanowiących materiał do określenia polityki cyberbezpieczeństwa państw Grypy V4. W ostatniej części tego rozdziału autor omawia strategie cyberbezpieczeństwa poszczególnych państw Grupy V4 i przedstawia analizę ich wydatków budżetowych w tym zakresie.

Rozdział trzeci, zatytułowany *Cyberzagrożenia jako czynniki kształtujące politykę państw Grupy Wyszehradzkiej*, składa się z dwóch części. Pierwsza stanowi charakterystykę ataków cybernetycznych i barier badawczych w analizie cyberzagrożeń. W drugiej autor omawia wybrane cyberataki i ich konsekwencje na obszarze państw Grupy V4 oraz czynniki określające cyberatak jako zjawisko polityczne. Dużo uwagi Autor poświęca rodzajom cyberincydentów w Grupie V4 oraz wymianie informacji na temat cyberzagrożeń między wybranymi podmiotami. Górka wysuwa słuszny wniosek, że dezinformacja stanowi niemałe wyzwanie dla polityki państw Grupy V4. Współpraca między państwami członkowskimi tej Grupy w zakresie wymiany specjalistycznej wiedzy na temat bezpieczeństwa informacji odgrywa ważną rolę w zwalczaniu cyberzagrożeń. Zdaniem autora polityka cyberbezpieczeństwa państw Grupy V4 ma charakter pasywny, a aktywność w tej dziedzinie można dostrzec wyłącznie podczas realizacji zadań wynikających z przynależności do Unii Europejskiej.

W rozdziale czwartym, który został poświęcony technologiom informacyjno-komunikacyjnym (dalej: ICT) w polityce cyberbezpieczeństwa państw członkowskich Grupy V4, autor charakteryzuje regiony europejskie w tym kontekście. Podkreśla znaczenie rozwoju ICT zarówno na płaszczyźnie społecznej, jak i gospodarczej. Za pomocą analizy porównawczej Górka starannie i szczegółowo zbadał cztery najważniejsze obszary w celu wskazania podobieństw i różnic w dziedzinie ICT między państwami Grupy V4 a innymi członkami UE. W części pierwszej autor analizuje wskaźniki zawarte w programie Europejskiej Agendy Cyfrowej, które pozwalają scharakteryzować stopień rozwoju ICT w państwach Grupy V4. Druga część stanowi kontynuację analizy postępu cyfrowego wśród państw członkowskich Unii Europejskiej w odniesieniu do indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI). W części trzeciej autor bada wskaźniki, które charakteryzują poziom innowacji w zakresie ICT w państwach Unii Europejskiej. Na tej podstawie określa pozycje państw Grupy V4 w tym obszarze. W części czwartej koncentruje się na czynnikach determinujących funkcjonowanie społeczeństwa cyfrowego, m.in. działaniu i stosowaniu ICT, popularności cyberusług, edukacji, rozwoju technologii, liczbie cyberużytkowników. Obszerna i precyzyjna analiza dokonana w tym rozdziale jest niezwykle wartościowa dla literatury przedmiotu z uwagi na charakterystykę członków Grupy V4 pod kątem wykorzystania ICT. Autor dobitnie podkreśla w wynikach analizy, że państwa członkowskie Grupy V4 w związku z rozwojem społeczeństwa cyfrowego osiągnęły znaczny postęp, ale ich wyniki są zwykle niższe od średnich norm Unii Europejskiej. Ponadto państwa Grupy V4 wykazują wiele podobieństw w obszarze korzystania z cybertechnologii, jednak Słowacja i Czechy prezentują częściej wyższy poziom zaawansowania ICT od Węgier i Polski.

Ostatni rozdział dotyczy perspektyw polityki cyberbezpieczeństwa państw Grupy V4. Autor udowadnia w nim na podstawie szczegółowych badań, że w poszczególnych państwach Grupy V4 profile cybernetyczne różnią się z uwagi na postrzeganie cyberbezpieczeństwa i kulturę polityczną. Dlatego trudno stwierdzić, że Grupa działała jak podmiot jednolity. Na uwagę zasługują cyberstrategie poszczególnych państw członkowskich Grupy V4, których podstawowym zadaniem jest

wzmocnienie krajowego bezpieczeństwa cybernetycznego i określenie działań prowadzących do skutecznego uczestnictwa w organizacjach międzynarodowych. Autor wyraźnie zaznacza, że różne jest postrzeganie i definiowanie cyberbezpieczeństwa w tych strategiach. Jednak wszystkie państwa członkowskie zapowiedziały w tych dokumentach doskonalenie krajowych zdolności w zakresie obrony cybernetycznej oraz zwiększenie środków na ten cel. Element, który występuje we wszystkich strategiach, to nacisk na edukację i badania naukowe w dziedzinie cyberbezpieczeństwa.

Zarówno język, styl, jak i składnia prezentowane w książce Marka Górki są poprawne, choć w wielu miejscach zdarzają się błędy, co świadczy o braku starannej korekty. Terminologia odnosząca się do kwestii ogólnych, jak administrowanie czy rządzenie państwem, nie zawsze jest odpowiednia. Projekt graficzny okładki wyraźnie sugeruje, że książka dotyczy państw Grupy V4. Niepokojące skojarzenia może wywołać jedynie kolorystyka (czerwona) mapy konturowej.

Autor pracy osiągnął wszystkie zamierzone cele badawcze wymienione we wstępie. Na podstawie przeprowadzonych badań scharakteryzował politykę bezpieczeństwa cybernetycznego państw Grupy V4 i wykazał, że jest ona niejako konsekwencją wzajemnych zależności między podmiotami państwowymi, prywatnymi oraz organizacjami pozarządowymi. Udowodnił też, że gwarancją poprawy cyberbezpieczeństwa w poszczególnych państwach członkowskich i w Grupie V4 jako całości jest współpraca sektora państwowego, prywatnego, naukowego i sił zbrojnych.

Monografia wpisuje się w nurt rozważań na temat bezpieczeństwa i polityki Grupy Wyszehradzkiej. Stanowi uzupełnienie i kontynuację refleksji naukowych, które zaprezentowano m.in. w pracach: *Współpraca regionalna państw Grupy Wyszehradzkiej: doświadczenia i perspektywy* autorstwa Anny Czyż (Katowice 2018), *Państwa Grupy Wyszehradzkiej: pomiędzy przeszłością a teraźniejszością. Wybrane aspekty polityki wewnętrznej i zagranicznej* Anny Czyż i Sebastiana Kubasa (Katowice 2014). Książka powinna zainteresować środowiska akademickie i polityczne. Może stanowić cenne źródło wiedzy dla funkcjonariuszy służb policyjnych.

Zamiarem autora było, aby praca uzupełniła literaturę przedmiotu i korespondowała z debatą na temat bezpieczeństwa cybernetycznego, która jest prowadzona na arenie międzynarodowej. Powstanie Grupy V4 miało gwarantować dynamiczną współpracę gospodarczą, polityczną i społeczną jej członków. W tym roku przypada 30. rocznica jej utworzenia, co jest dobrym pretekstem, aby monografię polecić każdemu czytelnikowi, którego interesują zagadnienia związane z tym subregionem. Publikacja Marka Górki stanowi istotny wkład w rozwój badań dotyczących Grupy Wyszehradzkiej.

MARIUSZ KRZYSZTOFIŃSKI
ORCID: 0000-0003-3905-1684

DOI: 10.4467/20801335PBW.21.011.13568

Tytus Jaskułowski, Filip Gańczak, Konrad Knoch, Piotr Abryszeński, Ewa Pejaś, *Raporty polskie Stasi 1981–1989.* Tom 1: *W przededniu stanu wojennego czerwiec–grudzień 1981*[1]

Wybór kardynała Karola Wojtyły na papieża (16 października 1978 r.)[2] oraz powstanie niespełna dwa lata później Niezależnego Samorządnego Związku Zawodowego „Solidarność" (31 sierpnia 1980 r.)[3] okazały się wydarzeniami, które znacząco wpłynęły na proces delegitymizacji władzy komunistycznej w poszczególnych krajach Europy Środkowo-Wschodniej pozostających pod supremacją Związku Sowieckiego. Za sprawą tych wydarzeń, ze zwielokrotnioną siłą, zostało obnażone zakłamanie oraz miałkość ideologiczna partyjnych ośrodków decyzyjnych krajów byłego bloku wschodniego.

We wspomnianym czasie – co zupełnie naturalne – uwaga wielu państw była zwrócona na Polską Rzeczpospolitą Ludową (dalej: PRL), pozostającą częścią imperium zewnętrznego ZSRS[4]. Taka sytuacja była następstwem co najmniej kilku przyczyn.

---

1 T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981–1989.* Tom 1: *W przededniu stanu wojennego czerwiec–grudzień 1981*, Szczecin–Warszawa 2020, IPN, 584 s.

2 G. Weigel, *Świadek nadziei. Biografia papieża Jana Pawła II*, tłum. D. Chylińska, Kraków 2005, s. 344, 355–360, 377–380.

3 Pewną rolę w tej sprawie odegrało uchwalenie 8 IX 1981 r. przez Krajowy Zjazd NSZZ „Solidarność" *Posłania do ludzi pracy Europy Wschodniej*. Zob. J. Holzer, *Polska i Europa. „W Polsce czyli nigdzie?"*, Warszawa 2008, s. 112; G. Majchrzak, *Posłanie I Krajowego Zjazdu Delegatów NSZZ „Solidarność" do ludzi pracy Europy Wschodniej*, „Encyklopedia Solidarności", https://encysol.pl/es/encyklopedia/hasla-rzeczowe/14202,Poslanie-I-Krajowego-Zjazdu-Delegatow-NSZZ-Solidarnosc-do-ludzi-pracy-Europy-Wsc.html [dostęp: 9 I 2021].

4 Zob. S. Weremiuk, *Specyfika stosunków polsko-radzieckich w latach 1944–1991*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11, s. 44. Autor podkreśla, że Polska przez dziesięciolecia była krajem, w którym system polityczny był spenetrowany przez ZSRS. Wyrazem tego było powołanie w 1955 r. i funkcjonowanie Układu Warszawskiego. Przy czym, co istotne, po 1981 r. „(…) nastąpił powrót do głębokiej penetracji" struktur państwowych. Tamże, s. 48–54.

Najważniejsze było jednak to, że od wieków jednym ze strategicznych celów Rosji, decydującym o powodzeniu jej imperialnej polityki już od czasów Piotra I Wielkiego (1672–1725), było kontrolowanie terytorium Polski, co z kolei umożliwiało władanie Europą Środkowo-Wschodnią[5]. Te założenia obowiązywały także w czasach ZSRS. Dodatkowo od początku istnienia komunistycznej Rosji (od 1922 r. – ZSRS) niezwykle istotna była dla niej możliwość swobodnego dotarcia do państwa niemieckiego. Geopolityczne położenie naszego kraju oraz zmiany zapoczątkowane w 1980 r. wzmocniły zainteresowanie Polską ze strony dwóch mocarstw stojących na czele przeciwstawnych bloków państwowych, tj. Stanów Zjednoczonych Ameryki[6] i ZSRS[7], rywalizujących między sobą na wielu polach, co określano mianem „zimnej wojny". Tym samym zmianie uległo postrzeganie Polski przez inne państwa[8] i działające na ich rzecz służby specjalne. Jednym z tych państw była Niemiecka Republika Demokratyczna (dalej: NRD), wysunięta najdalej za zachód sowieckiego „imperium zewnętrznego", obawiająca się – podobnie jak i Czechosłowacja[9] – że ferment ideologiczny, jaki wznieciła polska „Solidarność", może negatywnie oddziaływać również na jej obywateli[10]. Zagrożenie wyczuwane wówczas przez elity komunistycznej NRD było pochodną przekonania,

---

[5] Zob. W.A. Serczyk, *Piotr I Wielki*, Wrocław 1990, s. 167–168. Analizując założenia polityki zagranicznej ZSRS, Marek Kornat zwrócił uwagę na „zaborczość" Rosji Sowieckiej i zaznaczył, że: „U podstaw leninowskiej koncepcji przyszłości rewolucji tkwiła jego wizja bolszewizacji Niemiec". Zob. M. Kornat, *Program czy improwizacja? Idee polityki zagranicznej państwa sowieckiego*, „Dzieje Najnowsze" 2017, nr 4, s. 100. Autor ten dodał również, że zamysły Lenina zniweczyła przegrana wojna z Polską w 1920 r. Tamże, s. 110.

[6] Zob. P. Pleskot, *Kłopotliwa panna „S". Postawy polityczne Zachodu wobec „Solidarności" na tle stosunków z PRL (1980–1989)*, Warszawa 2015; *„Karnawał po amerykańsku". Placówki dyplomatyczne USA w PRL wobec polskich wydarzeń od sierpnia 1980 do grudnia 1981*, wprowadzenie, wybór i opracowanie P. Pleskot, Warszawa 2020.

[7] *Przed i po 13 grudnia. Państwa bloku wschodniego wobec kryzysu w PRL 1980–1982*, t. 1–2, Ł. Kamiński (red.), Warszawa 2006–2007.

[8] P. Jaworski, *Most przez Bałtyk. Szwecja wobec „Solidarności" 1980–1982*, Warszawa 2017; A. Kastory, *Syndrom Jałty. Polityka mocarstw wobec polskich kryzysów w latach 1968–1981*, Kraków 2019; A. Kastory, *Mocarstwa zachodnie wobec kryzysu w Polsce w grudniu 1980 r.*, „Studia Środkowoeuropejskie i Bałkanistyczne" 2017, t. 25, s. 113–126.

[9] A. Kobus, *Czechosłowacja wobec narodzin, rozwoju i delegalizacji „Solidarności" (1980–1982)*, Toruń 2006.

[10] Zob. W. Jarząbek, *Polska w polityce międzynarodowej i „zimnej wojnie" 1945–1989*, w: *Polski wiek XX*, t. 4: *PRL od grudnia 70 do czerwca 89*, P. Persak, P. Machcewicz (red.), Warszawa 2010, s. 324. W jednym z artykułów Piotr Zariczny stwierdził, że liberalna Polska „fascynowała" mieszkańców NRD podróżujących do tego kraju już w latach 70. XX w. Wyrazem tego były osobiste rozmowy i refleksje wyrażane po powrocie do NRD. Zob. P. Zariczny, *PRL i NRD – czy tylko związki wymuszone politycznie?*, w: *Po obu stronach Odry. Polska, Niemcy i ich wzajemne relacje w XX i XXI wieku – wybrane problemy*, K. Kącka (red.), Toruń 2011, s. 85. Choć, jak konkretyzował w innej pracy ten sam autor, w NRD „(…) ludzie obdarzali władzę dużym zaufaniem". Porównując realia funkcjonowania opozycji w obydwu krajach, argumentował, że opozycyjni intelektualiści w NRD „trzymali się dłużej socjalizmu". Zob. P. Zariczny, *Opozycja w NRD i w PRL – wzajemne relacje i oceny*, Gdańsk 2013, s. 19–20.

że „polska kontrrewolucja" stanowi wręcz śmiertelne zagrożenie istnienia tworu tak sztucznego jak państwo wschodnioniemieckie[11].

W przypadku NRD teoretyczna łatwość zdobywania informacji analizowanych następnie przez Centralną Grupę Analiz i Informacji Stasi (niem. Zentrale Auswertungs und Informationsgruppe, dalej: ZAIG) była pochodną tego, że PRL miała status formalnego sprzymierzeńca, co skutkowało regularnymi spotkaniami przedstawicieli obydwu służb oraz zgodą na działanie od września 1989 r. legalnej rezydentury Stasi w Polsce[12] (o nazwie Grupa Operacyjna Warszawa)[13]. Namacalnym rezultatem jej działalności były raporty przekazywane kierownictwu Stasi[14]. Dla rzetelnej oceny sposobu funkcjonowania wspomnianej Grupy i – pośrednio - wytworzonych przez nią dokumentów niezwykle przydatne by było choćby skrótowe zaprezentowanie w tekście głównym jej historii oraz omówienie składu osobowego, a także ukazanie karier poszczególnych funkcjonariuszy Stasi. Te dane wraz z pełniejszą charakterystyką ZAIG (czas działania, zadania, miejsce w strukturze resortu spraw wewnętrznych, kierownictwo, obsada personalna) byłyby pomocne w analizie, a następnie w szerszym wykorzystaniu opublikowanych dokumentów[15]. Ten brak, zdaniem autora recenzji, jest elementem, który wpływa na recepcję całej książki[16], aczkolwiek - jak się wydaje – przynajmniej częściowo wynika on z obawy przed prawnymi skutkami niezastosowania niemieckiej ustawy o zasobie archiwalnym byłego Ministerstwa Bezpieczeństwa

---

[11] Podobnego języka do określenia ruchu społecznego „Solidarność" używali przedstawiciele Komunistycznej Partii Czechosłowacji np. podczas posiedzeń KPCz. W takim samym tonie wypowiadano się także w tamtejszych reżimowych mediach. Zob. A. Kobus, *Czechosłowacja wobec narodzin, rozwoju i delegalizacji „Solidarności"*…, s. 62, 114, 171.

[12] Warto zaznaczyć, że relacje między Stasi a SB były raczej chłodne. Dla obydwu formacji suwerenem pozostawały bowiem sowieckie służby specjalne. Zob. T. Jaskułowski, *Przyjaźń, która nie istniała. Ministerstwo Bezpieczeństwa Państwowego NRD wobec MSW 1974–1990*, „Glaukopis" 2014, nr 31, s. 231–254; T. Jaskułowski, *Wymuszona przyjaźń. Stosunki państwowe NRD–PRL*, „Mówią Wieki. Magazyn historyczny" 2016, nr 11, s. 8–11.

[13] M. Tantzscher, *Grupy operacyjne Stasi w krajach bloku wschodniego*, „Pamięć i Sprawiedliwość" 2006, nr 1, s. 43–61; F. Gańczak, *Polski nie oddamy. Władze NRD wobec wydarzeń w PRL 1980–1981*, Warszawa 2017, s. 46–53; T. Jaskułowski, *Przyjaźń, której nie było. Ministerstwo Bezpieczeństwa Państwowego NRD wobec MSW 1974–1990,* Warszawa 2014, s. 362–391. Pochodną spraw poruszanych w tekście głównym jest zagadnienie dotyczące liczebności i jakości agentury Stasi w Polsce. Zob. F. Gańczak, *Agentura Stasi w PRL w czasach pierwszej „Solidarności". Wstęp do dyskusji*, „Pamięć i Sprawiedliwość" 2017, nr 2, s. 451–465; T. Jaskułowski, *Przyjaźń, której nie było*…, s. 391–419.

[14] T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981-1989.* Tom 1: *W przededniu*…, s. 15–16.

[15] Funkcjonowanie Stasi, jak również częściowo skład osobowy, zostały zarysowane w książce: H. Schwan, *Erich Mielke. Żywot w służbie Stasi*, Warszawa 2001 (s. 107-110). Autor, prezentując karierę szefa Stasi, stwierdza, że bez zgody E. Mielkego z ZAIG nie mogła się wydostać żadna informacja.

[16] Tym bardziej, że rolę tej jednostki pokrótce charakteryzuje - na podstawie prac innych historyków - Filip Gańczak, który przypisuje jej miano „mózgu" Ministerstwa Bezpieczeństwa Państwowego. Zob. F. Gańczak, *Polski nie oddamy*…, s. 45.

Państwowego NRD (niem. Ministerium für Staatssicherheit, MfS)[17] w kwestii ujawniania danych osobowych.

Recenzowana publikacja stanowi pierwszy widoczny rezultat realizacji projektu badawczego „Polskie raporty Stasi 1981–1989", który jest odpowiedzią na postulat wielokrotnie podnoszony przez historyków zajmujących się komunistycznymi służbami specjalnymi poszczególnych państw Europy Środkowo-Wschodniej, aby podjąć badania komparatystyczne i przygotować opracowania źródłoznawcze, ukazujące m.in. (…) *analizę zewnętrznych źródeł wywiadowczych w kontekście polityki wewnętrznej państw trzecich*[18]. Zrealizowanie tego zadania wymagało przeprowadzenia odpowiedniej kwerendy (rozpoczęto ją w 2017 r.) w archiwum urzędu Gaucka oraz podjęcia naukowej refleksji nad pracą analityczną Stasi wykonywaną na podstawie raportów oraz informacji na temat wydarzeń zachodzących w Polsce. Należy wspomnieć, że dodatkowym impulsem dla osób, które rozpoczęły kwerendę, było to, że urząd Gaucka kończy swoją działalność w czerwcu 2021 r.[19]

Z perspektywy służb specjalnych NRD na początku lat 80. XX w. najistotniejsze w odniesieniu do Polski było pozyskiwanie informacji pozwalających na prawidłową ocenę, a następnie przewidzenie zakresu i charakteru zmian zachodzących w naszym kraju. Dla historyków, którzy przystąpili do krytycznego opracowania źródeł pozostałych po Stasi, najważniejsze okazały się m.in. odpowiedzi na pytania: 1) jaki obraz zmian zachodzących w PRL przekazywały jednostki analityczne Stasi i w jaki sposób ten obraz wpływał na relacje między PRL i NRD?; 2) jak postrzegano sytuację wewnętrzną w Polskiej Zjednoczonej Partii Robotniczej (dalej: PZPR) i w „Solidarności", a także w innych środowiskach opozycyjnych?; 3) które aspekty życia polityczno-społecznego PRL były traktowane priorytetowo?; 4) jakie informacje uznawano za istotne, a jakim nadawano mniejszą wagę?[20] Tym pytaniom towarzyszyły postulaty pochodzące m.in. z obszaru nauk o bezpieczeństwie. Sztandarowa pozostaje próba

---

[17] Podobne rozwiązanie zastosowano w książce: T. Jaskułowski, *Przyjaźń, której nie było*…, s. 14-15.

[18] T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 198-1989.* Tom 1: *W przededniu*…, s. 12.

[19] Pełnomocnik Federalny do spraw Materiałów Państwowej Służby Bezpieczeństwa NRD, tzw. Urząd lub Instytut Gaucka (niem. Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik, BStU), został powołany do życia w roku 1990 w wyniku tzw. rewolucji pokojowej (niem. *Friedliche Revolution*) i spontanicznego działania społeczeństwa, które nie dopuściło do zniszczenia archiwów służb bezpieczeństwa byłej NRD. Samodzielna działalność tego urzędu wygasa w czerwcu 2021 r. Po tym terminie zasoby archiwalne BStU nadal będą dostępne, ale będą stanowić integralną część Archiwum Federalnego (niem. Bundesarchiv). Szerzej zob. J. Gauck, *Wystąpienie otwierające konferencję,* w: *Od totalitaryzmu do demokracji. Pomiędzy „grubą kreską" a dekomunizacją – doświadczenie Polski i Niemiec*, P. Kuglarz (red.), Kraków 2001, s. 12–29; K.W. Fricke, *Spuścizna tajnych służb i ich rola w czasach transformacji – przedstawione na przykładzie byłego Ministerstwa Bezpieczeństwa Publicznego (MfS),* w: *Od totalitaryzmu do demokracji*…, s. 333–348.

[20] T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981-1989.* Tom 1: *W przededniu*…, s. 18.

„oceny proporcji błędów do trafnych tez" w analizach przedstawianych decydentom politycznym[21].

Niewątpliwie nowatorskim posunięciem zastosowanym w przygotowaniu omawianej publikacji jest oddanie przetłumaczonych już dokumentów do oceny przez Centrum Rafinacji Informacji, w którym przeprowadzono analizę ilościową słów kluczowych, nazw i pojęć, które w nich występują

Publikacja składa się z kilku części. Funkcję wprowadzenia w tematykę książki pełnią trzy artykuły. Dwa z nich są autorstwa Tytusa Jaskułowskiego. Pierwszy prezentuje historię powstania polskich raportów Stasi oraz główne założenia projektu, w ramach którego zostały one opublikowane. Drugi przedstawia obraz PRL zawarty w raportach tygodniowych Stasi z drugiej połowy 1981 r.

Kolejnym elementem części wstępnej jest 14 diagramów (sporządzonych również przez Jaskułowskiego), pomocnych przy analizie meldunków (zarówno ich strony formalnej, jak i merytorycznej). Tę część zamyka tekst Filipa Gańczaka, który ukazuje krajobraz polityczny Polski w okresie poprzedzającym wprowadzenie stanu wojennego. Zreferowano w nim m.in. stanowisko wschodnioniemieckich notabli wobec najważniejszych wydarzeń politycznych tego okresu i ich wiedzę na ten temat.

Tytus Jaskułowski w drugim z artykułów stanowiących część wstępną scharakteryzował metodę tygodniowego raportowania, omówił objętość tego rodzaju raportów, ich strukturę formalną, proporcje przekazywanych informacji, nasycenie faktami i podejście do źródeł, a zwłaszcza stosunek do informacji niejawnych. Dość dużo uwagi poświęcił też językowi używanemu przez funkcjonariuszy Stasi, który wzmagał przekaz o permanentnej walce o władzę toczonej przez „kontrrewolucję", czyli „Solidarność", i PZPR. Efektem tego zabiegu było też uwypuklenie niezwykle krytycznego stosunku Stasi do partii komunistycznej dzierżącej władzę w Polsce, która to w obliczu powstania „Solidarności" była strofowana za nieprzeciwstawianie się jej i hołdowanie taktyce kapitulanckiej. Z uwzględnieniem tej właśnie perspektywy w raportach Stasi były omawiane także przywództwo i wszelkie inne sprawy personalne wewnątrz PZPR. W dokumentach wytworzonych przez tę służbę mniej miejsca poświęcono Kościołowi katolickiemu, który jednak zakwalifikowano jako „cynicznego" zwolennika „Solidarności". Według Jaskułowskiego, odwołującego się do wzorców anglosaskich, dyskusyjne pozostaje stwierdzenie, że raporty Stasi umożliwiały przewidywanie i zapobieganie (…) *negatywnym skutkom tzw. niespodzianki strategicznej dla własnego państwa*[22]. Ten historyk i zarazem politolog krytycznie odnosi się także do poziomu informacji dostarczanych przez Stasi i sposobu ich przekazywania, w którego przypadku nadmierne wyszczególnianie pewnych faktów było pozbawione głębszej analizy. Wymieniając też inne argumenty, uzasadnia, że obraz PRL przedstawiony w tych informacjach jest pełen stereotypów.

---

[21] Tamże, s. 20–21.

[22] Tamże, s. 45.

Zdaniem autora recenzji zestawianie działań i wysiłku analitycznego Stasi z praktyką dotyczącą tego zagadnienia w codziennej pracy służb specjalnych krajów anglosaskich jest niepotrzebne i zarazem mylące, gdyż zostało poczynione w oderwaniu od pierwotnego sposobu działania tej służby, wykształconego na podstawie wzorców sowieckich[23]. Priorytety Stasi były prostym następstwem założenia, że jej najważniejszym zadaniem pozostawało wykonywanie obowiązków policji politycznej chroniącej totalitarną władzę partii komunistycznej. Dlatego w kręgach Stasi praca operacyjna – prowadzona w znacznym stopniu przeciwko obywatelom NRD i krępująca ich dążenia do wolności - przez dziesięciolecia była uważana za najważniejszy rodzaj działań, w odróżnieniu od działań informacyjno-analitycznych. Funkcjonowanie Stasi „w gorsecie ideologicznym" wpływało na przebieg procesu wywiadowczego i jednocześnie na tzw. gotowy produkt informacyjny (uwzględniający rzetelność i trafność informacji) dostarczany kierownictwu politycznemu. Model analityczny (zawierający także prognozy i skutki) był bliższy sposobowi działania służb specjalnych krajów ówczesnego NATO. W ich obrębie bowiem służby specjalne w sposób wykluczający zagadnienia i uprzedzenia ideologiczne wpływają na decyzje tamtejszych sfer rządowych[24]. Taki sposób działania jest też pochodną kazusu, w którego przypadku właściwa selekcja i ocena zdobytego materiału informacyjnego wymagają wykorzystania specjalistycznego przygotowania i odpowiedniej wiedzy. Dlatego też anglosaskie służby specjalne – choć nie tylko one - coraz powszechniej traktują analizę informacji jako osobną specjalizację[25], a ich najlepszymi analitykami niejednokrotnie bywali cywilni naukowcy[26].

Zarówno w przypadku służb specjalnych NRD, jak i PRL najważniejszym zadaniem było zwalczanie przeciwników politycznych władzy sprawowanej przez partie komunistyczne w poszczególnych krajach. Ten imperatyw obowiązywał wszystkie służby specjalne krajów zależnych od ZSRS[27]. Jednym z fundamentalnych pytań jest to, dla kogo docelowo były przygotowywane wspomniane raporty. Wiadomo, że ich

---

[23] Jak pisze Zbigniew Siemiątkowski, w Związku Sowieckim „(…) prestiż służby informacyjno-analitycznej był niski i pozostawał w tyle za zachodnimi standardami". Autor przytoczył też opinię, że „(…) pion informacyjny Zarządu Głównego (Pierwszego) Wywiadowczego KGB znaczył tyle, ile 1/10 analiz CIA". Omawiając tę kwestię, podkreślił, że taki stan był charakterystyczny dla wywiadów państw totalitarnych. Zob. Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej w PRL*, Warszawa 2009, s. 34. Tę konstatację zawarto także w recenzowanej publikacji, wskazując na „(…) problem prymatu pracy operacyjnej nad analityczną w resortach bezpieczeństwa państw Układu Warszawskiego". Zob. T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981-1989.* Tom 1: *W przededniu*…, s. 26.

[24] Na ten temat zob. szerzej m.in.: S. Galij-Skarbińska, *Model zmiany cywilnych służb specjalnych w Polsce w latach 1989–1990. Powstanie Urzędu Ochrony Państwa*, Toruń 2019, s. 57-80.

[25] Zob. H. Batorowska, *Analityk w środowisku walki o dominację i przetrwanie*, w: *Walka informacyjna. Uwarunkowania, incydenty, wyzwania*, H. Batorowska (red.), Kraków 2017, s. 181–197.

[26] J. Keegan, *Wywiad w czasie wojny*, Warszawa 2003, s. 292.

[27] Zob. R. Terlecki, *Miecz i tarcza komunizmu. Historia aparatu bezpieczeństwa w Polsce 1944–1990*, Kraków 2007; J. Gieseke, *Stasi. Historia 1945–1990,* Kraków 2010.

odbiorcą zasadniczo było kierownictwo Stasi. Ale czy tylko ono? Można snuć różne supozycje.

Wiadomo też, że w jakiejś mierze raporty powstawały z wykorzystaniem źródeł ogólnodostępnych i – co istotne – jawnych: prasy oficjalnej, prasy podziemnej wydawanej przez „Solidarność", informacji urzędowych publikowanych i prezentowanych w różnych zestawieniach oraz raportach, a także informacji pochodzących z rozmów z przedstawicielami władzy. Wiadomości pozyskiwane z takich właśnie źródeł są powszechnie wykorzystywane w pracy wywiadowczej.

Wspomniana rezydentura Stasi w Warszawie w postaci Grupy Operacyjnej Warszawa, choć formalnie miała prowadzić działania o charakterze kontrwywiadowczym, nie mogła uchylać się od działalności wywiadowczej (na przykład tzw. kontrwywiadu ofensywnego czy zaczepnego)[28]. Istotnego znaczenia nabiera zatem odpowiedź na pytanie, czy ze względu na takie, a nie inne grono odbiorców raporty, o których mowa, miały taki, a nie inny charakter. Jak słusznie podkreślił we wstępie Tytus Jaskułowski, przeważają w nich informacje poddane analizie w sposób dość oszczędny. Niezwykle rzadko pojawia się w nich sformułowanie, że dana informacja została zdobyta w sposób „nieoficjalny". Takich zapisów - jak odnotowano w publikacji - jest tylko 27. Ich nieprecyzyjność wydaje się celowa, ale czy na pewno świadczy ona o „skromnym zakresie pracy operacyjnej Stasi w PRL"[29].

Grupa Operacyjna Warszawa podlegała – tak jak inne grupy operacyjne Stasi – Wydziałowi Głównemu II MfS NRD, czyli kontrwywiadowi. Tym samym rodzi się pytanie, czy przekazywane przez nią raporty (meldunki) nie były „filtrowane" przed przesyłaniem ich dalej. Z dużym prawdopodobieństwem można uznać, że tak właśnie było. Przecież podobny charakter miały informacje przekazywane działaczom partyjnym m.in. przez rodzimą Służbę Bezpieczeństwa PRL[30] (niejednokrotnie miały one formę tzw. informacji zbiorczej). W takim razie otwarte pozostają pytania: 1) czy funkcjonariusze Stasi, sporządzając dla swojego kierownictwa raporty dotyczące wydarzeń w Polsce, nie potrafili ich odpowiednio zanalizować? 2) czy kierując się oportunizmem i wyczuwając nastawienie (oczekiwania) swoich mocodawców, ograniczali się do przekazywania wiadomości o różnym znaczeniu, bez podejmowania próby ich weryfikacji

---

[28] Zob. T. Jaskułowski, *Przyjaźń, której nie było*…, s. 10–13. W rozmowie prezentującej publikację na stronie internetowej histmag Filip Gańczak podał też kilka przykładów działań o charakterze wywiadowczym, podjętych przez Stasi na terytorium Polski. P. Czechowski, *Stasi – jak wschodnioniemiecka służba bezpieczeństwa śledziła sytuację w PRL (cz.2.)*, https://old.histmag.org/Stasi-jak-wschodnioniemiecka-sluzba-bezpieczenstwa-sledzila-sytuacje-w-PRL-21126/2 [dostęp: 29 XII 2020]

[29] T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981-1989.* Tom 1: *W przededniu*…, s. 29.

[30] Analiza jest jednym z instrumentów pracy wywiadu. Wymogiem gwarantującym brak zakłóceń w tego rodzaju pracy jest „odizolowanie" od siebie wszystkich odcinków działań, jak również osób je wykonujących. Standardem jest, że informacja wywiadowcza podlega szczególnej ochronie nawet przed analitykami wywiadu. Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy*…, s. 33.

i systematyzacji? Jeśli przyjmiemy za uprawnioną jedynie tę drugą możliwość, to rzeczywiście tym raportom można przypisać zarówno funkcję mobilizującą, jak i – choć zdaniem autora recenzji w mniejszym zakresie - mitotwórczą[31]. Prezentując z kolei tę kwestię, można pokusić się o wysunięcie kolejnej hipotezy. Mianowicie służby specjalne działające w systemie demokratycznym i poddawane odpowiedniej kontroli w mniejszym stopniu są podatne na pokusę spełnienia funkcji przedstawionej powyżej niż służby ulokowane w systemie władzy totalitarnej[32].

Można też – również hipotetycznie - zastanawiać się, czy istniały inne źródła wiedzy o Polsce dostępne Stasi i kierownictwu NRD. Takim dodatkowym źródłem w odniesieniu do sytuacji w Polsce mógł być Komitet Bezpieczeństwa Państwowego przy Radzie Ministrów ZSRR – KBP ZSRR (ros. Комитéт государственной безопáсности СССР – КГБ СССР, pis. fon. Komitiet gosudarstwiennoj biezopasnosti pri Sowietie Ministrow SSSR), współpracujący ze Stasi, jak również Główny Zarząd Wywiadu[33] (którego funkcjonariusze zazwyczaj nie wchodzili w skład grup operacyjnych Stasi) i ewentualnie wywiad wojskowy NRD. Czy więc odpowiedź na pytanie, dlaczego publikowanych raportów nie otrzymywał szef wywiadu Stasi, Markus Wolf, może brzmieć tylko spekulatywnie. Czyżby dysponował on innymi danymi na temat wydarzeń w Polsce?

Clou publikacji stanowią zamieszczone w niej dokumenty (łącznie 27), sporządzone między 15 czerwca a 14 grudnia 1981 r. Język, jakim posługują się w nich funkcjonariusze Stasi, jest mocno zideologizowany, pełen uproszczeń i schematycznych klasyfikacji. Wskazuje jednocześnie na dezaprobatę dla obozu „kontrrewolucji".

Dokumenty zostały opatrzone wyczerpującymi przypisami rzeczowymi, które wraz ze słowniczkiem biograficznym zawartym na końcu opracowania stanowią wystarczającą pomoc w odbiorze publikacji.

W raportach wiele uwagi poświęcono zmianom zachodzącym wewnątrz PZPR, której „kondycję" bacznie obserwowano w obliczu konieczności zdławienia przez nią

---

[31] T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981–1989.* Tom 1: *W przededniu…*, s. 29.

[32] Sztandarowym przykładem jest zlekceważenie informacji przekazywanych przez wywiad Hitlerowi czy Stalinowi. Zob. J. Hughes-Wilson, *Największe błędy wywiadów świata*, Warszawa 2002, s. 19, 37–50. Gwoli ścisłości, autor wspomnianej rozprawy na jej kartach dokumentuje też błędy popełniane przez agencje wywiadowcze oraz instytucje krajów o demokratycznym systemie rządów.

[33] Postawienie tej hipotezy badawczej usprawiedliwia informacje, że 90% archiwaliów wytworzonych przez wywiad Stasi zostało zniszczonych. Trzeba jednak dodać, że głównym terenem działania wywiadu Stasi była Republika Federalna Niemiec oraz państwa NATO i Wspólnoty Europejskiej. Zob. K. Emmo, *Sieci wywiadowcze w świetle analizy sieciowej. Przypadek wywiadu wschodnioniemieckiego w Skandynawii*, „Pamięć i Sprawiedliwość" 2014, nr 1, s. 23. Z kolei Helmut Müller-Enbergs wskazywał, że Stasi nie była „niezależną agencją wywiadowczą", lecz „tworem KGB". Zob. H. Müller-Enbergs, *Jak to było naprawdę z sukcesami wywiadu Stasi na Zachodzie?*, „Pamięć i Sprawiedliwość" 2014, nr 1, s. 48. Filip Gańczak co najmniej dwukrotnie cytował w swoim tekście meldunki wywiadu wojskowego NRD dotyczące „Solidarności". Zob. T. Jaskułowski, F. Gańczak, K. Knoch, P. Abryszeński, E. Pejaś, *Raporty polskie Stasi 1981–1989.* Tom 1: *W przededniu…*, s. 67 (przyp. 52 i 53).

ruchu społecznego „Solidarność". Można wręcz wywnioskować, że w raportach zamieszczono więcej wartościowych danych na temat partii niż na temat „Solidarności". Zawarto w nich informacje o niektórych posiedzeniach Sejmu PRL, strukturach „poziomych" w szeregach PZPR, sytuacji w prokuraturze, koncepcji utworzenia Frontu Porozumienia Narodowego, problemach ekonomicznych czy materiały w formie załączników (np. przegląd komisji problemowych Komitetu Centralnego Polskiej Zjednoczonej Partii Robotniczej, podział obowiązków w Sekretariacie KC PZPR).

Reasumując, wymienione powyżej – raczej drobne, lekko polemiczne uwagi przedstawione w formie hipotetycznej – mogą skłonić autorów opracowujących kolejne tomy źródeł do mocniejszego osadzenia tych publikacji w realiach funkcjonowania Stasi, nawet kosztem ewentualnych zarzutów o powtarzanie treści już znanych i opisanych przez innych badaczy. Recenzowane opracowanie stanowi cenne źródło wiedzy, które może być pomocne m.in. badaczom historii, ekspertom w dziedzinie nauk politycznych, stosunków międzynarodowych i nauk o bezpieczeństwie w przybliżeniu działalności Stasi oraz jej relacji ze Służbą Bezpieczeństwa PRL, pozostającą w strukturze Ministerstwa Spraw Wewnętrznych PRL. Patrząc z szerszej perspektywy, ukazuje ono również charakter i częstotliwość oficjalnych relacji elit partyjno-państwowych PRL i NRD. Publikacja zaspokaja także potrzebę przeprowadzenia badań komparatystycznych leżącą u podstaw jej powstania. W przypadku kontynuowania podobnych prac może się stać punktem odniesienia dla innych projektów badawczych dotyczących opracowywania źródeł służb specjalnych państw komunistycznych pozostających w kręgu wpływów ZSRS.

IV

PRZEGLĄD PRAC KONKURSOWYCH

OVERVIEW OF THE WORKS

NORBERT NOWICKI
ORCID: 0000-0002-4068-7578

DOI: 10.4467/20801335PBW.21.016.13573

Normatywne ujęcie czynności operacyjno-rozpoznawczych w aspekcie dowodu nielegalnego[1]

Definicja czynności operacyjno-rozpoznawczych

Pojęcie czynności operacyjno-rozpoznawcze nie zostało zdefiniowane wprost w żadnym akcie prawnym. Pierwsza definicja legalna tej instytucji prawnej pojawiła się w poselskim projekcie ustawy o czynnościach operacyjno-rozpoznawczych z 7 lutego 2008 r. (druk sejmowy nr 353). Brzmiała następująco:

> (…) czynności operacyjno-rozpoznawcze są zespołem przedsięwzięć, jawnych i niejawnych[,] prowadzonych wyłącznie w celu rozpoznania, zapobiegania i wykrywania przestępstw; odnajdywania osób ukrywających się przed organami ścigania lub wymiarem sprawiedliwości oraz osób zaginionych, jeżeli zachodzi uzasadnione podejrzenie, że ich zaginięcie jest wynikiem przestępstwa, a także odnajdywania rzeczy utraconych w wyniku przestępstwa lub mających związek z przestępstwem, ustalenia tożsamości osób i zwłok, w przypadku uzasadnionego podejrzenia przestępczego działania.

Prace nad tym aktem prawnym zostały wstrzymane. W związku z tym, aby zdefiniować wskazane pojęcie, należy odwołać się do dorobku doktryny. Przede wszystkim warto podkreślić, że pojęcie „czynności operacyjno-rozpoznawcze" może być zamiennie używane z takimi pojęciami, jak: praca operacyjna, działania operacyjne, czynności operacyjne[2]. W literaturze przedmiotu jest kilka definicji czynności

---

[1] Fragment pracy magisterskiej pt. *Prawne granice panoptycznych metod panowania politycznego* (Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii). Autor wykorzystał rozdziały 4 i 5.

[2] Z. Niemczyk, *Czynności operacyjno-rozpoznawcze i możliwość wykorzystania ich rezultatów w postępowaniu karnym*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2013, nr 3, s. 5–6.

operacyjno-rozpoznawczych. Tadeusz Hanausek kwalifikuje je jako (…) *odrębny system poufnych lub tajnych działań organów policyjnych, które prowadzone są poza procesem karnym. Czynności te służą aktualnym lub przyszłym celom tego procesu*[3]. Z kolei Janusz Gołębiewski uważa, że są to (…) *działania, z jednej strony, zmierzające do realizacji określonego zadania, a z drugiej strony do zbierania interesujących informacji*[4]. W *Leksykonie policyjnym* omawiane pojęcie zostało zdefiniowane jako (…) *ogół działań podejmowanych przez wyspecjalizowanych policjantów służby kryminalnej z wykorzystaniem określonych w ustawie o Policji oraz w przepisach wydanych na jej podstawie form, metod i środków pracy operacyjnej*[5]. Celem ich stosowania jest rozpoznawanie i wykrywanie przestępstw oraz zapobieganie im, jak również ściganie ich sprawców.

Podstawą prawną do prowadzenia działalności operacyjnej są przepisy zawarte w ustawach policyjnych i aktach wykonawczych. Należy podkreślić, że czynności operacyjno-rozpoznawcze są czynnościami pozaprocesowymi. W praktyce oznacza to, że nie mają do nich zastosowania przepisy *Ustawy z dnia 6 czerwca 1997 r – Kodeks postępowania karnego*[6] (dalej: kpk), a podmiotami legitymowanymi do zarządzenia i przeprowadzenia takiej kontroli są wyłącznie organy państwowe wymienione w konkretnej ustawie regulującej kwestie dotyczące działań operacyjnych. Aktywność służb policyjnych w tym zakresie ma charakter autonomiczny w stosunku do podejmowanych czynności procesowych[7]. Mimo że działania operacyjne są realizowane poza postępowaniem karnym, nie wyklucza to wykorzystania materiałów operacyjnych w przyszłości[8]. Chodzi o to, że wyniki czynności operacyjno-rozpoznawczych nie mają bezpośredniego znaczenia dowodowego, w związku z tym nie mogą być wprowadzone wprost do postępowania dowodowego. Mają służyć konkretnemu, obecnemu lub przyszłemu postępowaniu karnemu wszczynanemu na podstawie zebranego materiału operacyjnego. Ponadto mogą być pomocne przy rozpracowywaniu określonych środowisk kryminogennych, nie muszą zatem być związane wyłącznie z konkretnym procesem[9].

Czynnościom operacyjno-rozpoznawczym przypisuje się następujące funkcje: rozpoznawczą, wykrywczą, dowodową oraz zapobiegawczą. Celem pierwszej z nich jest rozpoznawanie środowisk kryminogennych i przestępczych oraz czynników wpływających na te zbiorowości. Funkcja wykrywcza polega na wykrywaniu czynów zabronionych i ich sprawców, a dowodowa – na udowodnieniu winy i innych określonych

---

[3] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1996, s. 96.

[4] J. Gołębiewski, *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*, Warszawa 2008, s. 19.

[5] W. Pływaczewski, G. Kędzierska, *Leksykon policyjny*, Szczytno 2001, s. 56.

[6] Tekst jednolity: DzU z 2021 r. poz. 534.

[7] R. Teluk, *Inwigilacja i infiltracja jako efektywne metody uzyskiwania informacji operacyjnych na temat środowiska przestępczego lub kryminogennego*, „Zeszyty Prawnicze" 2014, nr 4, s. 179.

[8] Z. Niemczyk, *Czynności operacyjno-rozpoznawcze*…, s. 6.

[9] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, http://m.wspia.eu/file/21440/44-WÓJCIK.pdf [dostęp: 10 XII 2020].

ustawowo znamion popełnionego przestępstwa. Rolą funkcji zapobiegawczej jest zapobieganie określonym zagrożeniom, ewentualnie ich eliminowanie[10].

Kontrola operacyjna

Kontrola operacyjna jest jedną z ustawowych metod czynności operacyjno-rozpoznawczych. Jej istota została ujęta w art. 19 *Ustawy z dnia 6 kwietnia 1990 r. o Policji*[11]. Jest to czynność niejawna polegająca 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 w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
5) uzyskiwaniu dostępu i kontroli zawartości przesyłek[12].

Kontrola operacyjna jest zarządzana (…) *w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw*[13] wymienionych we wspomnianym artykule. Zarządzenie kontroli operacyjnej jest więc możliwe wyłącznie w przypadku ściśle określonych przestępstw, enumeratywnie wskazanych w art. 19 ustawy o Policji. Sąd Apelacyjny w Warszawie w wyroku o sygnaturze AKa 133/16 odniósł się do korzystania z materiałów uzyskanych w wyniku kontroli operacyjnej w sprawie o przestępstwa, które nie zostały wymienione w ust. 1 wskazanego artykułu. Orzekł, że jest to niedopuszczalne. Z uwagi na szczególny charakter omawianej regulacji przepisy nie mogą być bowiem interpretowane rozszerzająco[14].

Oprócz tego we wniosku o zarządzenie kontroli operacyjnej należy wskazać, że środki służące do zapobieżenia przestępstwom oraz wykrycia czynów zabronionych i ich sprawców okazały się bezskuteczne albo będą nieprzydatne dla dalszego toku procesu (tzw. klauzula subsydiarności)[15]. *Oznacza to kategoryczny zakaz stosowania kontroli*

---

[10] Z. Niemczyk, *Czynności operacyjno-rozpoznawcze*…, s. 6.

[11] Tekst jednolity: DzU z 2020 r. poz. 360, ze zm.

[12] K. Ożóg-Wróbel, *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, nr 4, s. 131–133.

[13] Art. 19 ust. 1 ustawy o Policji.

[14] Wyrok Sądu Apelacyjnego (dalej: SA) w Warszawie z 13 VI 2016 r., sygn. AKa 133/16, Lex nr 2171252.

[15] K. Ożóg-Wróbel, *Katalog metod*…, s. 131–132.

operacyjnej, jeżeli nie wyczerpano innych możliwych metod pracy operacyjnej albo też nie wykazano, że inne środki (biorąc pod uwagę konkretny stan faktyczny) będą nieprzydatne[16].

W polskim porządku prawnym wyróżnia się dwa rodzaje podsłuchów: procesowy i pozaprocesowy (operacyjny). Uregulowania dotyczące podsłuchu procesowego są zawarte w rozdziale 26 kpk. Zgodnie z nimi po wszczęciu postępowania sąd na wniosek prokuratora może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych[17]. Z kolei w art. 19 ust. 5 ustawy o Policji wprost wskazuje się, że podsłuch operacyjny może zostać zastosowany zarówno przed wszczęciem postępowania, jak i już po jego rozpoczęciu, gdyż zakres podmiotowy zarządzonej kontroli dotyczy osoby podejrzanej lub oskarżonego. W doktrynie istnieje spór na temat prowadzenia podsłuchu procesowego na etapie postępowania przygotowawczego. Przeciwnicy zarządzania kontroli operacyjnej po wszczęciu postępowania zauważają, że prowadzi to do konkurencji między czynnościami operacyjnymi i procesowymi. Innym argumentem krytycznym podnoszonym wobec rozwiązania prawnego z art. 19 ust. 5 ustawy o Policji jest obawa, że działania funkcjonariuszy będą realizowane bez wiedzy prokuratora, czyli gospodarza postępowania przygotowawczego. Może to prowadzić do ingerencji policji w materiał dowodowy zebrany przez prokuratora oraz do niespójności w procesie. W literaturze przedmiotu istnieje również odmienne stanowisko. Część autorów, np. Stanisław Hoc, Romuald Kmiecik, Katarzyna Dudka, nie widzi żadnych przeciwskazań do prowadzenia podsłuchu operacyjnego w trakcie trwania postępowania przygotowawczego. Przepisy prawne regulujące tę materię nie wykluczają jednoczesnego korzystania z podsłuchu operacyjnego i procesowego. Równoczesne ich stosowanie skutkuje większą skutecznością w wykrywaniu przestępstw[18].

Zakup kontrolowany. Tak zwana kontrolowana łapówka

Zakup kontrolowany i tzw. kontrolowana łapówka to kolejne metody działań operacyjnych. Reguluje je art. 19a ustawy o Policji. Zgodnie z nim zakup kontrolowany jest związany z (…) *dokonaniem w sposób niejawny nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi, albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione*[19]. Oprócz tego może polegać również na (…) *złożeniu propozycji nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi, albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione*[20]. W analogiczny sposób ustawodawca

---

[16] A. Łyżwa, M. Tokarski, *Art. 19 ustawy o Policji*, w: *Ustawa o Policji. Komentarz*, Ł. Czebotar i in. (red.), Warszawa 2015.

[17] Art. 237 § 1 kpk.

[18] P. Kosmaty, *Podsłuch pozaprocesowy (operacyjny). Czy można stosować podsłuch bez zgody sądu?*, „Prokurator" 2008, nr 2–3, s. 94–95.

[19] Art. 19a ust. 1 ustawy o Policji.

[20] Art. 19a ust. 2 ustawy o Policji.

scharakteryzował tzw. kontrolowaną łapówkę – jako przyjęcie lub wręczenie korzyści majątkowej albo złożenie propozycji przyjęcia lub wręczenia korzyści majątkowej[21].

Celem opisanych wyżej czynności operacyjno-rozpoznawczych jest sprawdzenie uzyskanych wcześniej wiarygodnych informacji o przestępstwie oraz ustalenie sprawców i uzyskanie dowodów przestępstwa[22]. Rozpoczęcie pracy operacyjnej, o której mowa w art. 19a ust. 1 i 2 ustawy o Policji, jest możliwe wyłącznie po uprzednim uzyskaniu wiarygodnych informacji o czynie zabronionym. Zebrane materiały operacyjne mają posłużyć ujawnieniu nie tylko pojedynczego przestępstwa, lecz przede wszystkim całego przestępczego procederu, czyli całokształtu działalności przestępczej sprawcy[23].

Zakres przedmiotowy zakupu kontrolowanego i tzw. kontrolowanej łapówki jest taki sam jak w przypadku zarządzenia kontroli operacyjnej. To oznacza, że organy Policji mogą prowadzić pracę operacyjną jedynie w przypadku przestępstw enumeratywnie wymienionych w art. 19 ust. 1 ustawy o Policji.

Z omawianej metody operacyjnej korzysta funkcjonariusz Policji działający pod przykryciem, aby ukryć swoją przynależność służbową, tożsamość oraz intencje. Posługuje się przy tym fałszywymi danymi oraz dokumentami. Zakup kontrolowany i tzw. kontrolowana łapówka są realizowane po uprzednim przeprowadzeniu innych czynności operacyjno-rozpoznawczych, zwłaszcza kontroli operacyjnej. Celem jest sprawdzenie i potwierdzenie wcześniejszych przypuszczeń oraz ustaleń, a także uzyskanie niezbędnych dowodów dla postępowania karnego[24].

Stosowanie technik prowokacyjnych skutkuje zdobyciem mocnych dowodów popełnienia przestępstwa, zatem art. 19a ust. 6 ustawy o Policji przewiduje, że takie czynności mogą być niejawnie rejestrowane za pomocą urządzeń służących do nagrywania obrazu lub dźwięku. Z analizy wskazanej normy wynika, że nagrywanie obrazu i dźwięku nie podlega rygorowi określonemu w art. 19, w związku z tym decyzję o prowadzeniu kontroli operacyjnej w toku realizacji zakupu kontrolowanego lub tzw. kontrolowanej łapówki może podjąć organ zarządzający omawiane czynności operacyjno-rozpoznawcze[25].

W doktrynie zwraca się uwagę, że w ustawie o Policji nie określono relacji między kontrolą operacyjną a tzw. kontrolowaną łapówką. Zgodnie z wykładnią celowościową obie metody należy stosować niezależnie od siebie, a nawet zamiennie. To oznacza, że w przypadku gdy zastosowanie kontroli operacyjnej, np. w postaci podsłuchu, okaże się bezskuteczne, można skorzystać z metod określonych w art. 19a ustawy o Policji

---

[21] Tamże.

[22] K. Ożóg-Wróbel, *Katalog metod*…, s. 135–136.

[23] M. Klejnowska, *Podsłuch operacyjny i prowokacja policyjna*, „Prokuratura i Prawo" 2004, nr 3, teza 5 Lex, https://sip.lex.pl/#/publication/151037556/klejnowska-monika-podsluch-operacyjny-i-prowokacja-policyjna?keyword=Pods%C5%82uch%20operacyjny%20i%20prowokacja%20policyjna&cm=SREST [dostęp: 10 XII 2020].

[24] K. Ożóg-Wróbel, *Katalog metod*…, s. 135–136.

[25] M. Kołodziejczak, A. Sobiech, *Prawnie dopuszczalne postacie prowokacji*, „Państwo i Prawo" 2010, nr 11, s. 40.

i odwrotnie. Oprócz tego wskazana metoda może zostać wykorzystana w celu sprawdzenia wiarygodności informacji uzyskanych w ramach podsłuchu operacyjnego[26].

Przechodząc do warunków, które muszą zostać spełnione, aby przeprowadzenie prowokacji stało się legalne, należy odnieść się do sposobu działania funkcjonariuszy wobec konkretnego sprawcy. Po pierwsze, propozycja złożona w ramach zarówno zakupu kontrolowanego, jak i tzw. kontrolowanej łapówki nie powinna być nachalna bądź połączona z groźbą bezprawną lub jakimkolwiek przymusem fizycznym lub psychicznym[27]. Po drugie, funkcjonariusze realizujący działania operacyjne nie mogą nakłaniać do popełnienia przestępstwa, organizowania albo kierowania działaniami przestępczymi[28]. Naruszenie tych zasad może spowodować odpowiedzialność karną funkcjonariuszy na podstawie art. 24 *Kodeksu karnego*[29] (dalej: kk) oraz będzie skutkować wypełnieniem znamion nielegalnej prowokacji[30]. Oprócz tego zwraca się uwagę, że opisywane metody pracy operacyjnej mogą powodować tzw. sztuczne przestępstwa, przez zachęcenie do popełnienia czynu zabronionego w wyniku stworzenia sprzyjających temu okoliczności[31].

Przesyłka niejawnie nadzorowana

Ten rodzaj postępowania został uregulowany w art. 19b ustawy o Policji. Obejmuje ono niejawne nadzorowanie wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia życia lub zdrowia ludzkiego, w celu udokumentowania przestępstw, o których mowa w art. 19 ust. 1, albo ustalenia tożsamości osób uczestniczących w tych przestępstwach lub też przejęcia przedmiotów. W praktyce Policja posługuje się w tych działaniach podstępem. Polega on na wykorzystaniu (…) *błędnego przeświadczenia osób wytwarzających, przemieszczających, przechowujących i dokonujących obrotu przedmiotami przestępstwa, że ich zachowanie pozostaje tajemnicą i nie znajduje się w zainteresowaniu organów ścigania*[32].

W piśmiennictwie wyodrębnia się następujące rodzaje przesyłek niejawnie nadzorowanych:

- „czyste" – przedmiot przestępstwa w całości lub części został w sposób tajny podmieniony na identyczny albo usunięty;

---

[26] M. Klejnowska, *Podsłuch operacyjny*…, teza 6 Lex.

[27] Wyrok Sądu Najwyższego (dalej: SN) z 10 X 2007 r., sygn. II KK 387/06, OSNwSK nr 1/2007, poz. 1587.

[28] R. Janiszewski-Downarowicz, G*ranice dozwolonej prowokacji w polskim prawie karnym*, „Prokuratura i Prawo" 2009, nr 3, s. 93.

[29] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

[30] M. Kołodziejczak, A. Sobiech, *Prawnie dopuszczalne*…, s. 39.

[31] Tamże, s. 43.

[32] A. Biernaczyk, *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a i 19b Ustawy z dnia 6 kwietnia 1990 roku o Policji*, w: *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, L. Paprzycki, Z. Rau (red.), Warszawa 2009, s. 138–139.

- „brudne" – nadzorowanie dotyczy przesyłek w stanie nienaruszonym;
- wewnątrzkrajowe – nadzorowanie dotyczy terytorium tylko jednego państwa;
- międzynarodowe „wewnętrzne" – informacje np. o przemycie uzyskują organy ścigania kraju docelowego, który jednocześnie podejmuje czynności koordynujące operację od kraju nadania (wysyłającego) przez kraje tranzytowe;
- międzynarodowe „zewnętrzne" – informacje o nielegalnej dostawie mają władze innych państw niż docelowe i to one uzgadniają warunki bezpiecznego przebiegu dostawy kontrolowanej do kraju docelowego[33].

Negatywną przesłanką opisanej metody pracy operacyjnej są wspomniane zagrożenia życia i zdrowia ludzkiego. Należy je rozumieć szeroko – nie tylko jako zagrożenia bezpośrednie, lecz także potencjalne. W przypadku ich zaistnienia Policja ma zakaz korzystania z tej metody operacyjno-rozpoznawczej[34]. W literaturze przedmiotu przesyłkę niejawnie nadzorowaną kwalifikuje się jako odmianę zakupu kontrolowanego, ponieważ ostatni etap realizacji tej metody operacyjnej może przyjąć formę takiego zakupu[35].

Tajny agent policji

Pojęcie tajny agent policji nie zostało zdefiniowane w ustawie o Policji. Działania takiego agenta odgrywają bardzo dużą rolę w tych metodach operacyjnych, które opierają się na prowokacji, czyli w zakupie kontrolowanym, kontrolowanej łapówce oraz przesyłce niejawnie nadzorowanej. Praca tajnego agenta polega na wejściu w środowisko przestępcze, z którym wiążą się przedsięwzięcia werbunkowe mające na celu pozyskanie informatorów. Tajnym agentem może zostać funkcjonariusz o ponadprzeciętnych predyspozycjach psychofizycznych. Musi on zostać przeszkolony w zakresie pozyskiwania informatorów i specyfiki funkcjonowania środowisk przestępczych[36].

Dowód nielegalny a dowód z czynności operacyjnych

Zagadnienia związane z problematyką dowodów nielegalnych wywołują obecnie duże kontrowersje ze względu na konstrukcję prawną zawartą w art. 168a kpk. Zgodnie z aktualnym brzemieniem tej normy dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 kk, chyba że został on uzyskany w związku

---

[33] P. Kosmaty, *Przesyłka niejawnie nadzorowana*, „Prokurator" 2010, nr 3, s. 32–33.

[34] Tamże, s. 37.

[35] R. Zakrzewski, A. Woźniak, *Nowelizacja ustawy o Policji – rozszerzenie uprawnień operacyjno-rozpoznawczych*, „Monitor Prawniczy" 1996, nr 1, s. 6.

[36] A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, s. 25, 49–50.

z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności[37].

Analizując treść art. 168a, należy zauważyć, że ustawodawca nowelizacją z 15 kwietnia 2016 r. dopuścił dowód uzyskany z naruszeniem przepisów oraz dowód uzyskany za pomocą czynu zabronionego określonego w art. 1 § 1 kk. W doktrynie podkreśla się, że wskazana norma umożliwia wykorzystanie dowodów nielegalnych, a ich niedopuszczalność ogranicza wyłącznie do bezdyskusyjnych nadużyć[38]. Za dowód nielegalny na gruncie piśmiennictwa uznaje się dowód, który: a) pochodzi z „nielegalnego źródła", tzn. został przeprowadzony mimo niedopuszczalności dowodzenia za jego pomocą, b) został pozyskany bez zachowania ustawowych warunków, c) został przeprowadzony niezgodnie z obowiązującymi przepisami karnoprocesowymi w pozostałym zakresie[39].

W literaturze przedmiotu dotyczącej dowodu nielegalnego istnieje tzw. doktryna owoców zatrutego drzewa. Zgodnie z nią dowód uzyskany za pomocą przestępstwa (dowód pierwotnie nielegalny), jak również pozostałe dowody wynikające z tego czynu zabronionego (dowód wtórnie nielegalny) są niedopuszczalne. Na gruncie polskiego ustawodawstwa ta koncepcja nie została jednak przyjęta, co potwierdza orzecznictwo[40]. W polskiej procedurze karnej można zatem dokonywać ustaleń faktycznych na podstawie dowodów uzyskanych z naruszeniem prawa. Ten pogląd podzielił Sąd Apelacyjny w Lublinie, który uznał, że (…) *kodeks postępowania karnego hołduje zasadzie swobodnej oceny dowodów, która nakłada na sąd obowiązek dokonania oceny wszystkich dowodów zgodnie z dyrektywami zawartymi w art. 7 k.p.k., także w aspekcie dyrektyw prawidłowej oceny dowodów*[41]. Również Sąd Najwyższy wypowiedział się na temat koncepcji owoców zatrutego drzewa. W postanowieniu z 14 listopada 2006 r. wywnioskował, że (…) *obowiązująca procedura karna nie wprowadza żadnego zamkniętego katalogu dowodów, uznając za takie w zasadzie wszystko, co może przyczynić się do wyjaśnienia prawdy, o ile nie jest objęte ściśle określonym zakazem dowodowym. Nieznany jest też tej procedurze zakaz wykorzystania dowodów określanych w literaturze procesowej jako „owoce z zatrutego drzewa"*[42]. Oprócz tego Sąd Najwyższy w uzasadnieniu do wyroku z 5 lutego 2008 r. wskazał następującą okoliczność: (…) *nie ulega wątpliwościom, że nagranie zostało dokonane bez przewidzianej w tym przepisie zgody sądu, jednakże Kodeks postępowania karnego nie eliminuje dowodów mających cechy „owoców*

---

[37] M. Florczak-Wątor, *Dopuszczalność wykorzystania w postępowaniu karnym dowodu nielegalnie pozyskanego. Glosa do wyroku s. apel. z dnia 27 kwietnia 2017 r., II AKa 213/16*, https://sip.lex.pl/komentarze-i-publikacje/glosy/dopuszczalnosc-wykorzystania-w-postepowaniu-karnym-dowodu-nielegalnie-386214361 [dostęp: 10 XII 2020].

[38] A. Rychlewska, *O przepisie art. 168a k.p.k. jako przyzwoleniu na korzystanie w ramach procesu karnego z dowodów zdobytych w sposób nielegalny*, „Palestra" 2016, nr 5, s. 14.

[39] C. Kulesza, *Art. 168a*, w: *Kodeks postępowania karnego. Komentarz*, K. Dudka i in. (red.), WKP 2018, https://sip.lex.pl/#/commentary/587774788/572228 [dostęp: 10 XII 2020].

[40] Wyrok SN z 2 II 2016 r., sygn. IV KK 346/14, Biul. PK 2016/1-3/79-88.

[41] Wyrok SA w Lublinie z 22 I 2013 r., Lex nr 1289474.

[42] Postanowienie SN z 14 XI 2006 r., sygn. V KK 52/06, Lex nr 202271.

zatrutego drzewa", które podlegają swobodnej ocenie sądu w połączeniu z pozostałymi dowodami[43]. Linia orzecznicza w tej materii nie jest jednak jednolita. W judykaturze istnieje również pogląd, zgodnie z którym dowód uzyskany z naruszeniem prawa ma charakter nielegalny, gdyż ze względów konstytucyjnych nie może stanowić podstawy ustaleń faktycznych. Takie stanowisko zajął Sąd Najwyższy, który w postanowieniu z 30 listopada 2010 r. orzekł, że (…) *niezachowanie określonych w art.19a ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2007 r. Nr 43, poz. 277 ze zm.) ustawowych warunków dopuszczalności przeprowadzenia czynności operacyjno-rozpoznawczych uniemożliwia w procesie karnym wykorzystanie uzyskanego w ich trakcie materiału dowodowego*[44]. Podobnie stwierdził Sąd Apelacyjny w Białymstoku: (…) *posługiwanie się w procesie dowodami, które stanowią tzw. „owoc zatrutego drzewa", jest niedopuszczalne: nie spełnia ono podstawowych wymogów konstytucyjnych, narusza prawa obywatelskie i stoi w kolizji z postanowieniami konwencji międzynarodowych, których Polska jest stroną*[45]. Ten pogląd podzielił również Sąd Apelacyjny w Krakowie: (…) *uzyskanie dowodu z zeznań świadka bez odpowiedniego poinformowania go o jego uprawnieniach (art. 173 § 2 kpk) sprawia, że dowód ten jest wadliwy, a przeto wyrok na takich zeznaniach oparty – nieprawidłowy jako „owoc zatrutego drzewa"*[46].

Analiza literatury przedmiotu oraz judykatury prowadzi do wniosku, że niewielką przewagę ma stanowisko, zgodnie z którym jest możliwe dopuszczanie dowodów uzyskanych z naruszeniem prawa. Jego zwolennicy twierdzą, że jest to zgodne z brakiem zakazu dowodowego w kpk dotyczącego owoców zatrutego drzewa, dotarciem do prawdy materialnej oraz działaniem organów państwa w granicach i na podstawie prawa. Dopuszczenie dowodów wynikających z doktryny owoców zatrutego drzewa nie wyłącza odpowiedzialności służbowej, dyscyplinarnej oraz karnej funkcjonariusza, który w procesie zdobywania informacji dopuścił się naruszenia prawa[47]. W celu uzupełnienia tego, co zostało wyżej powiedziane, należy wspomnieć o istnieniu pośredniego stanowiska. Zasygnalizował je Sąd Okręgowy w Białymstoku, który orzekł: (…) *o tym, czy dowód „pośrednio" skażony zostanie przyjęty i będzie stanowił podstawę ustaleń faktycznych decyduje Sąd, uwzględniając rozmiary przekroczenia obowiązujących zakazów dowodowych, wagę sprawy i wiarygodność pochodzącego z nielegalnego źródła dowodu*[48].

Brzmienie art. 168a kpk wprowadza ogólną zasadę dopuszczenia dowodów pozyskanych z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego

---

[43] Wyrok SN z 5 II 2008 r., sygn. SNO 2/08, Lex nr 432189.

[44] Postanowienie SN z 30 XI 2010 r., sygn. III KK 152/10, Lex nr 741307.

[45] Wyrok SA w Białymstoku z 18 III 2010 r., sygn. II AKa 18/10, Lex nr 577418.

[46] Wyrok SA w Krakowie z 2 II 1994 r., sygn. II AKr 248/93, Lex nr 28077.

[47] M. Gabriel-Węglowski, *Teoria „owoców zatrutego drzewa" a dopuszczalność przeprowadzania dowodów w postępowaniu karnym*, LEX/el. 2013, https://sip.lex.pl/#/publication/419618592 [dostęp: 10 XII 2020].

[48] Wyrok Sądu Okręgowego (dalej: SO) w Białymstoku z 26 XI 2009 r., sygn. III KK 224/08, Lex nr 1294013.

z art. 1 § 1 kpk. W związku z tym samo uzyskanie dowodów z naruszeniem prawa nie powoduje ich niedopuszczalności. Wynika to bowiem z konstrukcji komentowanej normy, która zawiera podwójną negację, tj. (…) *dowodu nie można uznać za niedopuszczalny*. Ustawodawca zakazał jednak wykorzystania takiego dowodu, w przypadku gdy został on uzyskany: a) w wyniku naruszenia przepisów postępowania, b) za pomocą czynu zabronionego. Posłużenie się wykładnią językową prowadzi do stwierdzenia, że przywołane przesłanki negatywne mogą wystąpić samodzielnie lub łącznie (alternatywa łączna)[49]. Warto podkreślić, że komentowana materia odnosi się zarówno do przepisów kpk, jak i innych przepisów pozakodeksowych regulujących czynności podejmowane w celu uzyskania dowodów, np. art. 19 ustawy o Policji. Tak wynika z wykładni językowej, gdyż ustawodawca nie dookreślił rodzaju postępowania[50]. Należy również nadmienić, że w omawianej normie stopniuje się naruszenie przepisów podczas uzyskiwania dowodów. Samo naruszenie prawa nie może stanowić bowiem wyłącznej przyczyny niedopuszczalności dowodu. Wspomniana wyłączność dotyczy właśnie stopniowalności naruszenia prawa w procesie uzyskiwania dowodów. Jest to na tyle istotne, że stopniowalność ma wpływ na dopuszczenie samego dowodu oraz jego wiarygodność[51]. Jako przykład może posłużyć przeszukanie w porze nocnej. W literaturze przedmiotu uznaje się, że dowody rzeczowe uzyskane w ramach takiego przeszukania mogą zostać włączone do postępowania. Z kolei dowody rzeczowe pozyskane podczas przeszukania przeprowadzonego pod nieobecność osoby dorosłej nie będą mogły stać się podstawą do ustalenia okoliczności faktycznych[52]. W piśmiennictwie podnosi się, że omawiana norma jest swoistym konsensusem pomiędzy całkowitym wyłączeniem a całkowitym przyzwoleniem na wykorzystanie dowodów uzyskanych z naruszeniem prawa[53]. Wskazany przepis pozwala zatem na stosowanie dowodów uzyskanych wbrew prawu z zastrzeżeniem dwóch wyjątków. Dotyczą one sytuacji, gdy dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności. W związku z nieprecyzyjnym sformułowaniem wyjątków określonych w art. 168a w doktrynie pojawił się spór co do zakresu stosowania komentowanej normy. Można wskazać trzy podejścia do tego zagadnienia.

Pierwsze z nich (ujęcie wąskie) jest związane z koniunkcją następujących warunków niedopuszczalności dowodu:

---

[49] S. Brzozowski, *Dopuszczalność dowodu w kontekście regulacji art. 168a k.p.k.*, „Przegląd Sądowy" 2016, nr 10, s. 63.

[50] S. Brzozowski, *Dopuszczalność dowodów uzyskanych z naruszeniem przepisów postępowania w kontekście art. 168a k.p.k.*, „Palestra" 2017, nr 1–2, s. 52–59.

[51] K.T. Boratyńska, *Procesowe konsekwencje wyjścia organów postępowania poza granice legalności czynności w nim podejmowanych*, w: *Granice procesu karnego. Legalność działań uczestników postępowania*, D. Gruszecka, J. Skorupka (red.), Warszawa 2015, s. 150–151.

[52] S. Brzozowski, *Dopuszczalność dowodu w kontekście*…, s. 71.

[53] D. Gruszecka, *W kwestii interpretacji znowelizowanego art. 168a k.p.k.*, „Palestra" 2017, nr 1–2, s. 60–78;

1) dowód został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 kk;
2) dowód został uzyskany w związku z pełnieniem obowiązków przez funkcjonariusza publicznego;
3) dowód został uzyskany w wyniku zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności[54].

W drugim podejściu (ujęcie szerokie) za dowód nielegalny uznaje się:

1) dowód uzyskany z naruszeniem przepisów postępowania w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych;
2) dowód uzyskany za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 kk, w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych;
3) dowód uzyskany za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 kk, oraz z naruszeniem przepisów postępowania w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych;
4) dowód uzyskany za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 kk, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności[55].

Trzecie podejście wskazuje na niedopuszczalność dowodu, jeżeli został on uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego przy jednoczesnym naruszeniu przepisów Konstytucji RP (np. art. 30, 47, 49, 51)[56].

Mając powyższe na uwadze, należy ustalić, jaka jest zależność między dowodem nielegalnym a dowodem pozyskanym w trakcie czynności operacyjno-rozpoznawczych. Na wstępie warto zaznaczyć, że zgromadzony materiał operacyjny na gruncie postępowania przygotowawczego ma wyłącznie charakter informacji o przestępstwie. Dowodem w rozumieniu kpk zostanie dopiero po wprowadzeniu go do postępowania. Zatem informacje operacyjne nie stają się automatycznie ustaleniami procesowymi[57]. Omawiana problematyka nie została unormowana w żadnej ustawie z zakresu prawa policyjnego. W związku z tym definicji wspomnianych czynności oraz ich związku z dowodem nielegalnym należy poszukiwać w orzecznictwie. Definicję dowodu uzyskanego w wyniku czynności operacyjno-rozpoznawczych, na przykładzie kontroli operacyjnej, podał Sąd Najwyższy w uchwale siedmiu sędziów z 23 marca 2011 r.:

> Dowodami uzyskanymi w wyniku kontroli operacyjnej, zarządzonej postanowieniem sądu, (…) które pozwalają na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego, są jedynie dowody dotyczące przestępstw,

[54] C. Kulesza, *Art. 168a…*

[55] Tamże.

[56] Tamże.

[57] K.J. Pawelec, *Substytuowanie dowodowe nielegalnych czynności operacyjno-rozpoznawczych. Zagadnienia podstawowe*, „Przegląd Sądowy" 2018, nr 3, s. 83.

> określonych w jej art. (…), które zostały wskazane w postanowieniu o zastosowaniu kontroli operacyjnej lub w postanowieniu o udzieleniu tzw. zgody następczej, w tym wydanej także w toku kontroli operacyjnej, (…) a popełnionych przez osobę, której dotyczyła zgoda pierwotna i osobę, co do której wydano zgodę następczą[58].

Przesłanki legalności dowodów uzyskanych w ramach czynności operacyjno-rozpoznawczych, na przykładzie kontroli operacyjnej, określił z kolei Sąd Apelacyjny we Wrocławiu. Stwierdził on, że skoro ustawa o CBA (…) *odnośnie kontroli operacyjnej wymaga, już we wniosku do sądu o jej zastosowanie, wskazania zarówno osoby, której ma ona dotyczyć, jak i czynu lub czynów, odnośnie których kontrola ta ma być zastosowana* (…)*, to jedynie w takim właśnie podmiotowym i przedmiotowym zakresie, określonym w postanowieniu sądu o zarządzeniu tej kontroli* (…)*, kontrola operacyjna staje się dopuszczalnym, legalnym wkroczeniem w sferę wolności*[59]. Dowody pozyskane w ramach kontroli zarządzonej przez sąd, ale poza jej granicami, a więc niezgodne z wymogami ustawy, nie są dowodami uzyskanymi legalnie. Druga przesłanka płynąca z tego orzeczenia jest związana z tym, że:

> (…) dowód może zostać uznany za niedopuszczalny, jeżeli został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego przy jednoczesnym naruszeniu przepisów Konstytucji RP (np. art. 30, 47, 49 czy 51). W takiej sytuacji ograniczenie ustawowe wyrażone zwrotem „wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego" (art. 168a k.p.k.) nie ma zastosowania[60].

Rola prokuratora i sądu w procesie kontroli operacyjnej

Uprawnienia prokuratora dotyczące zebranego materiału operacyjnego zostały wskazane przede wszystkim w art. 168b kpk:

> 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.

---

[58] *Uchwała składu siedmiu sędziów SN z dnia 23 marca 2011 r.*, sygn. I KZP 32/10, OSNKW 2011/3/22.

[59] Wyrok SA we Wrocławiu z 27 IV 2017 r., sygn. II AKa 213/16, Lex nr 2292416.

[60] Tamże.

Wskazana norma, podobnie jak art. 168a, wzbudziła niemałe kontrowersje, ponieważ interpretując ją w sposób literalny, można dojść do wniosku, że to prokurator jest podmiotem decydującym o wykorzystaniu materiału z kontroli operacyjnej, a nie sąd. Postawienie takiej tezy skutkowałoby tym, że w przypadku przekroczenia granic podmiotowych i przedmiotowych zarządzonej kontroli to sąd byłby związany decyzją prokuratora, a nie odwrotnie. Takie rozumienie art. 168b kpk prowadziłoby do sprzeczności, ponieważ podważałoby samodzielność jurysdykcyjną sądu. Ponadto oznaczałoby sprzeczność z art. 352 kpk, zgodnie z którym (…) *przewodniczący składu orzekającego po rozważeniu wniosków stron albo sąd z urzędu dopuszcza dowody, a przewodniczący zarządza ich sprowadzenie na rozprawę*. Sprzeczność dotyczyłaby także art. 368 § 1 kpk, który brzmi: (…) *o przychylnym załatwieniu wniosku dowodowego strony, któremu inna strona nie sprzeciwiła się, rozstrzyga ostatecznie przewodniczący; w innych wypadkach sąd wydaje postanowienie*. Mając powyższe na uwadze, należy podkreślić, że zgodnie z regulacjami kpk decyzja sądu o dopuszczeniu dowodu nie sprowadza się wyłącznie do wyrażenia formalnej zgody na przedłożony wniosek dowodowy, ale polega przede wszystkim na apriorycznej ocenie przydatności, celowości i dopuszczalności wykorzystania przedłożonego materiału operacyjnego. W związku z tym literalny sposób interpretacji komentowanej normy oznaczałby, że art. 352 kpk oraz art. 368 kpk są pozbawione jurydycznego znaczenia, a zarządzenie przewodniczącego lub postanowienie sądu o dopuszczalności dowodu sprowadzałoby się wyłącznie do bezwarunkowej akceptacji przez sąd wniosku prokuratora[61].

Warto zauważyć, że w art. 168b kpk ustawodawca posłużył się określeniem „decyzja w przedmiocie wykorzystania". Tymczasem w przepisach dotyczących wprowadzenia dowodu do postępowania ustawodawca używa sformułowania „dopuszczenie dowodu". Zatem właściwy sens komentowanego rozwiązania polega na tym, że w przypadku przekroczenia granic podmiotowych lub przedmiotowych w trakcie realizacji działalności operacyjnej to prokurator decyduje o zgłoszeniu takiego materiału jako środka dowodowego w akcie oskarżenia[62]. Ten pogląd podzielił Sąd Apelacyjny w Warszawie, wskazując, że decyzję w przedmiocie wykorzystania tego dowodu w postępowaniu karnym ustawodawca zastrzegł dla prokuratora, gdyż wyłącznie prokurator decyduje na etapie formułowania oskarżenia, jakie dowody na jego poparcie przedstawi sądowi. „Wykorzystanie" dowodu w rozumieniu analizowanego przepisu jest równoznaczne z jego zgłoszeniem do przeprowadzenia przed sądem[63]. Zatem decyzja prokuratora w rzeczywistości zastępuje wcześniej obowiązującą (od 11 czerwca 2011 r. do 14 kwietnia 2016 r.) instytucję tzw. zgody następczej sądu na wykorzystanie materiałów pochodzących z kontroli operacyjnej uzyskanych poza zakresem podmiotowym lub przedmiotowym postanowienia wyrażającego zgodę na jej stosowanie[64].

---

[61] D. Szumiło-Kulczycka, *Dalsze wykorzystywanie materiałów z kontroli operacyjnej (uwagi na tle art. 168b k.p.k.)*, „Państwo i Prawo" 2018, nr 10, s. 108–109.

[62] Tamże, s. 112.

[63] Wyrok SA w Warszawie z 13 VI 2016 r., sygn. II AKA 133/16, Lex nr 2171252.

[64] D. Szumiło-Kulczycka, *Dalsze wykorzystywanie materiałów*…, s. 112.

Innym zagadnieniem budzącym kontrowersje w kontekście art. 168b jest katalog przestępstw, wobec których prokurator może złożyć wniosek dowodowy. Wątpliwości dotyczą tego, czy przestępstwa nieskatalogowane (wobec których stosowanie kontroli operacyjnej nie jest przewidziane) wchodzą w zakres omawianej normy. Przede wszystkim dotyczy to materiałów przypadkowo uzyskanych podczas legalnie zarządzonej kontroli operacyjnej. W tej sprawie wypowiedział się Sąd Najwyższy we wspomnianej już uchwale składu siedmiu sędziów, który zauważył, że użyte sformułowanie „innego przestępstwa ściganego z urzędu lub przestępstwa skarbowego innego niż przestępstwo objęte zarządzeniem kontroli operacyjnej" w art. 168b kpk obejmuje swoim zakresem wyłącznie te przestępstwa, co do których sąd może wyrazić zgodę na zarządzenie kontroli operacyjnej, w tym te, o których mowa w art. 19 ust. 1 ustawy o Policji[65].

W związku z tym, jeżeli w wyniku legalnie prowadzonej kontroli operacyjnej okaże się, że rezultaty działalności operacyjnej przekraczają granice podmiotowe lub przedmiotowe zarządzonej kontroli, prokurator może zawnioskować w akcie oskarżenia o dopuszczenie tych dowodów, pod warunkiem że dotyczą one zamkniętego katalogu przestępstw zawartego w art. 19 ustawy o Policji. Należy jednak zaznaczyć, że art. 168b nie uprawnia prokuratora do zarządzenia kontroli operacyjnej ani do rozszerzenia jej zakresu. Ten przepis ma charakter techniczny i umożliwia prokuratorowi wybranie tych materiałów operacyjnych, na których oprze zarzuty zawarte w akcie oskarżenia[66]. Płynie z tego wniosek, że rolą prokuratora w zakresie postępowania z materiałami operacyjnymi jest sporządzenie aktu oskarżenia, w którym zawnioskuje o przeprowadzenie dowodów z zebranych materiałów operacyjnych, a ostateczna ich weryfikacja należy do sądu. Zgodnie ze stanowiskiem Sądu Okręgowego w Lublinie (…) *uznać zatem wypada, że na etapie postępowania sądowego prokurator może jedynie postulować przeprowadzenie takiego, wykorzystanego we wcześniejszej fazie postępowania, dowodu, zaś do sądu należeć będzie ocena takiego wniosku na gruncie art. 170 § 1 pkt 1*[67]. Ze względu na tę okoliczność sąd nie może oddalić wniosku dowodowego ani go pominąć tylko dlatego, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego. Dotyczy to zarówno przeprowadzenia, jak i wykorzystania dowodu[68]. Zatem ocena wniosków dowodowych zawartych w akcie oskarżenia sformułowanym przez prokuratora pod kątem ich nielegalności leży wyłącznie w kompetencji sądu. Nie wymaga się od sądu przeprowadzenia postępowania incydentalnego w celu ustalenia przesłanek wyrażonych w art. 168a. Tym bardziej nie jest wymagany prawomocny wyrok w sprawie o popełnione przestępstwo w celu uzyskania dowodu[69].

---

[65] Uchwała SN z 28 VI 2018 r., sygn. I KZP 4/18, Lex nr 2509692.

[66] D. Szumiło-Kulczycka, *Dalsze wykorzystywanie materiałów*…, s. 116.

[67] Wyrok SO w Lublinie z 13 IV 2017 r., sygn. XI Ka 120/17, Lex nr 2282522.

[68] R. Stefański, S. Zabłocki, *Art. 168a*, w: *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296*, R. Stefański, S. Zabłocki (red.), Warszawa 2019.

[69] C. Kulesza, *Art. 168a*…

Bibliografia

Biernaczyk A., *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a i 19b Ustawy z dnia 6 kwietnia 1990 roku o Policji*, w: *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, L. Paprzycki, Z. Rau (red.), Warszawa 2009, Wolters Kluwer.

Boratyńska K.T., *Procesowe konsekwencje wyjścia organów postępowania poza granice legalności czynności w nim podejmowanych*, w: *Granice procesu karnego. Legalność działań uczestników postępowania*, D. Gruszecka, J. Skorupka (red.), Warszawa 2015, C.H. Beck.

Brzozowski S., *Dopuszczalność dowodów uzyskanych z naruszeniem przepisów postępowania w kontekście art. 168a k.p.k.*, „Palestra" 2017, nr 1–2, s. 52–59.

Brzozowski S., *Dopuszczalność dowodu w kontekście regulacji art. 168a k.p.k.*, „Przegląd Sądowy" 2016, nr 10, s. 60–74.

Florczak-Wątor M., *Dopuszczalność wykorzystania w postępowaniu karnym dowodu nielegalnie pozyskanego. Glosa do wyroku s. apel. z dnia 27 kwietnia 2017 r., II AKa 213/16*, https://sip.lex.pl/komentarze-i-publikacje/glosy/dopuszczalnosc-wykorzystania-w-postepowaniu--karnym-dowodu-nielegalnie-386214361 [dostęp: 10 XII 2020].

Gabriel-Węglowski M., *Teoria „owoców zatrutego drzewa" a dopuszczalność przeprowadzania dowodów w postępowaniu karnym*, Lex 2013.

Gołębiewski J., *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*, Warszawa 2008, Wydawnictwa Akademickie i Profesjonalne.

Gruszecka D., *W kwestii interpretacji znowelizowanego art. 168a k.p.k.*, „Palestra" 2017, nr 1–2, s. 60–78.

Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 1996, Zakamycze.

Janiszewski-Downarowicz R., G*ranice dozwolonej prowokacji w polskim prawie karnym*, „Prokuratura i Prawo" 2009, nr 3, s. 87–97.

Klejnowska M., *Posłuch operacyjny i prowokacja policyjna*, „Prawo i Prokuratura" 2004, nr 3, s. 94–110, teza 5, 6 Lex, https://sip.lex.pl/#/publication/151037556/klejnowska-monika--podsluch-operacyjny-i-prowokacja-policyjna?keyword=Pods%C5%82uch%20operacyjny%20i%20prowokacja%20policyjna&cm=SREST [dostęp: 10 XII 2020].

Kołodziejczak M., Sobiech A., *Prawnie dopuszczalne postacie prowokacji*, „Państwo i Prawo" 2010, nr 11, s. 35–46.

Kosmaty P., *Przesyłka niejawnie nadzorowana*, „Prokurator" 2010, nr 3, s. 28–42.

Kulesza C., *Art. 168a*, w: *Kodeks postępowania karnego. Komentarz*, K. Dudka (red.), WKP 2018, https://sip.lex.pl/#/commentary/587774788/572228 [dostęp: 10 XII 2020].

Łyżwa A., Tokarski M., *Art. 19 ustawy o Policji*, w: *Ustawa o Policji. Komentarz*, Ł. Czebotar i in. (red.), Warszawa 2015, Wolters Kluwer.

Niemczyk Z. *Czynności operacyjno-rozpoznawcze i możliwość wykorzystania ich rezultatów w postępowaniu karnym*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2013, nr 3, s. 5–21.

Ożóg-Wróbel K., *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych,* „Roczniki Nauk Prawnych" 2012, nr 4, s. 113–145.

Pawelec K.J., *Substytuowanie dowodowe nielegalnych czynności operacyjno-rozpoznawczych. Zagadnienia podstawowe*, „Przegląd Sądowy" 2018, nr 3, s. 74–85.

Pływaczewski W., Kędzierska G., *Leksykon policyjny*, Szczytno 2001, Wydawnictwo Wyższej Szkoły Policji.

Rychlewska A., *O przepisie art. 168a k.p.k. jako przyzwoleniu na korzystanie w ramach procesu karnego z dowodów zdobytych w sposób nielegalny*, „Palestra" 2016, nr 5, s. 11–18.

Stefański R., Zabłocki S.*, Art. 168a*, w: *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296*, R. Stefański, S. Zabłocki (red.), Warszawa 2019, Wolters Kluwer.

Szumiło-Kulczycka D., *Dalsze wykorzystywanie materiałów z kontroli operacyjnej (uwagi na tle art. 168b k.p.k.)*, „Państwo i Prawo" 2018, nr 10, s. 107–120.

Taracha T.A., *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, Wydawnictwo UMCS.

Teluk R., *Inwigilacja i infiltracja jako efektywne metody uzyskiwania informacji operacyjnych na temat środowiska przestępczego lub kryminogennego*, „Zeszyty Prawnicze" 2014, nr 4, s. 177–196.

Zakrzewski R., Woźniak A., *Nowelizacja ustawy o Policji – rozszerzenie uprawnień operacyjno-rozpoznawczych*, „Monitor Prawniczy" 1996, nr 1.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (tj.: DzU z 2020 r. poz. 1444, ze zm.).

Ustawa z dnia 6 czerwca 1997 r – Kodeks postępowania karnego (tj.: DzU z 2021 r. poz. 534).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (tj.: DzU z 2020 r. poz. 360, ze zm.).

Orzecznictwo

Uchwała SN z 28 VI 2018 r., sygn. I KZP 4/18, Lex nr 2509692.

Wyrok SN z 2 II 2016 r., sygn. IV KK 346/14, Biul. PK 2016/1-3/79-88.

Uchwała składu siedmiu sędziów z dnia 23 marca 2011 r., sygn. I KZP 32/10, OSNKW 2011/3/22.

Postanowienie SN z 30 XI 2010 r., sygn. III KK 152/10, Lex nr 741307.

Wyrok SN z 5 II 2008 r., sygn. SNO 2/08, Lex nr 432189.

Wyrok SN z 10 X 2007 r., sygn. II KK 387/06, OSNwSK 2007/1/1587.

Postanowienie SN z 14 XI 2006 r., sygn. V KK 52/06, Lex nr 202271.

Wyrok SA we Wrocławiu z 27 IV 2017 r., sygn. II AKa 213/16, Lex nr 2292416.

Wyrok SA w Warszawie z 13 VI 2016 r., sygn. II AKA 133/16, Lex nr 2171252.

Wyrok SA w Lublinie z 22 I 2013 r., Lex nr 1289474.

Wyrok SA w Białymstoku z 18 III 2010 r., sygn. II AKa 18/10, Lex nr 577418.

Wyrok SA w Krakowie z 2 II 1994 r., sygn. II AKr 248/93, Lex nr 28077.

Wyrok SO w Lublinie z 13 IV 2017 r., sygn. XI Ka 120/17, Lex nr 2282522.

Wyrok SO w Białymstoku z 26 XI 2009 r., sygn. III KK 224/08, Lex nr 1294013.

Abstrakt

Zagadnienia omawiane w niniejszym artykule dotyczą statusu normatywnego czynności operacyjno-rozpoznawczych w kontekście ustawy o Policji oraz kodeksu postępowania karnego. Podjęto próbę wskazania warunków, które rzutują na legalny charakter inwigilacji, a co za tym idzie – na skuteczne wykorzystanie materiału operacyjnego w procesie karnym. W tym celu scharakteryzowano niejawną aktywność Policji, wyszczególniając dopuszczalne metody operacyjne oraz definiując czynności operacyjno-rozpoznawcze w świetle literatury przedmiotu. Aby w pełni zobrazować problematykę poruszoną w artykule, przeanalizowano relację prawną między dowodem nielegalnym, o którym mowa w art. 168a kpk, a dowodem z czynności operacyjno-rozpoznawczych, na przykładzie zarządzonej kontroli operacyjnej. Praktyczny wymiar tych rozważań omówiono z punktu widzenia postępowania dowodowego, z uwzględnieniem ról i obowiązków procesowych prokuratora oraz sądu.

Słowa kluczowe: metody operacyjne, doktryna owoców zatrutego drzewa, kontrola operacyjna, zakup kontrolowany.

Normative approach to operational and reconnaissance activities in terms of illegal evidence

Abstract

The issues discussed in this article refer to the normative status of operational and investigative activities in the context of the Police Act and the Code of Criminal Procedure. Namely, an attempt was made to demonstrate the conditions that affect the legal nature of surveillance, and thus the effective use of operational material in a criminal trial. For this purpose, the covert activity of the Police has been characterized by listing acceptable operational methods and defining operational and reconnaissance activities in the light of the literature on the subject. Therefore, in order to fully illustrate the issues discussed, an analysis was conducted of the legal relationship between the illegal evidence referred to in Art. 168a of the Code of Criminal Procedure and the evidence from operational and reconnaissance activities, on the example of an ordered operational control. The practical dimension of these considerations is discussed from the point of view of evidence proceedings, taking into account the procedural roles and responsibilities of the prosecutor and the court.

Keywords: operational work, fruit of the poisonous tree doctrine, operational control, sting operation.

ANDRZEJ KARAŚ
ORCID: 0000-0002-0028-0706

DOI: 10.4467/20801335PBW.21.015.13572

Modelowanie operacji informacyjnych z wykorzystaniem teorii sterowania refleksyjnego[1]

Słowa Heraklita z Efezu, że jedyną stałą rzeczą w życiu jest zmiana, doskonale oddają rzeczywistość, w jakiej żyjemy. Zmiany środowiska, układu sił politycznych, postęp w nauce, zmiany kulturalne czy technologiczne są możliwe do zaobserwowania w dłuższych odstępach czasu. Niezmienne pozostało niestety istnienie konfliktów między ludźmi oraz między innymi podmiotami. Dzięki osiągnięciom nauki i techniki zmieniają się jedynie formy tych konfliktów. Ponadto żyjemy w czasach, w których te zmiany przybierają na intensywności. Informacja zawsze odgrywała ważną rolę w sytuacjach konfliktowych, jednak w dzisiejszych czasach ta zależność jest jeszcze bardziej widoczna. Jako główną przyczynę tej sytuacji należy wskazać informatyzację oraz technokratyzację praktycznie każdej dziedziny życia. Powoduje to, że całe społeczeństwa, firmy czy instytucje państwowe są coraz bardziej uzależniane od potrzeby przetwarzania oraz wymiany informacji. Na bazie tych doświadczeń oraz osiągnięć nauki i techniki powstała koncepcja wojny informacyjnej oraz operacji informacyjnej jako nowoczesnych form rozstrzygania sytuacji konfliktowych.

Dzięki technologii zastosowanie operacji informacyjnych w konfliktach zbrojnych czy działań informacyjnych w konfliktach niemilitarnych, np. biznesie, stało się o wiele prostsze. Powszechny dostęp do internetu spowodował, że wpływanie na opinię całych społeczeństw nigdy nie było tak łatwe. Każdy może opublikować w krótkim czasie wiadomość dla odbiorców z całego świata, czego nie może zaoferować telewizja czy prasa. Skalę problemu pokazuje liczba tak zwanych *fake newsów* w mediach. Nie bez powodu współczesne społeczeństwa są nazywane społeczeństwami informacyjnymi. Obecnie odpowiednio dobrane słowa ludzi, którzy cieszą się dużym

[1] Fragment pracy magisterskiej pt. *Modelowanie operacji informacyjnych z wykorzystaniem teorii sterowania refleksyjnego* (Wojskowa Akademia Techniczna, Wydział Cybernetyki). Autor wykorzystał fragmenty rozdziału 1., *Wstęp* oraz w całości podrozdziały od 3.3. do 4.2. włącznie.

autorytetem w społeczeństwie, mogą równać się dawnej sile militarnej wywierającej wpływ na jednostki oraz rządy. Operacje informacyjne były wykorzystywane w walce od zawsze, do dziś przesądzają one o klęsce lub wygranej na konwencjonalnym polu walki. Teoretycy wojenni oraz historycy porównują zjawisko wojny informacyjnej do wynalezienia czołgu oraz bomby atomowej i ich wpływu odpowiednio na pierwszą oraz drugą wojnę światową. Dowódcy są zgodni także co do wzrostu znaczenia operacji informacyjnych w przyszłych konfliktach. Pisze o tym także Gabriel Nowacki: *Coraz częściej w sferze pozamilitarnych form walki szukać się będzie możliwości obrony lub ataku, uzyskania równowagi lub przewagi i być może decydujących rozstrzygnięć*[2].

Pojęcie refleksji

Koncepcja sterowania refleksyjnego opiera się na pojęciu refleksja. Podobnie do informacji, refleksja ma wiele definicji. Każdy z autorów podaje wykładnię refleksji w zależności od swoich potrzeb oraz obszaru badań. *Słownik języka polskiego* objaśnia ten termin jako: (…) *głębsze zastanowienie się nad czymś, wywołane silnym przeżyciem*. Jednym z filozoficznych wyjaśnień podanych przez słownik jest: (…) *zwrócenie się podmiotu myślącego ku własnej aktywności*[3]. Refleksja może być rozumiana zwyczajowo jako ludzka umiejętność do zajmowania stanowiska obserwatora w stosunku do własnych myśli, przekonań oraz uczuć[4]. Ten termin może oznaczać także subiektywne uwzględnienie wiedzy oraz krytyczną analizę jej istoty. Przejawem tego jest na przykład samoaktualizacja ludzi, tzn. poprawianie swoich działań na podstawie popełnionych błędów[5]. Może to być również wyciąganie nowych wniosków na podstawie dotychczasowej wiedzy. Dzięki refleksji w ludzkich umysłach istnieje odwzorowanie, tzw. obraz realnej rzeczywistości. Ta rzeczywistość jest tworzona przez obiekty zarówno materialne, np. przedmioty, jak i niematerialne, np. słowa. Rzeczywistość wytworzona w umyśle człowieka w procesie refleksji jest nazywana rzeczywistością refleksyjną.

Należy wyróżnić dwa rodzaje refleksji. Refleksją pierwszego rodzaju lub inaczej samorefleksją jest nazywany proces analizy własnych myśli, przekonań oraz zasad działania. Produktem tego procesu jest obraz rzeczywistości w umyśle podmiotu. Refleksja drugiego rodzaju przejawia się przez umiejętność podmiotu do tworzenia wyobrażeń na temat obrazów rzeczywistości innych podmiotów. Obejmuje ona przeświadczenie

---

[2] G. Nowacki, *Współczesne poglądy na prowadzenie walki informacyjnej. Studium teoretyczne*, Warszawa 2001.

[3] *Słownik języka polskiego*, https://sjp.pwn.pl/szukaj/refleksja.html [dostęp: 8 IV 2019].

[4] V.A. Lefebvre, *Sketch of Reflexive Game Theory*, Irvine 1998.

[5] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational and Strategic Reflexion: a Survey*, „Advances in Systems Science and Application" 2014, nr 3, s. 254–278.

danego podmiotu na temat przekonań, zasad działania oraz samorefleksji innych podmiotów[6].

Należy dodać, że ten proces jest nieskończony z powodu swojej rekurencyjnej[7] istoty, tzn. jedno przekonanie tworzy kolejne przez refleksję[8]. Pojęcie „refleksja" uogólnił oraz rozszerzył Vladimir A. Lefebvre[9], rosyjski psycholog i matematyk.

Dzięki rekurencyjnemu charakterowi zjawiska oraz uogólnieniu wprowadzonemu przez autora teorii można wyróżnić hierarchię rzeczywistości, którą obrazuje rys. 1.

Rys. 1. Hierarchia rzeczywistości jako wynik procesu refleksji.

Źródło: V.A. Lefebvre, *Sketch of Reflexive Game Theory*, Irvine 1998.

Największa z głów odpowiada podmiotowi (agentowi) refleksyjnemu, tzn. osobie dokonującej refleksji – (a). Dwie zagnieżdżone głowy przedstawiają „obraz siebie" (a) oraz „obraz innego agenta" (b) z punktu widzenia zewnętrznego obserwatora. Dla agenta (a) pełnią one rolę „prawdziwy ja" oraz „prawdziwy inny". Cztery zagnieżdżone głowy przedstawiają obrazy rzeczywistości z perspektywy agenta (a) – lewa para twarzy oraz z perspektywy agenta (b) – prawa para twarzy. Hierarchię rzeczywistości można przedstawić także w postaci drzewa, które Lefebvre nazywa strukturą refleksyjną (rys. 2)[10].

---

6 Tamże; M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-ee571f3e-2942-46ce-9e19-af8e970c6f7a [dostęp: 30 III 2019].

7 Rekurencyjny – w matematyce, logice, programowaniu: dający się obliczyć, wyrazić za pomocą wielkości uprzednio znanych, https://sjp.pl/rekurencyjny (przyp. red).

8 R. Kasprzyk, *The Essence of Reflexive Control and Diffusion of Information in the Context of Information Environment Security*, w: *Internetional Conference in Intelligent Systems in Production Engineering, and Maintenance. ISPEM 2018. Advances in Intelligent Systems and Computing*, t. 835, A. Burduk i in., A. Tubis (red.), Cham 2018, s. 720–728.

9 V.A. Lefebvre, *Sketch of Reflexive Game Theory*…

10 Tamże.

Rys. 2. Struktura refleksyjna.

Źródło: V.A. Lefebvre, *Sketch of Reflexive Game Theory*, Irvine 1998.

Korzeń drzewa przedstawionego powyżej odpowiada działaniom agentów. Węzły na drugim poziomie drzewa przedstawiają rzeczywistość widzianą przez agenta. Węzły na trzecim poziomie drzewa reprezentują rzeczywistość dla pierwszego oraz drugiego agenta z punktu widzenia pierwszego agenta[11]. Hierarchia rzeczywistości może zostać uogólniona do *n* poziomowej hierarchii, co Lefebvre pokazuje w swoim artykule. Jak można zauważyć na powyższych rysunkach, rzeczywistości wytworzone przez agentów są jedynie subiektywnymi reprezentacjami realnej rzeczywistości[12].

Refleksja a sterowanie

Zgodnie ze słowami Mariana Mazura sterowaniu zawsze towarzyszy dążenie do pewnego ustalonego celu[13]. Może być ono także definiowane jako (…) *celowy wpływ wywierany na kontrolowany system w celu zapewnienia jego wymaganego zachowania*[14]. Zgodnie z teorią sterowania, wyróżniamy system sterujący oraz sterowany, które są połączone wzajemnie torami sterowniczymi. Możliwe jest także uwzględnienie zewnętrznych zakłóceń oddziałujących na oba systemy[15]. Opisywaną sytuację ilustruje rys. 3.

[11] Tamże.

[12] R. Kasprzyk, *The Essence of Reflexive Control*…

[13] M. Mazur, *Jakościowa teoria informacji*, Warszawa 1970.

[14] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational*…, s. 255.

[15] M. Mazur, *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966.

Rys. 3. System sterowany i sterujący jako układ cybernetyczny.

Źródło: D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational and Strategic Reflexion: a Survey*, „Advances in Systems Science and Application" 2014, nr 3, s. 254–278.

Najważniejszą funkcją systemu sterującego jest wybór oraz wykonanie odpowiedniej akcji w celu wymuszenia na systemie kontrolowanym pożądanego działania. Trudnością dla wspomnianego systemu kontrolującego jest wpływ zewnętrznych zakłóceń na wybór akcji. Najważniejszym elementem jest tor sterowniczy, który pełni funkcję środowiska umożliwiającego wzajemne oddziaływanie obu systemów. Dzięki temu może zaistnieć sprzężenie zwrotne między systemem sterowanym a systemem sterującym[16].

Wspomniane sprzężenie zwrotne może być rozumiane jako proces refleksji, tzn. budowanie obrazu systemu sterowanego przez system sterujący. Jest to pierwsze powiązanie między procesem sterowania a procesem refleksji. Drugie powiązanie opiera się na tym, że każdy z aktywnych systemów, tj. ludzie bądź dana zbiorowość, jest zdolny do wykonania refleksji pierwszego stopnia[17]. Tylko takie systemy będą rozpatrywane w dalszej części tekstu.

W celu przewidywania zachowania oraz odpowiedzi podmiotu kontrolowanego jest potrzebny jego model. Jest on rozumiany jako obraz danego systemu, który może zostać przedstawiony w postaci schematu, fizycznego obiektu lub istnieć jedynie w świadomości podmiotu kontrolującego. Sam proces modelowania, tj. tworzenia obrazu danego systemu, może być rozpatrywany jako proces refleksji. Z tego wynika trzecie powiązanie między sterowaniem a refleksją rozumiane jako umiejętność podmiotu sterującego oraz sterowanego przeprowadzenia procesu refleksji w stosunku do innych podmiotów czy obiektów[18].

Decydującym czynnikiem wykorzystywanym w sterowaniu refleksyjnym jest możliwość kontrolowania samego procesu refleksji oraz jej wyników. Ta relacja stwarza możliwość informacyjnej oraz refleksyjnej kontroli (sterowania refleksyjnego)[19].

---

[16] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational…*

[17] Tamże.

[18] Tamże.

[19] Tamże.

Pojęcie sterowania refleksyjnego

Była już mowa o koncepcji wojny informacyjnej oraz operacji informacyjnej (te terminy będą stosowane zamiennie). Jednym z niemilitarnych sposobów prowadzenia operacji informacyjnych jest sterowanie refleksyjne. To zjawisko jest znane także pod nazwą zarządzania refleksyjnego. Autorem tej teorii jest wspomniany Lefebvre. Głównym celem sterowania refleksyjnego jest wpłynięcie na nieświadomą jednostkę lub daną zbiorowość tak, aby dokonała pewnego, z góry założonego przez atakującego, czynu.

Najważniejszą „bronią" wykorzystywaną w procesie zarządzania refleksyjnego jest odpowiednio spreparowana informacja. Obiektem tego procesu jest umysł człowieka – jego przekonania oraz poglądy. Bardzo trafnie ujął to Michał Wojnowski: *Mimo upływu stuleci, obiektami manipulacji nadal pozostają: świadomość, emocje i zachowania ludzi. Ciągłemu doskonaleniu ulegają natomiast sposoby i narzędzia wywierania wpływu na zbiorowości ludzkie, do czego przyczynia się intensywny rozwój nauki i techniki*[20]. Cel jest realizowany za pomocą technik manipulacji oraz sterowania społeczeństwem.

Jak napisano wcześniej, każdy podmiot tworzy własny obraz rzeczywistości w procesie refleksji. Pozostające poza świadomością podmiotu oddziaływanie agresora na jego myśli, przekonania oraz na sam proces refleksji będzie pośrednio wpływało na proces decyzyjny tego podmiotu. Tym samym późniejsze działania podmiotu powinny być zgodne z założeniami agresora.

Według Lefebvre'a zarządzanie refleksyjne można realizować przez:

- kreowanie oraz przekazywanie fałszywego obrazu sytuacji;
- przedstawienie przeciwnikowi uwiarygodnionego planu własnych działań;
- zobrazowanie oponentowi wielu nieprawdziwych celów.

Inne techniki wykorzystywane w procesie zarządzania refleksyjnego Wojnowski opisuje szerzej w swoim artykule[21].

Zastosowanie wyżej wymienionych technik, z wykorzystaniem takich kanałów dystrybucji informacji, jak media społecznościowe lub środki masowego przekazu, powinno umożliwić skuteczne manipulowanie percepcją jednostek czy całych społeczności. Na potwierdzenie tej tezy należy przedstawić sposób, w jaki ludzie pozyskują oraz weryfikują wiarygodność informacji[22]. Niestety w dzisiejszych czasach większość informacji jest przyjmowana bezkrytycznie, co może być wykorzystane do niezauważalnego wprowadzenia informacji do świadomości człowieka[23].

---

[20] M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat*…, s. 11.

[21] Tamże.

[22] R. Kasprzyk, *The Essence of Reflexive Control*…

[23] M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat*…

Sterowanie refleksyjne jako model sytuacji konfliktowych

Teorię sterowania refleksyjnego należy rozpatrywać także w kontekście modelowania sytuacji konfliktowych, co zauważył sam autor teorii. To podejście jest alternatywną formą modelowania sytuacji strategicznych w przypadku braku pełnej informacji. Tym zagadnieniem zajmuje się teoria gier refleksyjnych zaproponowana przez Lefebvre'a. Wspomniane podejście różni się także od teorii zachowania zbiorowego, która uznaje, że każdy z graczy prowadzi własny proces decyzyjny, przy równoczesnej niewiedzy na temat zachowań oraz informacji posiadanych przez przeciwników.

Metoda sterowania refleksyjnego wydaje się bardziej adekwatna do opisu sytuacji strategicznych niż modele budowane za pomocą klasycznej teorii gier. Żaden z graczy w rzeczywistości nie ma takich samych przekonań, zasad działania ani informacji o stanie danej gry. Dlatego należy przyjąć, że żaden z nich nie odbiera sytuacji konfliktowej obiektywnie. Różnice przejawiają się w postrzeganiu zasad, celów, ról oraz świadomości poszczególnych graczy[24].

Sterowanie refleksyjne wykorzystuje zjawisko refleksji także do budowania wyobrażenia o innych graczach oraz ich poczynaniach – hierarchii przekonań. Ta technika bazuje na modelu refleksyjnym stworzonym na podstawie informacji posiadanych przez gracza, stąd tak ważne są działania wywiadowcze w rzeczywistym świecie. Pozwala lepiej przewidzieć poczynania przeciwników oraz wydaje się bardziej adekwatna niż probabilistyczne[25] oszacowania. Dodatkowo daje możliwość przedstawienia, jak dany gracz postrzega siebie oraz swoich przeciwników, czego nie zapewniają inne modele. Potwierdzają to słowa autora teorii: (…) *model podmiotu powinien odzwierciedlać nie tylko sferę jego zachowania, lecz także jego zdolność do pojmowania samego siebie i drugich podmiotów, włączając i te, które próbują uzyskać kontrolę nad jego działaniem*[26]. Wiedza o tym, jak rozumuje przeciwnik, uzyskana na podstawie modelu refleksyjnego daje dużą przewagę na każdym polu. Lefebvre twierdził, że każda sytuacja konfliktowa toczy się w trzech sferach:

- sferze fizycznej – przez wszelakiego rodzaju starcia oraz interakcje;
- sferze technicznej – dzięki przeciwstawnym systemom informacyjno-kierowniczym;
- sferze kognitywnej[27], w której potyczka dotyczy procesów mających wpływ na decyzje uczestników konfliktu[28].

Poprawne odwzorowanie danej sytuacji konfliktowej jest najważniejszym czynnikiem decydującym o zwycięstwie. Z tego powodu sterowanie refleksyjne skupia się

---

[24] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational*…

[25] Probabilistyka – dział matematyki zajmujący się badaniem prawidłowości występujących w zdarzeniach losowych, https://sjp.pwn.pl/slowniki/probabilistyczny.html (przyp. red.).

[26] M. Wojnowski, „*Zarządzanie refleksyjne*" *jako paradygmat*…, s. 20.

[27] Poznawczej (przyp. red.).

[28] Zob. M. Wojnowski, „*Zarządzanie refleksyjne*" *jako paradygmat*…

na ingerencji w świadomość oraz poglądy przeciwnika w celu zmiany jego obrazu myślenia. Takie działania wpływają na proces decyzyjny oponenta.

Tworzenie modelu refleksyjnego jednostki lub danej społeczności bazuje na portretach psychologicznych. Jednak ten model jest znacznie szerszym pojęciem niż portret psychologiczny[29]. Zgodnie z wcześniejszymi rozważaniami powinien on zawierać odwzorowanie rozumowania oraz samoświadomości podmiotu, wraz z opisem jego potencjalnych zachowań w danej sytuacji.

Co więcej, ta teoria znajduje zastosowanie także na innych polach. Potwierdzają, słowa Wojnowskiego: *Teoria ta może też znajdować zastosowanie w tworzeniu tzw. modeli refleksyjnych przestępców, terrorystów, a nawet całych grup i organizacji*[30]. Wspomniany autor podkreśla także wkład Mariana Mazura w teorię tworzenia profili psychologicznych w postaci układów samodzielnych, która służy do typowania przywódców organizacji przestępczych[31].

Refleksja informacyjna a strategiczna

Klasyfikacja refleksji ze względu na stopień świadomości podmiotu została opisana wcześniej. Istnieje jednak jeszcze jeden dość istotny podział: ze względu na cel lub wynik refleksji.

Na proces oraz wyniki refleksji informacyjnej składają się dane na temat parametrów niepewnych co do wartości, posiadane przez dany podmiot oraz jego przeciwników. Natomiast wyniki refleksji strategicznej zawierają informacje o zasadach decyzyjnych stosowanych przez przeciwników dzięki zbudowanej przez siebie świadomości – na podstawie strategii informacyjnej. Należy dodać, że obie te techniki znajdują zastosowanie w sytuacji, gdy mamy do czynienia z niepełną lub niewystarczającą informacją[32].

Szkielet sterowania refleksyjnego

Na podstawie informacji przedstawionych wcześniej można stwierdzić, że proces sterowania refleksyjnego pod wieloma względami jest podobny do procesu sterowania. Z tego względu może zostać opisany za pomocą definicji oraz schematów procesu sterowania. W celu uproszczenia opisu zagadnienia w procesie sterowania refleksyjnego zostaną wyróżnione dwa systemy. Są nimi: podmiot sterujący (system sterujący) oraz podmiot sterowany (system sterowany), które można przedstawić za pomocą schematu (rys. 4). Zadaniem systemu kontrolującego jest całkowite przejęcie kontroli

---

[29] Tamże.

[30] Tamże, s. 35.

[31] Tamże.

[32] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational*…

lub wpłynięcie na proces decyzyjny systemu kontrolowanego. W tym celu podmiot kontrolujący musi zbudować z posiadanych przez siebie informacji model podmiotu kontrolowanego. Następnie na podstawie modelu jest preparowana odpowiednia informacja, która ma wpłynąć na przekonania bądź zasady działania obiektu[33]. Po czym jest ona przesyłana do obiektu kontrolowanego przez specjalnie wyselekcjonowany kanał komunikacji (o czym pisze Wojnowski oraz co pokazuje model rozprzestrzeniania się informacji[34]).

Rys. 4. Tworzenie obrazu systemu sterującego w procesie refleksji.

Źródło: Opracowanie własne na podstawie: R. Kasprzyk, *The Essence of Reflexive Control and Diffusion of Information in the Context of Information Environment Security*, w: *Internetional Conference in Intelligent Systems in Production Engineering, and Maintenance. ISPEM 2018. Advances in Intelligent Systems and Computing*, t. 835, A. Burduk, E. Chlebus, T. Nowakowski, A. Tubis (red.), Cham 2018, s. 720–728.

Nieodpowiednio dobrany kanał do transmisji informacji może prowadzić do skutków przeciwnych niż zamierzone. Ostatnim krokiem w procesie sterowania refleksyjnego jest pobranie nowej informacji o obiekcie sterowanym przez podmiot sterujący. Ten krok jest nazywany sprzężeniem zwrotnym lub właśnie refleksją. Każda nowa informacja rozbudowuje model podmiotu sterowanego, który posiada podmiot sterujący. Kilkakrotne powtórzenie wymienionych kroków zazwyczaj prowadzi do wywarcia zamierzonego wpływu na podmiot sterowany[35].

Liczba podmiotów sterujących oraz kontrolowanych jest zazwyczaj większa w przypadkach praktycznych. Co ważniejsze, każdy z nich pełni obie te funkcje naraz, tzn. stara się zmienić świadomość swoich przeciwników oraz jest poddany takim działaniom ze strony swoich oponentów. Zasadniczym problemem przy modelowaniu

[33] R. Kasprzyk, *The Essence of Reflexive Control…*

[34] M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat…*; A.P. Mikhailov, N.A. Marevtseva, *Models of Information Warfare,* „Mathematical Models and Computer Simulations" 2012, nr 3, s. 251–259.

[35] R. Kasprzyk, *The Essence of Reflexive Control…*

procesu sterowania refleksyjnego w mediach społecznościowych jest zrozumienie procesu rozprzestrzeniania się (dyfuzji) informacji w systemach sieciowych[36].

Bazowy model sterowania refleksyjnego

Przed zdefiniowaniem bazowego modelu gry refleksyjnej należy omówić pojęcie równowaga Nasha. Oznacza ono, że gracz po określeniu własnej strategii i po wybraniu strategii przez jego oponentów nie zwiększy swojej wypłaty przez zmianę swojego planu działania. Można to przedstawić za pomocą poniższej nierówności, która musi być spełniona dla każdego z *n* graczy:

$$u_i(s_i, \theta_{-i}) > u_i(s_i', \theta_{-i})$$

gdzie:
i = 1, …, n.

Za pomocą równowagi Nasha można wyznaczyć najlepsze rozwiązania (równowagę) dla danej gry[37].

Składowe opisu modelu

Model teoriogrowy lub zbiorowego zachowania może być rozpatrywany na trzech poziomach:

- fenomenologicznym – opisuje on działanie systemu za pomocą odpowiednio zbudowanego modelu gry;
- predykcyjnym – jest równoznaczny z przewidywaniem zachowania się systemu, tzn. ustalaniem się równowagi;
- normatywnym – opisuje proces kontroli systemu, tzn. osiąganie wcześniej założonej równowagi przez odpowiednie dobranie parametrów opisujących system[38].

Biorąc pod uwagę refleksję informacyjną oraz strategiczną, można wyróżnić trzy elementy składające się na wcześniej wymienione poziomy opisu modelu. W przypadku refleksji informacyjnej są nimi: struktura świadomości (ang. *awareness structure*), równowaga informacyjna oraz sterowanie informacyjne. Natomiast refleksję

[36] R. Kasprzyk, *Diffusion in Networks*, „Journal of Telecommunications and Information Technology" 2012, nr 2, s. 99–106; tenże, *Modele ewolucji systemów złożonych i metody badania ich charakterystyk dla potrzeb komputerowej identyfikacji potencjalnych sytuacji kryzysowych*, 2012 r., Wojskowa Akademia Techniczna, praca doktorska.

[37] J. Watson, *Wprowadzenie do teorii gier*, Warszawa 2011.

[38] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational*…

strategiczną można opisać za pomocą: struktury refleksyjnej (ang. *reflexive structure*), równowagi refleksyjnej oraz sterowania refleksyjnego[39].

Model gier refleksyjnych

Zgodnie z wcześniejszymi rozważaniami idea sterowania refleksyjnego opiera się na budowaniu przez każdego z graczy subiektywnych obrazów rzeczywistości. Ten proces może zostać opisany za pomocą modelu zwanego *grą refleksyjną* Γ_I, w którym to pojęcie jest definiowane jako następująca krotka[40]:

$$\Gamma_I = \{N, (X_i)_{i\epsilon N}, f_i(\cdot)_{i\epsilon N}, I\}$$

gdzie:
N = {1, 2, …, n} – zbiór graczy (agentów);
X_i – zbiór możliwych akcji gracza *i*;
$f_i(\cdot):\Theta\times X' \rightarrow R^1$ – funkcja wypłaty gracza *i*, jako iloczyn kartezjański na zbiorze wartości parametrów Θ (nieokreślonych jednoznacznie co do wartości) oraz *X'* zbiorze akcji;
I – struktura świadomości[41].

Szerszego wyjaśnienia wymaga struktura świadomości. Załóżmy, że nieokreślony (co do wartości) parametr będzie oznaczany symbolem θ, dodatkowo $\theta \in \Theta$. Przez symbol Θ jest rozumiany zbiór wspólnej wiedzy dla każdego z graczy. Zawiera on wszystkie możliwe wartości parametrów θ. Struktura świadomości gracza *i* zawiera następujące elementy:

- przekonanie gracza *i* na temat wartości parametru; jest ono oznaczane przez θ_i, gdzie $\theta \in \Theta$;
- przekonanie gracza *i* o przekonaniach innego z graczy na temat wartości parametru θ; jest ono oznaczane przez θ_{ij}, gdzie $\theta_{ij} \in \Theta$ oraz $j \in N$;
- przekonanie gracza *i* o przekonaniach gracza *j* oraz o przekonaniach innego z graczy na temat wartości parametru θ; jest ono oznaczane przez θ_{ijk}, gdzie $\theta_{ijk} \in \Theta$ oraz $k \in N$. Jak można zauważyć ten proces może być rozwijany w nieskończoność[42].

Należy dodać, że struktury świadomości wszystkich graczy składają się na strukturę świadomości danej gry. Zaznaczenia wymaga fakt, że żaden z graczy nie ma pełnej

[39] Tamże.

[40] Krotka – struktura danych będąca odzwierciedleniem matematycznej n-ki, tj. uporządkowanego ciągu wartości. Za: Wikipedia [dostęp: 26 III 2021] – przyp. red.

[41] D.A. Novikov, A.G. Chkhartishvili, *Mathematical Models of Informational*…

[42] Tamże.

wiedzy składającej się na strukturę świadomości. Struktura świadomości jest nazywana także strukturą informacyjną lub hierarchią przekonań.

Równowaga informacyjna a sterowanie informacyjne

Novikov i Chkhartishvili wprowadzili w swoim artykule także pojęcie równowaga informacyjna (ang. *information equilibrium*), które zawiera dane:

- o skończonej liczbie realnych graczy oraz graczy fantomowych, tzn. wyobrażeń na temat graczy w umysłach ich przeciwników;
- o tym, że dwóch agentów o identycznej strukturze świadomości podejmie taką samą decyzję lub akcję;
- o tym, że każdy z agentów dąży do maksymalizacji swojej wypłaty przez odpowiednio wybrane akcje[43].

Należy dodać, że w tym celu gracze wykorzystują przekonania o innych graczach, podstawiając wyobrażenia o ich możliwych akcjach do swojej funkcji celu. Co więcej, świadomość na temat oponentów danego gracza będzie się zmieniać. Dzieje się tak dzięki połączeniu wiedzy o ich aktualnych działaniach oraz przekonań danego gracza na ich temat.

Na podstawie pojęcia równowagi informacyjnej została sformułowana definicja sterowania informacyjnego. Polega ono na odpowiednim manipulowaniu świadomością (w istocie strukturą świadomości) oponentów. Wynikiem tej manipulacji jest osiągnięcie pożądanej równowagi informacyjnej, która jest jednym z możliwych rozwiązań gry[44]. Innymi słowy, zmanipulowany gracz podejmie decyzje, które będą korzystne dla jego przeciwnika.

Struktura, równowaga refleksyjna a sterowanie refleksyjne

Alternatywną formą refleksji jest refleksja strategiczna, która może zostać opisana za pomocą struktury oraz równowagi refleksyjnej.

Istnieje wiele modeli refleksji strategicznej, jednak mogą one zostać uogólnione do modelu opisanego za pomocą poniższej funkcji celu:

$$w_i(x_{-i}^t) = \arg \max_{y \in \mathcal{R}^1} F_i(y, x_{-i}^t)$$

gdzie:

$w_i(x_{-i}^t)$ – funkcja wypłaty w zależności od akcji oponentów i-tego gracza w chwili t;

y – akcja i-tego gracza;

F_i – funkcja celu i-tego gracza[45].

---

[43] Tamże.

[44] Tamże.

[45] Tamże.

Jak można zauważyć, decyzja oraz wypłata i-tego gracza nie zależy od poprzednich akcji graczy, jak ma to miejsce w teorii zbiorowego zachowania. Zależą one jedynie od subiektywnej oceny działań graczy na podstawie refleksji. Dlatego też Novikov i Chkhartishvili wprowadzili pojęcie refleksyjny podział zbioru graczy ℵ, dzielącego graczy na podstawie poziomu ich refleksji. Poniżej została przedstawiona definicja refleksyjnego podziału zbioru:

$$\aleph = \{N_0, N_1, \dots, N_m\}$$

gdzie:
N_i – zbiór graczy o poziomie refleksji *i*, *i = 1, …, m*, gdzie *m* oznacza maksymalny poziom refleksji danego gracza[46].

Należy dodać, że gracz o poziomie refleksji *i* uznaje, że każdy z jego oponentów jest na poziomie refleksji co najmniej o jeden mniejszym, co obrazuje poniższy wzór:

$$\aleph_{jk} = \{N_0, N_1, \dots, N_{k-2}, N_{k-1} \cup N_k \cup \dots \cup N_m \setminus \{j\}, j \in N_k\}$$

gdzie:
$\aleph_{jk}$ – subiektywny podział zbioru gracza *j* o poziomie refleksji *k*.

Takie założenie prowadzi do błędnej klasyfikacji oponentów o poziomie refleksji *k* do zbioru o poziomie refleksji *k*–1. Autorzy przedstawili w swoim artykule także równania opisujące sposób wyboru akcji przez gracza o każdym poziomie refleksji[47].

Strukturą refleksyjną jest nazywany zbiór subiektywnych, refleksyjnych podziałów zbioru wszystkich graczy. Należy dodać, że struktura świadomości może być jednoznacznie zdefiniowana także przez refleksyjny podział zbioru ℵ. Terminem równowaga refleksyjna jest opisywany zbiór akcji graczy, który tworzy najlepsze odpowiedzi na akcje oponentów, w odniesieniu do istniejącej struktury refleksyjnej w umysłach graczy. Ten zbiór może być przedstawiany także jako następujący wektor kolejnych akcji graczy[48]:

$$x^*(\aleph) = \{xk_j^*(\aleph_{jk})\}_{j \in N_k, k=0,\dots,m}$$

[46] Tamże.

[47] Tamże.

[48] Tamże.

Trzeba nadmienić, że równowaga refleksyjna istnieje zawsze. Jednak akcje poszczególnych graczy nie zawsze są najlepszymi odpowiedziami. Wynika to z różnic w poziomie refleksji graczy, błędach w ich klasyfikacji oraz rozbieżności w wiedzy graczy[49].

Definicja sterowania refleksyjnego może zostać sformułowana w analogii do definicji sterowania informacyjnego. Polega ono na odpowiedniej manipulacji refleksyjnymi podziałami zbioru graczy przez jednego z nich. Celem manipulacji jest zmiana zasad podejmowania decyzji przez oponentów, co w konsekwencji prowadzi do wykonania przez nich akcji zakładanej przez agresora. Oczywiście akcje wykonane przez oponentów różnią się od wyobrażeń danych graczy na ich temat. Stąd w każdej iteracji gracze modyfikują swoje wyobrażenia na temat innych graczy, przez co udoskonalają swoje przyszłe decyzje.

Budowa modelu operacji informacyjnych z wykorzystaniem teorii sterowania refleksyjnego

Większość modeli, które pozwalają na modelowanie wojny informacyjnej oraz operacji informacyjnych, ma swoje fundamenty w teorii gier. Szczególnym przykładem modelowania sytuacji strategicznych z niepełną wiedzą jej uczestników jest model hipergier. Alternatywnym podejściem jest wcześniej opisana koncepcja gry refleksyjnej zaproponowana przez Lefebvre'a. Połączenie pojęć refleksji informacyjnej, strategicznej, sterowania informacyjnego i refleksyjnego z teorią gier refleksyjnych pozwala na uzyskanie złożonego modelu, który umożliwia formalny opis operacji informacyjnych. Próba połączenia wspomnianych zagadnień zostanie przedstawiona poniżej.

Przedstawienie ogólnego modelu

Teoria sterowania wprowadza podział obiektów biorących udział w procesie sterowania na podmioty aktywne, tj. istoty ludzkie, grupy czy społeczności, oraz systemy pasywne np. urządzenia techniczne[50]. Model opisany poniżej będzie odnosił się jedynie do grupy podmiotów aktywnych.

Pierwszym z najważniejszych elementów modelu jest skończony zbiór graczy. W jego skład wchodzą wszystkie osoby bądź społeczności biorące udział w operacji informacyjnej. Kolejnym elementem są preferencje graczy reprezentowane przez wspomnianą wcześniej funkcję lub ogólnie zbiór funkcji wypłat, przypisany każdemu z graczy. Następną składową modelu jest zbiór możliwych akcji, które mogą być podjęte przez graczy. W szczególnym przypadku do opisu akcji, którymi dysponuje dany gracz, może być wymagane przedstawienie zbioru akcji i-tego gracza, innymi słowy nie wszyscy gracze muszą dysponować takimi samymi umiejętnościami. Jak wiadomo, decyzje

[49] Tamże.

[50] Tamże.

strategiczne, które składają się na operacje informacyjne, są podejmowane na podstawie pozyskanych wcześniej informacji. Stąd model operacji informacyjnych powinien umożliwiać opis wiedzy każdego z graczy na temat kluczowych parametrów (dokładnie ich wartości). W teorii gier refleksyjnych ta składowa jest nazywana strukturą świadomości. Oczywiście dana operacja informacyjna nie składa się z jednej czynności albo akcji. Dlatego model powinien umożliwiać opis sekwencji czynności podejmowanych przez graczy. Składnikiem modelu, który rozszerza typowy model gier refleksyjnych, jest podział refleksyjny zbioru, a dokładnie jego podział przedstawiający wzajemną ocenę graczy co do poziomu swojej refleksji. Kolejnym ważnym rozszerzeniem modelu jest przedstawienie powiązania między strukturą świadomości, podziałem refleksyjnym zbioru a akcjami podejmowanymi przez graczy. W zależności od poziomu refleksji, postrzegania poziomu refleksji innych graczy oraz wiedzy na temat zasadniczych parametrów gry gracz podejmie inną decyzję. Warto także dodać, że zazwyczaj nie można wskazać dwóch graczy o takiej samej strukturze świadomości oraz podziale refleksyjnym. Potwierdza to przytoczone wcześniej stwierdzenia o istnieniu odrębnych subiektywnych rzeczywistości dla każdego z graczy. W przypadku gdy gracz jest pewny zdobytych informacji, modyfikuje swoją strukturę świadomości, co pozwala mu na podejmowanie lepszych decyzji. Gracze za pomocą akcji oddziałują na postrzeganie przeciwników w celu uzyskania przewagi. Należy także założyć, że niektóre akcje wchodzące w skład modelu opisują proces komunikacji między graczami. Ważnym czynnikiem jest również możliwość opisu częstości występowania akcji za pomocą prawdopodobieństwa. Połączenie struktury świadomości oraz podziału refleksyjnego będzie nazywane zunifikowaną strukturą świadomości. Natomiast gry opisane powyższym modelem będą nazywane macierzowymi grami refleksyjnymi. Ta gra jest definiowana przez następującą krotkę:

$$\Gamma_U = \{N, (W_i)_{i\epsilon N}, (X_i)_{i\epsilon N}, (c_i)_{i\epsilon C}, (A_i)_{i\epsilon N}, (\aleph_i)_{i\epsilon N}\}$$

gdzie:

N = {1, 2, …, n} – zbiór graczy (agentów);

$W_i = \{w_{i1}, w_{i2}, \ldots, w_{ik}\}$ – zbiór funkcji wypłat (preferencji) i-tego gracza, gdzie w_{ij}: $\Theta \times \aleph \times X \rightarrow R^1$, tzn. j-ta funkcja wypłaty gracza i jako iloczyn kartezjański na zbiorze wartości parametrów Θ (nieustalonych jednoznacznie co do wartości), pewnym podziale refleksyjnym $\aleph$ oraz zbiorze akcji X, a k jest równe liczbie funkcji wypłat dla każdego z graczy;

$X_i = \{x_{i1}, \ldots, x_l\}$ – zbiór możliwych akcji gracza i będący podzbiorem zbioru X, gdzie x_i – i-ta akcja;

$c_i = \langle <x_1, p_1>, <x_2, p_2>, \ldots, <x_l, p_l> \rangle$ – i-ta n-tka kolejnych akcji gracza wraz z ich prawdopodobieństwami wystąpienia (sekwencji czynności). Każda oryginalna n-tka będzie nazywana charakterem gracza, gdzie zbiór charakterów graczy będzie oznaczany symbolem C. Należy także dodać, że $L = |X|$, $l \leq L$ oraz $p_i \in <0,1>$; gdzie $L = |X|$ nazywamy mocą zbioru X;

$A_i = [a_{jk}]_{n \times n}$ – struktura świadomości i-tego gracza, gdzie:

$$a_{wk} = \begin{cases} \theta_{jk} \in \Theta \; jeżeli \; znany \\ - \; w \; przeciwnym \; wypadku \end{cases}$$

$\aleph_i = [n_{jk}]_{n \times n}$ – podział refleksyjny i-tego gracza, gdzie: $n_{jk} \in \{0,1, \ldots, m\}$; m to maksymalny poziom refleksji dostępny graczom, istnieje także ograniczenie takie, że $\forall_{n_{ii}, n_{i-} \in N}\ n_{ii} > n_{i-}$.

Analogicznie do równowagi refleksyjnej oraz sterowania refleksyjnego można zdefiniować zunifikowaną równowagę refleksyjną, która wyznacza najlepsze odpowiedzi (akcje) gracza w odniesieniu do konkretnej zunifikowanej struktury świadomości, tzn. połączenia konkretnej struktury świadomości A_i oraz podziału refleksyjnego $\aleph_i$, danego gracza. Natomiast wpływ na struktury świadomości oraz podziały refleksyjne przeciwników w celu osiągnięcia założonej wcześniej zunifikowanej równowagi refleksyjnej może być nazywany zunifikowanym sterowaniem refleksyjnym.

Opis gry p-Beauty Contest Game *za pomocą modelu*

W podstawowej wersji tej gry każdy z jej uczestników wybiera liczbę z przedziału od 0 do 100. Następnie jest wyznaczana średnia z wyników, którą mnoży się przez współczynnik *p*. Gracz, który podał liczbę najbliższą wynikowi, wygrywa daną rundę[51]. W przypadku remisu gracze, którzy podali taką samą liczbę, uzyskują wygraną *ex aequo*. Na koniec każdej rundy gracze dowiadują się o wyniku oraz wyborach swoich przeciwników – jest to gra z tzw. pełną informacją. Istnieją także alternatywne wersje gry, tj. gry z niepełną wiadomością, w których gracze dowiadują się jedynie o swojej wygranej lub przegranej. Najbardziej skrajnym przykładem gry jest sytuacja, w której gracze nie otrzymują żadnej wiadomości na koniec rundy.

Aby opisać p-Beauty Contest Game za pomocą przedstawionego wcześniej modelu, należy zdefiniować wszystkie elementy składające się na krotkę Γ_U ze wzoru macierzowych gier refleksyjnych. Pierwszym, najważniejszym elementem jest zbiór graczy (podmiotów) uczestniczących w grze *N*.

$$N = \{1,2, \ldots, n\}$$

gdzie:
n = 6.

W klasycznym podejściu funkcja wypłat wskazuje hierarchię rozwiązań danej gry, które w ocenie danego gracza są dla niego najlepsze. W przypadku gier z niepełną wiedzą oraz wielu ruchów, które dany gracz może wykonać, dobrym podejściem jest opis jego preferencji w odniesieniu do znanych parametrów. W przypadku p-Beauty Contest Game funkcja preferencji dla wszystkich racjonalnych graczy będzie wyglądać następująco:

[51] S. Skeath, J.A. Livingston, *A Step Ahead? Experienced Play in the p-Beauty Game*, https://ssrn.com/abstract=1680542.

$$\mathrm{w}_i = \arg \min_{x_i \in <0,100>} \left| \frac{p \sum x_{i*}}{n-p} - x_i \right|$$

gdzie:
p – parametr, przez który jest mnożona średnia z liczb podanych przez graczy;
x_i – wybór i-go gracza, który jest zarówno parametrem funkcji optymalizacji;
$\sum x_{i*}$ – suma wyborów przeciwników i-tego gracza wyznaczona na podstawie informacji posiadanych przez tego gracza;
n – liczność zbioru graczy biorących udział w grze.

Na podstawie wzoru można zauważyć, że każdy gracz stara się dokonać wyboru, który zminimalizuje różnicę między średnią swoich oponentów a własnym wyborem. Takie podejście gwarantuje wygraną w danej rundzie. Należy przyjąć, że za każdą wygraną dany gracz otrzymuje jeden punkt.

Kolejnym elementem modelu wymagającym zdefiniowania są akcje, które mogą zostać podjęte przez graczy. Zgodnie z założeniami ogólnego modelu gracz nie musi dysponować wszystkimi dostępnymi akcjami.

Poniżej zostaną wymienione wszystkie akcje. Będą one unikalnie definiowane przez numer akcji:

- wybór liczby – numer akcji 1;
- wykonanie refleksji – numer akcji 2;
- poprawna podpowiedź co do swojego wyboru – numer akcji 3;
- niepoprawna podpowiedź co do swojego wyboru – numer akcji 4;
- podglądanie wyborów innych graczy – numer akcji 5;
- zaniżanie wyniku gry – numer akcji 6;
- zawyżanie wyniku gry – numer akcji 7.

Następnie zostanie zaprezentowany opis zbiorów akcji dostępnych dla graczy:
$X_1 = \{1,2,5\}$;
$X_2 = \{1,6\}$;
$X_3 = \{1,7\}$;
$X_4 = \{1,2,3\}$;
$X_5 = \{1,2,4\}$;
$X_6 = \{1,2\}$.

Jak można zauważyć, każdy z powyższych graczy ma inny zbiór akcji, stąd należy zdefiniować tyle samo sekwencji czynności, tzn. charakterów graczy.

$c_1 = \langle <2; 1>, <6; 1>, <2; 1>, <1; 1> \rangle$;
$c_2 = \langle <7; 0.5>, <1; 1> \rangle$;
$c_3 = \langle <8; 0.5>, <1; 1> \rangle$;
$c_4 = \langle <2; 1>, <4; 0.5>, <2; 1>, <1; 1> \rangle$;
$c_5 = \langle <2; 1>, <5; 0.5>, <2; 1>, <1; 1> \rangle$;
$c_6 = \langle <2; 1>, <2; 1>, <1; 1> \rangle$.

Kolejnym elementem, który wymaga zdefiniowania, jest struktura świadomości każdego gracza. Zgodnie z ogólnym modelem w tym celu należy zbudować dla każdego z graczy macierz o wymiarach n x n określającą ich świadomość. Przykładowa macierz dla gracza pierwszego zostanie zaprezentowana poniżej.

$$A_1 = \begin{bmatrix} 67 & 42 & 16 & 28 & 17 & 10 \\ - & 42 & - & - & - & - \\ - & - & 16 & - & - & - \\ - & - & - & 28 & - & - \\ - & - & - & - & 17 & - \\ - & - & - & - & - & 10 \end{bmatrix}$$

Element $a_{11} = 67$ należy rozumieć jako wybór gracza pierwszego, element a_{12} jako wybór gracza drugiego z perspektywy gracza pierwszego. Natomiast elementy $a_{22} = 42$ lub $a_{33} = 22$ obrazują, jak gracz pierwszy wyobraża sobie wybór gracza drugiego oraz trzeciego. Z macierzy można także odczytać, że gracz pierwszy nie jest świadomy oceny wyborów przeciwników przez innych graczy. Macierze reprezentujące strukturę kolejnych graczy są budowane w analogiczny sposób. Oczywiście macierz świadomości może zostać zmodyfikowana w procesie operacji informacyjnej. Ostatnim elementem składającym się na model gry jest refleksyjny podział zbioru graczy, który opisuje subiektywną ocenę poziomów refleksji przeciwników danego gracza. Należy także założyć maksymalny poziom refleksji graczy, który w tym wypadku będzie równy $m = 5$. Macierz przedstawiająca refleksyjny podział zbioru z perspektywy gracza pierwszego przedstawia się następująco.

$$\aleph_1 = \begin{bmatrix} 5 & 2 & 1 & 4 & 3 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 2 & 4 \\ 2 & 0 & 2 & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Zgodnie z założeniami dany gracz uważa, że jego przeciwnicy są na poziomie refleksji co najmniej o jeden niższym niż jego własny poziom refleksji. Dlatego też na podstawie subiektywnej oceny gracz może wydedukować możliwą wersję ocen poziomów refleksji swoich przeciwników o innych graczach. Ten sposób pozwala na przedstawienie, jak dany gracz ocenia innych graczy $a_{12} = 1$, $a_{13} = 1$, oraz postrzeganie poziomów refleksji przez innych, np. ocena poziomu refleksji gracza trzeciego przez gracza drugiego z perspektywy gracza pierwszego $a_{23} = 1$.

Wnioski

Techniki wojny informacyjnej oraz operacji informacyjnych, jakkolwiek inaczej nazywane, były znane już w starożytnych Chinach, imperium mongolskim czy Macedonii rządzonej przez Aleksandra Wielkiego. Charakter wojen informacyjnych oraz operacji informacyjnych będzie nadal ściśle zależał od rozwoju nauki oraz technologii.

Ten temat jest zagadnieniem interdyscyplinarnym oraz wieloaspektowym, co dodatkowo komplikuje jego skuteczną analizę.

Badania nad tym zjawiskiem są niezbędne w celu jego poznania, późniejszej identyfikacji oraz opracowania metod przeciwdziałania. Niniejszy artykuł jest próbą modelowego podejścia do opisu zjawiska, jakim jest wojna informacyjna. Główne założenie zostało zrealizowane przez zbudowanie modelu operacji informacyjnych.

Zaproponowany w pracy model macierzowych gier refleksyjnych jest połączeniem teorii gier, teorii sterowania refleksyjnego, refleksji informacyjnej oraz strategicznej. Pozwala na szczegółowy opis elementów niezbędnych do przedstawienia procesu operacji informacyjnych. Użyteczność modelu została zweryfikowana przez jego użycie do opisu gry p-Beauty Contest Game.

W literaturze przedmiotu istnieje wiele opisów jakościowych. Opis ilościowy w postaci modelu macierzowych gier refleksyjnych oraz zastosowanie technik symulacji pozwalają jednak na łatwiejsze rozpoznanie wszelkich aspektów składających się na zjawisko operacji informacyjnych.

Bibliografia

Kasprzyk R., *Diffusion in Networks*, „Journal of Telecommunications and Information Technology" 2012, nr 2, s. 99–106.

Kasprzyk R., *Modele ewolucji systemów złożonych i metody badania ich charakterystyk dla potrzeb komputerowej identyfikacji potencjalnych sytuacji kryzysowych*, 2012 r., Wojskowa Akademia Techniczna, praca doktorska.

Kasprzyk R., *The Essence of Reflexive Control and Diffusion of Information in the Context of Information Environment Security*, w: *Internetional Conference in Intelligent Systems in Production Engineering, and Maintenance. ISPEM 2018. Advances in Intelligent Systems and Computing*, t. 835, A. Burduk i in. (red.), Cham 2018, Springer, s. 720–728.

Lefebvre V.A., *Sketch of Reflexive Game Theory*, Irvine 1998, University of California School of Social Sciences.

Mazur M., *Jakościowa teoria informacji*, Warszawa 1970, Wydawnictwa Naukowo-Techniczne.

Mazur M., *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966, Państwowe Wydawnictwo Naukowe.

Mikhailov A.P, Marevtseva N.A., *Models of Information Warfare*, „Mathematical Models and Computer Simulations" 2012, nr 3, s. 251–259.

Nowacki G., *Współczesne poglądy na prowadzenie walki informacyjnej. Studium teoretyczne*, Warszawa 2001, Akademia Obrony Narodowej.

Novikov D.A., Chkhartishvili A.G., *Mathematical Models of Informational and Strategic Reflexion: a Survey*, „Advances in Systems Science and Application" 2014, nr 3, s. 254–278.

S. Skeath, J.A. Livingston, *A Step Ahead? Experienced Play in the p-Beauty Game*, https://ssrn.com/abstract=1680542.

Słownik języka polskiego, https://sjp.pwn.pl/szukaj/refleksja.html [dostęp: 8 IV 2019].

Watson J., *Wprowadzenie do teorii gier*, Warszawa 2011, Wolters Kluwer Polska.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-ee571f3e-2942-46ce-9e-19-af8e970c6f7a [dostęp: 30 III 2019].

Abstrakt

Współczesne społeczeństwa są często określane mianem społeczeństw informacyjnych. Dzięki rozwojowi sieci Internet praktycznie każda osoba na kuli ziemskiej może zdobyć potrzebne informacje. Ta możliwość jest zarazem wadą i zaletą. Informacja jest coraz częściej traktowana jako kolejny rodzaj broni, który może zostać wykorzystany do realizacji określonych celów. Jednak już od dawna posługiwano się nią w celach militarnych oraz politycznych przez dezinformację, propagandę czy prowadzenie wywiadu. Rozwój technologii nadał konfliktowi informacyjnemu jedynie inną formę. Działania wchodzące w skład operacji informacyjnych są ukierunkowane na wywarcie wpływu przez podmiot sterujący na podmiot sterowany, w celu wykonania przez niego czynności wcześniej założonej przez podmiot sterujący. Celem tego rodzaju konfliktów nie jest przejęcie danego terytorium, skupiają się one na świadomości danego społeczeństwa. Dlatego też należy się zastanowić nad sposobami oraz możliwościami modelowania oraz symulacji sytuacji strategicznych z niepełną wiedzą, jakimi są operacje informacyjne. Jedno z podejść do modelowania operacji informacyjnych jest opisane w teorii sterowania refleksyjnego, która opisuje również techniki ich prowadzenia. W artykule przedstawiono koncept sterowania refleksyjnego oraz model zbudowany na jego podstawie.

Słowa kluczowe: operacje informacyjne, sterowanie refleksyjne, modelowanie operacji informacyjnych.

Information operation modeling using reflexive control theory

Abstract

Modern societies are often referred to as information societies. Thanks to the development of the Internet, virtually every person on the globe can get the information they need. This possibility is both a disadvantage and an advantage. Information is increasingly used as another kind of weapon that can be used to achieve specific goals. However, it has long been used for military and political purposes through disinformation, propaganda and intelligence. The development of technology has only given information conflict a different form. Actions involved in information operations are aimed at exerting influence by the controlling entity on the controlled entity in order to perform an action previously assumed by the controlling entity. The purpose of this type of conflict is not to take over a given territory; they focus on the consciousness of a given society. Hence, it is necessary to consider the ways and possibilities of modeling and simulating strategic situations with incomplete knowledge, which are information operations. One of the approaches to modeling information operations is constituted by the theory of reflexive control, which at the same time describes the techniques of conducting them. The article presents the concept of reflexive control and the model built on its basis.

Keywords: information operations, reflexive control, information operation modeling.

V

WYBRANE ARTYKUŁY W JĘZYKU ANGIELSKIM

SELECTED ARTICLES IN ENGLISH

Krzysztof Izak
Orcid: 0000-0001-9815-6035

DOI: 10.4467/20801335PBW.21.017.13574

Changes in the perception of immigration, integration, multiculturalism and threats of Islamic radicalism in certain EU member states

The concepts of integration, assimilation and multiculturalism have become highly popular in the present century[1]. This is the result of the influx of immigrants to Europe, which resembles a sine wave – a curve showing the increase or decrease in migration flows to our continent. This phenomenon was at its greatest in 2015, compounding the problems and threats that had already emerged. The study of them is the purpose of this article. The author will also answer the question of whether the actions taken by the authorities to solve the problems and counteract them could have the desired effect and contribute to calming the public mood, and if so, to what extent. Or whether, on the contrary, these activities may lead to even greater antagonisation of various social groups, and thus to their radicalisation.

The research assumptions of the article focus on problems important for the present and future of Europe related to the migration to our continent of citizens of Muslim countries, who are not always able or willing to integrate with the inhabitants of the host countries. The author also draws attention to the changing attitude of the authorities of selected EU countries to the integration and multicultural projects implemented over the years. There were numerous criticisms of the concept of integration policy, connected with the belief the adaptation of foreigners to European society was ineffective. Some states have begun to officially withdraw from immigrant projects and dismiss the public discussion related to multiculturalism, which proves the failure of the concept of the integration policy of Muslim immigrants. These actions were accompanied by the religious radicalisation of Muslim minorities leading to

[1] These concepts have been defined and analysed in several publications. The author refers to the book by Janusz Balicki, *Imigranci z krajów muzułmańskich w Unii Europejskiej. Wyzwania dla polityki integracyjnej*, Warszawa 2010.

acts of brutal violence. After many years of distracting the public from the essence of the threat, it sparked a harsh response from several governments in the EU, other than Brussels itself. Studying the above problems, the author used the following methods to analyse this phenomenon: historical – allowing to understand changes taking place in immigrant environments, behavioural – which is understood as the behaviour of individuals and social groups, and comparative – showing changes in the reaction of state authorities to threats from the radicalised part of Muslim minorities.

Manifestations and effects of the policy of multiculturalism

In France the negative effects of social changes caused, among others, by the policies of successive governments towards immigration and the welfare system of the state are conspicuous. They derive from, among others, ideas propagated by the French left, which for years has been portraying the immigrants from former colonies only as victims of harm caused by the French state. The latter in turn awakens among the immigrants revendicating and demanding attitudes and contributes to the formation of an aversion towards the host country. France is the country with the largest Muslim population in the European Union. It is also the country most threatened by terrorism in the EU. According to official data, there are 6 million Muslims in France (with a population of 70 million), and according to other sources, there may be between 8 and 10 million of them[2].

The history of terrorism in France is very long[3]. After World War II, it was associated with the Algerian War of Independence. After its end, more than a million people had to leave Algeria. According to the French historian Alain Besançon, the first president of the 5th Republic, General Charles de Gaulle (1959–1969), preferred to surrender Algeria rather than admit too many Muslims to the French society. De Gaulle opposed keeping French Algeria because he feared that France's demographic balance would be undermined by an excessive number of Muslims. He did not yield to the supporters of French Algeria, many of whom were Gaullists, such as Prime Minister Michel Debré. It was only under the rule of Georges Pompidou (1969–1974) and Valery Giscard d'Estaing (1974–1981) that Muslim immigration gained momentum. It should be noted, however, that all the political forces of France contributed to the welcoming of Muslims. Religious communities – Catholics, Protestants, and Jews – wanted to show that they were open to others, entrepreneurs were looking for cheap labour, the left

[2] M. Widy, *Życie codzienne w muzułmańskim Paryżu*, Warszawa 2005, p. 22. Many contemporary publications still give the number of 6 million Muslims in France. Thus, the population of French Muslims has remained stable for the past 15 years, when this figure was first reported. Such a figure seems unreliable. The estimates, characterised by significant discrepancies, result from the fact that in France, during the censuses, it is forbidden to ask about the religion of the respondent.

[3] The 13 July 1793, when the Girondist Charlotte Corday stabbed to death the Jacobin tribune, Jean-Paul Marat, is considered the beginning of terrorism in the industrial society.

wing did it in the name of humanitarian ideas, while the right wing wanted to maintain ties with former colonies[4].

In the 1990s, France began to face the Islamic extremism. It was spread mainly by Frenchmen of Algerian origin, who opposed the authorities because the French government supported the military regime in Algeria in the ongoing civil war with Islamists. At that time, a large group of refugees came to France from Algeria, who, like the previous immigrants, settled in apartment blocks on the outskirts of large cities. In these districts, back in the 1960s and 1970s, flats were built for local and foreign workers in tower blocks, popularly known as housing at moderate rent (fr. *habitation à loyer modéré* or HLM). Over the years, the French moved out to better apartments or their own homes. Educated, integrated and enriched foreigners did the same[5]. Imams and missionaries who travelled from Muslim countries to France and other Western European countries at that time were involved in preaching the teachings of Islam. However, they found it difficult to convince immigrant workers to obey Islam because they did not know their life problems. Moreover, the immigrants were more concerned with providing for their families than with satisfying their spiritual needs. The first generation of immigrants also took care of educating the many children growing up in European culture and thus fulfilled the assumptions of the policy of social inclusion.

France is an example of a country associated with the immigrant assimilation model as are other countries, incl. Germany. In the countries of Western Europe, it was believed that by the end of the 20th century all newcomers would be assimilated with their new environment. It was supposed to take two or even three generations. However, some began to question such assumptions. According to them, even in the next generation, the cultural difference between immigrants and their children and the environment will not disappear completely. It could also be observed that they are aware that full integration with society and participation in state institutions does not require immigrants to give up their own identity. In the French Jacobin tradition, the main emphasis is on the individual relationship between citizen and state, without intermediaries. This model assumes that immigrants will achieve a high level of cultural adaptation to the new environment. Those who do so have many opportunities, while others risk being marginalised. It turned out that most of them had been marginalised[6].

The situation changed after 1989, considered to be the apogee of the expansion of the fundamentalist movement until the beginning of the 21st century. The generation of immigrant children then reached adulthood. It was already familiar with European

---

[4] J. Bielecki, *Nie przyjaźnię się z żadnym muzułmaninem*, https://www.rp.pl/artykul/1171826-Nie-przyjaznie-sie-z-zadnym-muzulmaninem.html [access: 16 I 2015].

[5] J. Kubera, *Francuzi, Algierczycy? Relacje między identyfikacjami Francuzów algierskiego pochodzenia*, Toruń 2017, pp. 381–383. Similar estates were built in West Germany for Turkish workers, the so-called *gastarbeiter* (in German: guest workers). The German authorities assumed that they would return to the native country after ending their employment, but in the meantime, for various reasons, they stayed and brought their families.

[6] J. Balicki, *Imigranci z krajów muzułmańskich*…, p. 27.

culture and was exposed to numerous social obstacles, including in the labour market, which were often caused by school failures. It was in this environment that for the first time in Western Europe a group of poor Muslim urban youth emerged, which turned out to be more susceptible to the calls of fundamentalist activists than their parents. The fundamentalist ideology penetrated the new generation all the easier because the integration policy failed. In France, there were movements, like: S.O.S. Racism, which was to connect young people from all walks of life in a great anti-racist outburst, and Rebeu[7]. The latter tried to change the mentality of young Frenchmen of Arab origin that would correspond to their bicultural identity. It turned out, however, that young people were more susceptible to the influence of Muslim preachers and missionaries than to Western culture. Organisations derived from the Al-Ichwan al-Muslimin (Muslim Brothers), Jama'at-e Islami Pakistan (the Muslim Party of Pakistan) and the Turkish Refah Partisi (the Welfare Party), well-established in Europe, have adapted their message to the needs of this part of the youth which was quickly re-Islamised. On this occasion, conversion to Islam flourished in languages such as French, English, German as well as Polish. The works of Muslim theoreticians of political Islam and jihad: Sayyid Qutb and Abu al-Ala al-Maududi were translated into these languages[8]. At the same time, the agitation went beyond the range of Muslim communities. The inhabitants of Paris found leaflets in their mailboxes that read: *We Muslims will take over France, just as you once colonised Algeria. French families have one child each, while we give birth to five. In twenty years, we will be controlling France*[9].

The process of converting and radicalising young people accelerated after 11 September 2001, which was a kind of turning point for contemporary terrorism. European jihadists began to travel to conflict zones in Iraq and Afghanistan. The spectacular return of jihadist terrorism to France took place in March 2012[10]. It coincided with the beginning of the great campaign that led to the election of François Hollande as president. Part of the victory was made by the masses of Muslims voting in his favour. This campaign was followed by parliamentary elections, in which for the first time more than 400 candidates of immigrant background, the vast majority of them Muslims, appeared. The followers of Islam voted for their candidates this time. This was strongly felt by deputy Jacques Myard, a French native who was seeking re-election in the Yvelines department near Paris. In the city of Satrouville, where a large number of Maghreb people live, Myard visited a local market. Here he was accosted by an Arab who instructed the deputy: *You have nothing to do here. This is Arab land. Muslim*

---

7 In French, a colloquial term for European-born people whose parents or grandparents were immigrants from the Maghreb.

8 G. Keppel, *Święta wojna. Ekspansja i upadek fundamentalizmu muzułmańskiego*, Warszawa 2003, pp. 204–205.

9 A. Pamuła, *Wrzenie. Francja na krawędzi*, Warszawa 2020, p. 369.

10 On 11th, 15th and 19th of March 2012, Mohammad Merah shot and killed seven people in Toulouse and seriously injured two.

land is not French land. You are a racist, a Zionist, and you should go away from here[11]. Thus, the results of political education, not social integration, were clearly revealed. A parallel society developed in France. The Muslim minority demanded unrestricted access to citizenship, the same rights as Christians and Jews, but maintaining religious distinctiveness and the resulting privileges, obviously disregarding the recognition of the principles of the secular state[12]. These privileges were granted during the Hollande's presidency (2012–2017), which significantly differed it from the presidency of Nicolas Sarkozy (2007–2012), who tried to restore relative "normality" in relations with the Muslim minority and control its claims. First of all, he proposed to end the traditional definition of the secular nature of the state, which simply meant excluding Christianity from public space. According to Sarkozy, France should no longer be cut off from its Christian roots. The secularism of the state was used by the followers of Islam, as it helped them spread its ideas. It is true that in 2004 the wearing of religious symbols, including Muslim veils, was banned in schools, but other elements of Muslim customs were introduced, including Halal food in educational institutions, gender separation in physical education lessons, burkinis in swimming pools and beaches, turning a blind eye to bigamy and circumcising girls, etc. These practices became common during the Hollande presidency. The then Socialist Interior Minister Manuel Valls spoke only of Islamophobia and anti-Semitism in parliament. At the same time, the acts of profaning Christian objects were understated or omitted. If there was a mosque profanation, voices calling racism and Islamophobia could be heard or anti-Semitism if synagogues or Jewish cemeteries were the object of vandalism. Churches and Christian cemeteries were devastated and profaned, which passed without much publicity. Every year the number of acts of anti-Semitism increases. In 2014, more than 850 of them were recorded in France, which is twice as many as in the previous year. Anti-Semitism by the followers of Islam differs from the actions of the extreme right. Right-wingers focused mainly on anti-Jewish propaganda, Muslims used robbery, violence with torture and even murder. No wonder that around 50,000 French Jews left for Israel between 2000 and 2017, the largest number (almost 20,000) after the attacks at the Hyper Cacher supermarket in January 2015[13]. The same year (13 November), assassinations at the editorial office of the weekly "Charlie Hebdo" and a series of the bloodiest attacks took place in Paris. Therefore, all the secularism of the state, instead of being a defence against violence by the followers of Islam, turned against France and its people. This is noticed by French intellectuals, but their statements and publications are met with hostility by Muslim activists and left-wing politicians and experts[14].

---

[11] B. Dobosz, *Emiraty francuskie*, Warszawa 2016, p. 176.

[12] G. Keppel, A. Jardin, *Terror we Francji. Geneza francuskiego dżihadu*, Warszawa 2017, p. 43.

[13] A. Pamuła, *Wrzenie. Francja na…*, p. 351.

[14] Georges Bensoussan and his book from 2002: *Les Territoires perdus de la République – antisémitisme, racisme et sexisme en milieu scolaire* (*Lost territories of the Republic – anti-Semitism, racism and sexism at school*) are worth mentioning. The author writes in it about the anti-Semitism of French

Germany is home to the second largest Muslim community in the EU. Unofficial statistics, including illegal and unregistered Muslims, suggest that even more than 7 million. Immigrants in this country cannot remember its colonial past[15]. Germany, on the other hand, opened up to immigrants, thus wanting to compensate foreigners for the crimes and wrongs of Nazism. Politicians made sure that the constitution of their country included provisions ensuring broadly understood tolerance. Germany also pursued the most liberal asylum policy in the world. Groups deemed to be terrorist were allowed to operate, raise funds and recruit new members; provided, however, that they were foreign terrorists, not native, German. Even planning a terrorist operation was not in itself illegal, as long as the attack was to take place abroad. The police were to focus their efforts on tracking down local right-wing extremists, and paid little attention to the groups of foreigners. There was a tacit agreement between the Germans and the radicals living in their country, whereby foreigners could do whatever they wanted, as long as they did not attack the citizens of their adopted country. In an attempt to break with its own past, Germany opened its doors wide to strangers.

Most of the Muslims in Federal Republic of Germany are Turkish citizens and Germans of Turkish origin in the second and third generations – children and grandchildren of Turkish workers who came to Germany in the 1960s and 1970s. Members of this large community sympathised from the beginning with the movement Hizmet (Service) founded by the renowned preacher Fethullah Gülen. The international mission of spreading Islam in the ideology typical of the Muslim Brothers was carried out under the slogans: *Let's build schools, not mosques* and *Our jihad is education*. It acted in a way that seemingly appeared to support interreligious and intercultural dialogue, lulling the authorities into a false sense of security. In Germany, the movement worked quietly but effectively, creating special schools, private gymnasiums and universities, local centres for the study of the *Koran* and the so-called Lichthäuser (germ. *lantern*), i.e. male collectives with strict discipline, total obedience, compulsory reading of the *Koran* and common prayers five times a day. Gülen promoted the creation of the public image of the ecumenical Islamic movement striving for

schoolchildren of Arab origin. In another publication by this author, *Une France soumis* (*France has succumbed*), published in 2017, he presents a sad picture of the state that allows its immigrant community to do anything. Renaud Camus in his work: *Le Grand Remplacement* (*The Great Exchange*), published in 2011, announced the replacement of white Europeans by the increasing number of immigrants from the Middle East and Africa. Bernard Rougier, in his study: *Les territoires conquis de l'islamisme* (*Conquered Territories of Islamism*), published in 2020, highlights immigrant neighbourhoods controlled by Muslim radicals. In the same year, Patrick Stefanini published the book *Immigration - Ces réalités qu'on nous cache* (*Immigration – the reality we hide*). Also, worth mentioning are the works of Michel Houellebecq and Gilles Kepel translated into Polish, and the publications of the Polish authors mentioned in the footnotes: Bogdan Dobosz, Marek Orzechowski and Anna Pamuła.

[15] After World War I, Germany lost its colonies in Africa: Togo, Cameroon, German South-West Africa (now Namibia) and German East Africa – Tanganyika, which is now the mainland of Tanzania.

international dialogue by establishing 15 associations of dialogue in Germany[16]. As a side note, it should be added that the Gülen's movement founded private educational institutions in Poland: the international Meridian school (a primary school, middle school and secondary school in Warsaw and a kindergarten and elementary school in Lodz) and the University of Economics and Information Technology. The owner of these educational institutions is Meridian Limited Company[17], which has branches in many countries. Gülen's followers were not preparing for armed jihad, but for language jihad, or missionary activity. Their activities are subtle and sophisticated to avoid being accused of spreading religious hatred and violence. This is to be the mission of spreading Islam extended in time, according to a sermon once given by Gülen to his disciples. This harmonious – it would seem – coexistence of Germans and Muslims and their integration, which was more of a wishful thinking than reality, was emphasised by President Christian Wulf, who during the momentous celebrations marking the 20th anniversary of the country's reunification said the following memorable words: *Christianity doubtless belongs in Germany. Judaism belongs doubtless in Germany. That is our Judeo-Christian history. But by now, Islam also belongs in Germany*. This speech first caused astonishment, but thanks to the propaganda efforts of the media and statements of politicians, they were socially accepted and analys[18].

The first prominent person in Germany who did not hesitate to criticise the existing state was Thilo Sarrazin. In 2010, his book was published: *Deutschland schafft sich ab: Wie wir unser Land aufs Spiel setzen* (*Germany Abolishes Itself: How we're putting our country at risk*), in which he stated that immigrants from Muslim countries cause more social costs to the state than they provide benefits to the economy. He refused to recognise as equal citizens those immigrants who live on state benefits, while at the same time reject the state and not care about the education of their children. He blamed this on Islam, which, in his opinion, stands in opposition to Europe's liberal values. The publication became a bestseller (1.5 million copies had been sold by the end of 2010) and sparked a nationwide debate about immigrants. The author suffered severe consequences. He was expelled from his party, the SPD, and forced to step down as a Bundesbank member. At the same time, pro-government media and Muslim associations launched an attack on Sarrazin, who was labelled, like many similar to him, an Islamophobe and racist. However, he won public support[19].

---

[16] *Media w USA ostro o przejęciu „Zaman": „Zamach Erdogana na prasę"*, 8 III 2016, https://wiadomosci.wp.pl/media-w-usa-ostro-o-przejeciu-zaman-zamach-erdogana-na-prase-6027417304052353a, [access: 19 VII 2016].

[17] A. Rusinek, *Nurt radykalny wśród społeczności muzułmańskich w wybranych państwach Unii Europejskiej*, Warszawa 2012, p. 213.

[18] M. Orzechowski, *Mój sąsiad islamista. Tunis–Paryż–Bruksela…*, 2nd edition updated, Warszawa 2016.

[19] P. Madajczyk, *Między fundamentalizmem a asymilacją. Muzułmanie w Niemczech*, Warszawa 2015, pp. 178–181.

In 2013, Recep Tayyip Erdoğan, while still the Prime Minister of Turkey, during his visit to Germany, warned the over three million Turkish minority against integrating with Germany, because Islam prohibits (according to the doctrine) intercourse with infidels. On the other hand, during a visit in 2015 to one of the exhibition halls in Karlsruhe, Erdoğan asked the nearly 14 thousand gathered supporters of the Turkish leader: *Do you want us, starting here in Germany, to build a new Turkey?* In response, he heard a resounding yes. Erdoğan emphasised then that the Pan-Turkish identity was supported by language and Islam. He explained to his countrymen: *You cannot learn German or English if you do not speak Turkish*[20]. During his speech, he also called the name of Allah several times and appealed for the Turkish communities in Germany to strengthen the global influence of Turkey, which had sent 900 imams to Germany. Each of them may legally reside and work in Muslim communities in Germany for five years. Some German politicians cautioned then against that Turkish imams and preachers in Germany were implementing the policy of the Turkish authorities and were loyal to their own country, not to the country of their residence[21]. Politicians also demanded to discontinue financing the activities of Islamic religious communities from abroad. However, the Central Council of Muslims in Germany adamantly opposed calls to stop the sending of imams from Turkey. It is no secret that these imams guard Turkishness and guard Islamic separateness. From the minbars (pulpits) of mosques, they condemn and banish the West, and compare the unbelievers to rotten fruit that smells. At the same time, when from October 2014 German citizens participated in the weekly Pegida (Patriotic Europeans Against the Islamisation of the Occident) marches in Dresden, they were denounced by left-wing politicians and pro-government media as Islamophobes, Nazis and people who portray Germany in a bad light. The grassroots opposition movement was too weak to stop Chancellor Angela Merkel from opening Germany to hundreds of thousands and ultimately millions of immigrants. Only a small part of the newcomers were refugees. In this human wave that travelled across the Balkans to the EU, it was mostly young, strong men with smartphones. They were quartered in hotels, recently renovated palaces and castles, in abandoned historic monasteries and private summer houses, without often asking for permission from the owners. New tenants quickly destroyed these facilities[22]. The German pro-immigration policy was transferred to the European Parliament, which promoted the principle of the compulsory sharing of immigrants among the Member States. In 2016, the most short-sighted idea came from Ska Keller, co-president of the Greens/EFA group in the European Parliament, who wanted to relocate whole Syrian villages to Eastern Europe, because only in this way would immigrants be able to integrate[23].

---

[20] AEW, *Jak Turcja kontroluje islam w Niemczech*, https://euroislam.pl/jak-turcja-kontroluje-islam-w-niemczech/ [access: 27 IV 2016].

[21] Ibidem.

[22] U. Ulfkotte, *Niemcy jako Mekka. Cicha islamizacja Europy*, Wrocław 2019, pp. 211–212.

[23] K. Izak, *Dokumenty, tożsamość, służby i politycy*, "Człowiek i Dokumenty" 2017, no. 46, p. 59.

Germany has another very serious problem that has also appeared in Sweden. Namely, there are criminal gangs of Arab origin that have a clan structure. A few years ago, the number of criminal clans operating in Berlin was estimated at about 20, and the number of their members at 10,000. Currently, German police sources list as many as 100 Arab crime clans operating in North Rhine-Westphalia alone. Over the last two years, about 6,450 suspects have been registered there who have committed 14,225 crimes, which is 25 percent of the total number of criminal acts. In the Ruhr and Bremen, Arab clans are responsible for 30 percent of crimes. They compete with each other for territories and spheres of influence, taking over entire districts of many cities in Germany. They come into conflict with members of rock and motorcycle clubs, which often end in bloody scores. Arab crime groups Abu Czaker and Miri, as well as Omeirat, Remmo, Rabih, Al-Kadi, Serhan, Nemr, Tamr and Kurdi are also known for their criminal activities in Sweden, Belgium and the Netherlands, countries where a large number of Muslims have migrated. These clans run all kinds of crime. Their members are difficult to track, surveil and identify because they are not registered with foreigners' offices, use false documents, and can count on help from a group or fellow believers. The long-term policy of tolerance and political correctness towards foreign religious and cultural immigrants has led to the present situation in Germany in which clan criminal structures have developed into a parallel society, almost impossible to penetrate and eliminate[24]. The situation is aggravated by the shortage of staff in the German police which hinders effective action against organised crime.

In the literature on the subject, Great Britain is usually seen as the prototype of the multiculturalism model. The United Kingdom took care to preserve the cultural differences of minorities, even emphasised their value. It provided refuge to all those persecuted in their countries. It was no surprise then that the capital of the country, sometimes referred to as 'Londonistan', became the main centre of Islamic radicalism. The extremists expelled from Muslim countries, but also from France, sought refuge here and openly proclaimed their views. London has become an important centre of Islamic extremism influencing the entire world. In Great Britain there are editorial offices of Arabic-language newspapers: "Al-Arab" ("Arabia"), "Al-Hajat" ("Life"), "Al-Quds al-Arabi" ("Arab Jerusalem") and "Ash-Shark al-Awsat" ("Middle East"), editorial boards of radical Islamic organisations: "Filistin al-Muslima" ("Muslim Palestine"), Hamas magazine, or "Risalet al-Ichwan" ("Message of the Brothers") – of the Muslim Brothers, and the headquarters of important Muslim institutions and great assemblies of Islamic activists. Many radical imams who preach anti-Western sermons lived or still live there. Despite evident verbal and sometimes physical aggression, Muslims enjoy great freedom in Great Britain and can still count on indulgence. The reason for this is the legal system into which the European Convention on Human Rights of 1989

[24] A. Dworak, *Ulica należy do klanu. Arabscy gangsterzy opanowali miasta Niemiec*, "Polska Times", 1 II 2019, https://polskatimes.pl/ulica-nalezy-do-klanu-arabscy-gangsterzy-opanowali-miasta-niemiec/ar/c1-13853448 [access: 1 II 2019].

was incorporated in 1997. On this basis, you can be punished for even the slightest criticism of Muslim minorities, including the term 'Islamic terrorism', recognised as Islamophobia. Even after the attacks in London on 7 July 2005, in which more than 50 people were killed and 700 injured, the media and politicians used the term 'terrorism' without religious connotations so as not to arouse discontent and tension in British Muslim community. To this day, their organisations bringing together citizens of the United Kingdom in various parts of the world can count on financial aid. Islamic ideologues were allowed to propagate the most militant ideas provided that they did not try to implement them in Great Britain, as in Germany. It is true that after the 9/11 attacks, a set of anti-terrorist laws was passed in Great Britain, but for a long time they remained only on paper. It was not until the London attacks in July 2005 that more decisive action was taken against Muslim hate preachers, but it took more than years to expel them from the country. Mustafa Kemal Mustafa, alias Abu Hamza al-Masri, was not extradited to the US until October 2012, and Omar Mahmoud Othman, alias Abu Qatada al-Filastini, was not handed over to Jordan until July 2013. After hearing adverse verdicts, they both appealed to the higher court institutions and the European Court of Human Rights. International humanitarian organisations stood up for them, despite the fact that they had committed the crimes of terrorism and had the blood of innocent people on their hands. These examples did not fit in with the regular work of UK law enforcement. The policy of appeasing Islam, i.e. the use of concessions and privileges towards Muslims, was still applied. They were given special rights at the expense of other social groups. This special status exempted Muslims from adhering to norms, the violation of which by members of other social groups is subject to sanctions. In Great Britain, as the only former EU country, Muslim minorities were allowed to use Sharia in civil matters (including marriage and inheritance issues).

The multiculturalism support program aimed at stopping the discontent among newcomers, mainly from Muslim countries, and weakening their critical attitude towards the new homeland. These calculations, however, completely failed, and the friendly policies of successive governments only led to an increase in Islamic extremism[25]. The problems compounded after the great migration wave in 2015. British police, like in other Western countries, notoriously concealed from the public crimes committed by Muslim minorities. Fear of being accused of racism paralyses the actions of Western security forces. An example of this is the diligent police cover-up of the sexual abuse by Pakistani gangs of approximately 1,400 British girls which dragged on for 10 years. It was only when the whole case could no longer be covered up that the report stated, among other things, that the reason for the failure to explain, for silencing and understating the crimes was the law enforcement agencies' fear of

[25] G. Wilk-Jakubowski, *Sytuacja społeczna muzułmanów w Wielkiej Brytanii*, Kraków 2013, pp. 152–153. M. Phillips wrote extensively about the anti-British activity of Muslim groups and the British government's policy towards these minorities, see idem, *Londonistan.* Jak Wielka Brytania stworzyła państwo terroru, Warszawa 2010, (*Londonistan. How Britain is Creating a Terror State Within*, New York 2006).

racist allegations, as well as the political consequences of turning against an ethnic minority[26].

For a time, the model of multicultural society present in Great Britain was also endorsed by Sweden. The Swedish state is perceived as one of the most liberal and immigrant-friendly. In 2015, the country received over 160,000 immigrants, the largest number in Europe in terms of the total number of inhabitants (10 million). Sweden was second only to Belgium in the EU in terms of the number of volunteers per capita who left to fight in the Middle East. It was 32 jihadists per million inhabitants. Volunteer trips to the Islamic State and participation in combat were not considered a crime. Swedish foreign fighters could safely return to the country, heal their wounds, and go to the jihad front again. In Finland, too, foreign fighting was not considered a crime, nor was the mere membership of organisations recognised as terrorist. Sweden has long been one of the most attractive countries for immigrants, because apart from many benefits granted to them, they could completely enjoy impunity here[27]. There is a great deal of political correctness here. The Swedish elite in the EU has probably made the most progress in their oicophobia, i.e. aversion to their own identity and civilisation, and xenophilia – preferring foreign cultures. In 2006, Swedish Prime Minister Fredrik Reinfeldt of the liberal-conservative Moderate Coalition Party stated: *Only barbarism is genuinely Swedish. All further development was brought from the outside*[28]. In this culture of self-criticism, the Swedish churches supported the political class. Both Archbishop Antje Jackelén and other famous clergymen argued that Swedish immigration policy must take into account the fact that Jesus himself was a refugee. Later it was only worse. In December 2014, the same Prime Minister Reinfeldt gave a television interview in which he said that the Swedes were "uninteresting", that the borders were "fictional" and that Sweden belonged to the people who had come there in search of a better life, not to those who had lived there for generations. During the 2015 migration wave, politicians but also alleged and true Islamophiles, often coming from journalistic and scientific circles, even went so far as to say that immigrants (...) *enrich the declining European culture*[29]. They assured that the population would not be bothered if they were replaced by newcomers from other regions of the world. While the situation was certainly not normal in 2015, the authorities of many EU countries pretended that nothing was wrong. For example, in October 2015, the Swedish government organised a conference entitled "Sweden together" to promote its migration policy. The conference was attended by the royal couple and most of the political elite. Ingrid Lomfors, head

---

[26] G. Drymer, *Afery seksualne w Wielkiej Brytanii. Gwałty muzułmańskich gangów*, "Rzeczpospolita", 30 IX 2017, https://www.rp.pl/Spoleczenstwo/309289949-Afery-seksualne-w-Wielkiej-Brytanii-Gwalty-muzulmanskich-gangow.html [access: 1 X 2017].

[27] K. Izak, *Ograniczenia i problemy w zwalczaniu terroryzmu i przestępczości imigrantów w Europie*, "Przegląd Bezpieczeństwa Wewnętrznego" 2017, no. 17, pp. 118–120.

[28] D. Murray, *Przedziwna śmierć Europy. Imigracja. Tożsamość. Islam*, Poznań 2017, p. 325.

[29] Ibidem, p. 164.

of the Living History Forum (Holocaust awareness-raising institution) gave a speech, which was widely praised. Lomfors put forward three theses: 1. Immigration to Sweden is nothing new; 2. Everyone is a migrant; 3. There is no such thing as Swedish culture[30]. The latter thesis proves the absurd views of the supporters of mixing different nations, cultures and religions. This attitude is represented by the political class of Sweden, despite undeniable facts, incl. the highest number of rapes per 1,000 inhabitants in the world after Lesotho in 2015. The Swedish press rarely reported such incidents, and when it did, it deliberately misrepresented the facts. In addition, the police in Sweden are subject to code 291. This number conceals a ban to inform the media of any incidents involving immigrants. No wonder then that in 2016 Adly Abu Hajar, an imam from Malmö, stated that Sweden was the best Islamic country[31].

Change in the perception of the "benefits" of immigration and multiculturalism

After the attacks on 13 November 2015 in Paris (which killed 131 people and injured over 300), President François Hollande said the French must remain strong against terrorism. The former prime minister, François Fillon, said that the war is already here. Police asked Parisians to stay in their homes for their safety. In response to the attacks, the borders of France were temporarily closed and the armed forces were put on alert. A state of emergency was declared nationwide and extended several times (it was lifted on 1 November 2017)[32]. However, this did not protect the country from further attacks. Another bloody attack took place on the national holiday, 14 July 2016. The terrorist drove his truck into crowds of people walking on the promenade. 87 people were killed and over 200 injured. During the declaration of national mourning, Prime Minister Manuel Valls said the words: *France will have to learn to live with terrorism*, which stuck in the memory of the French. Many of them saw these words as an expression of the arrogance of a government that does not fulfil its obligation to protect its citizens, but fights all manifestations of nationalism, Islamophobia and racism. The authorities did not take consistent measures against radical Muslims, but the French society reacted. For the first time Frenchmen in such a large number voted in the presidential election on Marine Le Pen, the leader of the far-right National Front. She qualified for the second round of elections, in which she obtained nearly 34 percent support, but lost to Emmanuel Macron. In the program, she promised, among others priority for the French on the labour market, greater taxation for companies

[30] Ibidem, pp. 165–166.

[31] A. Gromkowska-Melosik, *Mniejszość muzułmańska w Szwecji: między ekstremistycznym izolacjonizmem a procesami reprodukcji ekonomicznej*, "Studia Edukacyjne" 2013, no. 26, www.repozytorium.amu.edu.pl, p. 64.

[32] *Francja zamyka granice. Stan wyjątkowy w całym kraju*, TVN24, 14 XI 2015, https://tvn24.pl/swiat/francja-zamyka-granice-i-wprowadza-stan-wyjatkowy-ra594403-3318007 [access: 14 XI 2015].

employing foreigners, combating illegal immigration and reducing it to zero, as well as deportation of all people who have entered the country illegally, foreigners with court judgments and people filed in the "Fiche S"[33], i.e. posing a serious threat to national security. In those elections, second-generation Muslims made up 8 percent of Le Pen's electorate, despite her anti-immigrant electoral program. They did not hide that their compatriots should be bound by the principle of integration or return to the country. They realised that the French perceive Arabs worse and worse. They treat everyone equally, to the detriment of assimilated immigrants, who in turn are considered traitors by their fellow believers. Many assimilated immigrants also believe that their people from the new generation who avoid work, extort benefits, proclaim anti-French slogans or commit crimes, should be deported[34].

After taking office as president, Emmanuel Macron slowly tightened his policy against illegal immigrants. On the one hand, he officially supported humanitarian actions and agreed to accept more people crossing the Mediterranean Sea to Europe, but on the other, officials made it difficult to legalise their stay. By surprise, in order not to provoke members of humanitarian organisations and human rights organisations, illegal immigration camps were liquidated in Calais (the famous "jungle"), in Paris and in other big cities. The police began transporting immigrants detained on French territory who had no documents and who reached France via the city of Ventimiglia or the Alps to the Italian side of the border. For the first time, it was evident that the authorities were increasingly using force rather than verbal persuasion and promises. A record number of immigrants in France strained the functioning of the social welfare system, generated enormous costs for both social housing and funds offering benefits. The mayors of seven French cities: Nantes, Lille, Bordeaux, Grenoble, Rennes, Toulouse and Strasbourg signed an open letter addressed to the government asking for help from a social catastrophe caused by a huge number of immigrants, and also demonstrated against Muslims organizing prayers in the streets of the cities. Immigration expert Patrick Weil from the Center national de la recherche scientifique (French National Center for Scientific Research, the equivalent of the Polish Academy of Sciences) stated that Macron's approach towards immigrants is (...) *the most extreme since the war*[35]. In the survey, 60 percent of the French expressed the opinion that immigration had

[33] "Fiches S" is a file of people who potentially threaten the security of the state, prepared by the Direction Générale de la Sécurité Intérieure – DGSI (Directorate General for Internal Security). In 2015, Prime Minister Manuel Valls announced that there are 20,000 people on the record including 10.5 thousand related to Islamic extremism. The rest are members of the far-right, leftist movements, etc.

[34] A. Pamuła, *Wrzenie. Francja na…*, pp. 150–152.

[35] O. Górzyński, *Macron robi „porządek" z migrantami. Le Pen triumfuje*, 27 XII 2017, https://wiadomosci.wp.pl/macron-robi-porzadek-z-migrantami-le-pen-triumfuje-6202896011315329a [access: 27 XII 2017]; J. Muller, *„Kryzys na niespotykaną skalę". Burmistrzowie 7 miast Francji przeciw fali imigrantów*, 19 XII 2017, https://www.o2.pl/artykul/kryzys-na-niespotykana-skale-burmistrzowie--miast-francji-przeciw-fali-imigrantow 6200161017976449a [access: 19 XII 2017].

negatively affected their way of life. In a report by the French senate on the fight against the radicalisation of Muslims, the authors stated directly that Muslim immigrants are unable to integrate into society, and the amount of 100 million euros spent by the state in recent years on prevention and education centres has brought poor results. Interior Minister Gerard Collomb stated in December 2017 that France was in danger of a serious crisis because the situation was already explosive[36].

The attitude of the authorities towards Islamic extremists in penal institutions changed. It was found that they were able to influence other prisoners, which resulted in the organisation of strikes in 2014 and 2016. In 2014, prisoners demanded the right to shower in their underwear and not be searched by the guards, which they argued with religious modesty and obliging them no contact with "unclean" unbelievers. If the prison authorities agreed to these demands, it would allow prisoners to freely pass on any objects. In 2016, however, there were several weeks of riots in prisons, and then 200 prisoners in various penal institutions (at the behest of several terrorists who had returned from the Islamic State) refused to return to their cells. The prison authorities responded by creating special units, the so-called Unité de prévention de la radicalisation, UPRA (Anti-Radicalisation Units). Their task was to conduct various activities for the most radicalised prisoners. In this way, an attempt was made to deradicalise them. This solution proved to be unworkable after Bilal Taghi, a Franco-Moroccan jihadist convicted of a trip to Islamic State in Syria who was deemed deradicalised, attempted to murder two guards. Following Taghi's attack, the Interior Minister announced that he would strengthen security procedures to protect the guards. However, in 2018 there was another attempt to murder three guards who were attacked by a jihadist from Germany. The attack was followed by a strike by prison staff and even stricter security rules. The ambitious goal of "deradicalisation" of jihadists was therefore abandoned and replaced with a more modest "restraining from violence". A new special service was created, called the Service national du renseignement pénitentiaire, SNRP (National Prison Intelligence Service). First of all, the radicalised prisoners, who until then had been held mainly in four prisons of the Paris region, were transferred to 79 special-procedure prisons with properly trained guards, scattered throughout the country. In place of the UPRA, seven Quartiers d'évaluation de la radicalisation, QER (Radicalisation Assessment Units) were established, with 140 places prepared. Radicalised prisoners are monitored for four months not only by specially trained prison guards but also by parole specialists, psychologists and educators. Thus, the tolerance and privileges for detained Muslims ended[37].

---

[36] B. Dobosz, *Francja marnotrawi setki milionów euro na asymilację muzułmanów. Przywłaszczenia to codzienność*, 13 VII 2017, http://www.pch24.pl/francja-marnotrawi-setki-milionow-euro-na-asymilacje-muzulmanow--przywlaszczenia-to-codziennosc,53044,i.html [access: 13 XII 2017].

[37] G. Lindenberg, *Najwięcej ekstremistów we francuskich więzieniach*, 4 X 2020, https://euroislam.pl/najwiecej-ekstremistow-we-francuskich-wiezieniach/ [access: 4 X 2020]. In mid-2020, there were 3,000 prisoners in French prisons "considered to be radicalised or suspected of being radicalised". Of these, 522 people were convicted of crimes related to Islamic terrorism, and 900 – radical Muslims convicted of common crimes.

On the 25 September 2020, an immigrant severely wounded two people with a knife. The incident took place near the former editorial office of the satirical weekly "Charlie Hebdo", which again featured caricatures of the Prophet Muhammad on the 1 September. The terrorist believed that he was attacking the journalists of the weekly, while the journalists of the Premieres Lignes agency were the victims. The attacker did not know that after the terrorist attacks of the 7 January 2015, the satirical weekly had changed its seat and its new address was kept secret. After the September attack on the 2 October 2020, President Macron presented a five-point plan to combat Islamist separatism. He announced his intention to "free" Islam in France from foreign influence and create an "enlightened" Islam. He also announced that a special law would be passed at the end of the year, the aim of which was to defend the secular nature of the Republic against the gathering steam conservative and political Islam. He also said that France had to deal with Islamist separatism, describing it as: (...) *a conscious, theoretical, political and religious project*[38] aimed at creating a counter-society based on principles contrary to the applicable law. The state was to take control of the training of imams and the financing of Muslim organisations. In this way, the system that had been in force since 1977 and responsible for sending radical imams from countries such as Algeria, Morocco and Turkey to French mosques would be abolished. It would be easier to fight not only radical Islam, but also agents of influence. Compulsory education in the spirit of republican values would be introduced in schools (including private ones). Children who remained in the home education system would have to return to school. It concerned 62 thousand students. Illegal schools, often run by religious extremists, were planned to close. France wanted to create a version of "enlightened" Islam that is compatible with the secular values of the Republic. The way to achieve this goal is to limit the influence of Koranic schools and other schools educating children and youth in the Islamic spirit. Macron added that the certification of imams in the country would change with the formalisation of their education by the Conseil français du culte musulman, CFCM (French Council for Muslim Worship)[39]. The authorities justified the introduction of the new law by the need to combat Islamic separatism, in which

[38] https://religie.wiara.pl/doc/6553063.Macron-Nowe-prawo-i-ostrzejsze-zasady-wobec-separatyzmu [access: 3 X 2020].

[39] The Council was established in December 2002 on the initiative of Nicolas Sarkozy, the then minister of the interior, who wanted to have a single partner for talks with the fragmented Muslim community. The Council was created as a result of a complex procedure. In order to maintain a balance in the Council, the state made sure that its chairman was Dalil Bubaker, the rector of the Muslim Institute at the Great Mosque of Paris, the oldest Muslim institution in the country, strongly influenced by Algiers (representatives of the Muslim Institute had a poor result in the elections to the CFCM authorities, therefore the French Ministry of the Interior appointed Bubaker as its chairman). An influential person was its vice-president Fuad Alawi, then secretary general of the Union des organisations islamiques de France, UOIF (Union of Muslim Organisations of France). In 2013, UOIF left the CFCM, and in February 2017 it became the Musulmans de France (Muslims of France), usurping the right to represent the entire Muslim minority in the country. Currently, the CFCM represents nine Muslim federations and associations.

religious rights are favoured at the expense of the secular values of the French Republic. Macron defined Islam as a religion that is currently in crisis around the world. In his speech, he focused on the fight against Islamic radicalism in France. He also announced that he would supervise the funding of mosques. He also admitted that the French state was partly responsible for the "ghettoisation" of Muslim residents. Religious organisations took advantage of the errors in integration policy for their own purposes, including intensifying social antagonisms. Macron also said that France's colonial past, including the colonisation of Algeria, left scars in public awareness that sometimes hampered the integration of immigrants from the former colonies. He noted: *We have not got to grips with our past*[40]. Deputy Interior Minister Marlene Schiappa, responsible for citizenship, announced that polygamists would be deported from France. They cannot be protected from the fact that they are already nationals of the country or that they have a residence permit. They will only be able to stay there if they obey French law. The minister also announced that issuing "virginity certificates" for women and girls would be prohibited. They cannot be treated as "cows in the market"[41].

A turning point in the perception of the "benefits" of immigration and multiculturalism was the brutal murder of the history teacher Samuel Paty by the 18-year-old radicalised Chechen Abdullah Anzorov. The crime took place on the 16th of October 2020. The investigation showed that other young Muslims and their parents were involved in the attack. This event was met with decisive action by the authorities for the first time. Interior Minister Gerald Darmanin ordered the police to deport 231 illegal immigrants known for their extreme religious views and to tighten checks on applicants for a residence permit in France in terms of their attitude towards the host country and Islam. He also instructed the police to tighten checks on people seeking refugee status and scrutinise the applications more carefully to exclude further Islamic extremists, and to prepare a list of Muslim organisations and institutions known for promoting radical ideas. Actions were announced to eradicate hate speech in social media. On 20 October, the authorities ordered the closure of the Grand Pantin Mosque in Seine-Saint-Denis, on the outskirts of Paris, for six months, where sermons full of hatred against France and Europe had been delivered. Collectif contre l'islamophobie en France, CCIF (Collective Against Islamophobia in France) spoke in response to the authorities' actions. It felt concerned about the political pressure exerted by top politicians and the intimidation campaign against an organisation tasked with combating discrimination and hate crime against Muslim citizens. Minister Darmanin reacted harshly to this statement, announcing that the CCIF

---

[40] O. Bault, *Francuska dziwna wojna z islamizmem*, "Do Rzeczy", 29 X 2020, https://dorzeczy.pl/swiat/158991/francuska-dziwna-wojna-z-islamizmem.html [access: 29 X 2020]; P. Kryszak, *Narasta konflikt Francji z Turcją*, "Gazeta Polska Codziennie" of 26 October 2010; P. Ślusarczyk, *Prezydent Francji zapowiada walkę z islamskim separatyzmem*, https://euroislam.pl/prezydent-francji-zapowiada-walke-z-islamskim-separatyzmem/ [access: 5 X 2020].

[41] P. Petrović, *Francja walczy z islamskim separatyzmem*, "Gazeta Polska Codziennie" of 7 October 2020.

would be banned. The dissolution was to apply to 50 other Muslim organisations and institutions, such as BarakaCity[42]. Its founder, Idris Sihamedi, was previously accused of harassing, publicly insulting and making criminal threats against a journalist on the RMC radio station Zohra Bitan, who allegedly committed contempt of the prophet Muhammad. The French authorities decided to dissolve the pro-Hamas Sheikh Yassin Collective, led by radical Abdelhakim Sefriui. He was arrested along with other people for participating in organising a campaign on social media against Samuel Paty, which ended with his murder[43].

On 29 October, there was another attack. A Tunisian immigrant, armed with a knife, attacked in the basilica of Notre Dame in Nice. Three people were killed, one of them (a woman) was decapitated by the terrorist. After this incident, the control of the Franco-Italian border was tightened and joint patrols of the border services of both countries were organised in order to catch illegal immigrants trying to enter France. Another reaction of the Elysée Palace to the increased terrorist threat was commissioning the CFCM to develop a code of ethics for imams. The authorities, in agreement with the CFCM, decided to establish the Conseil national des imams, CNI (National Council of Imams), which would be responsible for educating Muslim preachers (in Arabic: *chatib*) and imams. CNI workers would be required to oversee their work and disqualify those imams and preachers who preach radical content and sympathise with Islamic extremists. The aforementioned code of ethics for imams was to be based on a set of rules applicable to doctors and lawyers. The postulates of the code include the statement that Islam is a religion, not a political movement, and cannot be subject to foreign interference in the affairs of Muslim communities in France. During a meeting with CFCM representatives, President Macron presented the *Charte des valeurs républicaines* (*Charter of Republican Values*), asking for its approval within 15 days. The government was to put pressure on the charter to be signed by organisations and institutions associated with the Muslim Brothers and communities from Turkey that use religion to exert political influence in Europe. The activities of the state authorities were complemented by the book *Immigration – Ces réalités qu'on nous cache* (*Immigration – these realities that are hidden from us*), published in November 2020. Its author is Patrick Stefanini[44], member of the Council of State and former prefect. For years he had dealt with the problem of immigration. His book is the first reliable study of this type. It contains detailed information and statistics that successive French governments for 30 years refused to disclose to the public. The same month, the CCIF announced its decision to dissolve itself. On

[42] French, Muslim NGO involved in charity, https://pl.wikipedia.org/wiki/Barakacity [access: 2 III 2021] – editor's note.

[43] J. Bielecki, *Emmanuel Macron w końcu wypowiada wojnę islamistom*, "Rzeczpospolita" of 20 October 2020; https://www.rp.pl/Polityka/201029902-Emmanuel-Macron-w-koncu-wypowiada-wojne-islamistom.html [access: 22 X 2020].

[44] B. Dobosz, *Islamski terroryzm przestaje być tabu*, "Najwyższy czas" 2020, no. 50–51.

9 December 2020, at the meeting of the Council of Ministers, Prime Minister Jean Castex[45] presented a draft bill on combating Islamist separatism. The document listed in detail the tasks awaiting the administration and Muslim communities aimed at limiting the influence of Islamic radicals, who currently posed the greatest threats to the security of citizens and the cohesion of the state. At the same time, the CCIF was dissolved by a decree of the Council of Ministers (probably so that its activists would not make a decision to resume operations in some time), but Human Rights Watch and the Human Rights League stood up in defence of the organisation, which condemned this decision, and the Council on American-Islamic Relations (CAIR), which is strongly influenced by the Muslim Brothers, offered its support. With the support of these institutions, the former CCIF activists filed a complaint to the Court of Justice against the Minister of the Interior for an unfounded accusation that the CCIF was directly involved in the murder of Samuel Paty and announced that it was challenging the decree of the Council of Ministers regarding the delegitimisation. The investigation did not support the hypothesis that the organisation was involved in the murder of the teacher[46]. On 29 December the rector of the Grand Mosque of Paris, Chems Eddine Hafiz, announced his withdrawal from the meetings scheduled to establish the CNI. Moreover, Islamist groups with influence in the CFCM successfully impeded the signing of the *Charter of Republican Values*[47]. It was approved on 17 January 2021, even though several Muslim federations opposed claims that Islam could be reconciled with French laws and values. The signing of the document by representatives of the authorities of organisations associated in the CFCM does not mean, however, that the provisions contained therein will be implemented in practice, because only now is a discussion to start with imams and leaders of Muslim community in France about obtaining the broadest possible support for the *Charter*[48].

In Germany, the 2015 migration wave led to a political crisis two years later. Angela Merkel's decision to open Germany widely to refugees from the Middle East can be considered the second so ground-breaking after the country's reunification in 1989. The political slogan: "We can do it" (in German: "*Wir schaffen das*") coined by the chancellor herself actually reflected the hope and optimism well prevailing in the circles of power at the time as to the possibility of overcoming the refugee crisis. However, support for accepting more refugees decreased from month to month.

---

[45] J. Kowalkowska, *Macron tworzy muzułmańską kurię*, "Gazeta Polska Codziennie" of 23 November 2020; AFP, "*Séparatismes": un projet de loi "pas contre les religions", selon Jean Castex,* https://www.france24.com/fr/france/20201209-séparatismes-le-gouvernement-présente-son-projet-de-loi-contre-l-islamisme-radical [access: 9 XII 2020].

[46] https://en.wikipedia.org/wiki/Collective_Against_Islamophobia_in_France [access: 20 XII 2020].

[47] *La grande Mosquée de Paris annonce son retrait du projet de Conseil national des imams*, "Le Monde" of 29 December 2020, https://www.lci.fr/societe/la-grande-mosquee-de-paris-annonce-son-retrait-du-projet-de-conseil-national-des-imams-2174082.html [access: 30 XII 2020].

[48] *Francuska Rada Kultu Muzułmańskiego akceptuje zasady Macrona*, https://euroislam.pl/rada-muzulmanow-akceptuje-zasady-macrona/ [access: 18 I 2021].

In November 2016, polls showed that as much as 69 percent respondents in Germany wanted an immediate halt to admitting refugees. Violence against newcomers and the growing anti-Islamic movement became an increasingly visible element of German society and German politics. With hindsight, there are more and more signs that the decision about the uncontrolled admission of refugees was more an expression of wishful thinking than a rational settlement taking into account the actual political situation[49]. The wave of a million immigrants that came to Europe caused a dynamic increase in the ratings of far-right and populist groups. Nevertheless, in 2018, the German authorities prepared another great project implementation plan – the admission of several hundred thousand immigrants as part of family reunification with those who had already obtained the right of residence.

Despite the increase in the number of employees at the consular post, the waiting period for German visas increased to seven months or even a year, which caused dissatisfaction of supporters of admitting immigrants. The Green party, then sitting in the government, demanded the introduction of new solutions. In its opinion, visa applications could also be processed by the staff of the Ministry of Foreign Affairs in Berlin, and not only by German embassies and consulates. It would be an unprecedented situation, invented by someone who has completely lost touch with reality. According to information from the German Ministry of the Interior, by the end of 2017, approximately 180,000 asylum applications had been filed by refugees from Iraq and Syria, and in the next year more than twice as many, which, with the size of Arab families, meant bringing in several times more people, of course at the expense of the state – assuming that they would be only members of the immediate family, not distant relatives. The centre-right and liberal Freie Demokratische Partei, the FDP (Party of Free Democrats), which terminated the talks on the formation of a government coalition in November 2017, refused to accept these new groups of immigrants, which were to come to Germany from 2018. It is worth adding that in 2018 the ban on family reunification of refugees and asylum seekers, introduced as a result of the immigration crisis in 2015, expired. The new government was formed only in mid-March 2018 from a coalition of three political groupings: Christlich Demokratische Union Deutschlands, CDU (Christian_Democratic Union), Christlich-Soziale Union in Bayern, CSU (Christian Social Union in Bavaria) and Sozialdemokratische Partei Deutschlands, SPD (Social Democratic Party of Germany). At that time, one could also observe an increasing polarisation of society, which resulted in pro- and anti-immigrant demonstrations, an increase in the support for far-right organisations, including the presence of Nazi sympathisers in the army and police, promoting Nazi slogans and symbols in cyberspace. The authorities, however, recognised that the extreme right posed a greater threat than the Muslim ghettos and criminal clans. This opinion was issued as a result of the electoral success of the anti-immigrant and xenophobic

[49] M. Sulkowski, *Polityczne konsekwencje kryzysu imigracyjnego w Niemczech*, "Chrześcijaństwo–Świat–Polityka. Zeszyty Społecznej Myśli Kościoła" 2016, no. 20, p. 59.

Alternative fur Deutschland, AfD (Alternatives for Germany), which won third place in the 2017 parliamentary elections (12.5 percent of votes and 94 seats). This party was also successful in local elections. Appearing on the official political scene contributed to the further radicalisation of all extreme-right groups. The same process was also taking place in the ranks of the AfD, as evidenced by the re-election of Björn Höcke, known for his neo-Nazi sympathies, as party leader in Thuringia. This was accompanied by information about the activities of racist groups in the army and police, and even in the military anti-terrorist unit. The Bundeskriminalamt, BKA (Federal Criminal Police Office) reported that over 13,000 those associated with the extreme right were willing to use violence, and at least 65 of them posed a direct terrorist threat. The turning point in the government's behaviour towards the right-wing extremism was the attack on the head of the administration of the Kassel district, Walter Lubke, murdered in June 2018[50].

However, none of the politicians wanted to admit that the source of the aggravation of the domestic situation in the country was the opening of German borders to hundreds of thousands of immigrants. Therefore, it might have been a big surprise to appeal to the Green party to intensify the fight against the Islamist threat and the murderous ideology behind it. The leader of the Greens, Robert Habeck, presented a plan under the slogan: *Islamism is still one of the most serious threats to the internal security of all free societies*. One of the elements of the plan was to increase security forces in places where 24-hour surveillance of extremists must be carried out. There were also calls for the deportation of those who were dangerous. It was also expected that the activities of Salafi organisations would be banned and the funding of these groups would be monitored. The Greens want an extensive, countrywide anti-radicalisation network. It would be based on preventive cooperation with mosques and Muslim communities. In confrontation with a growing group of terrorists about to leave prisons, the party wanted to monitor their activities at large. The party's initiative is surprising for those who associate the left wing mainly with pro-immigration policies, multiculturalism and concessions to Muslim minorities. In the West, there is often talk of a Muslim-leftist alliance. Nevertheless, the German Greens cannot be classified that easily. For years, Robert Habeck was considered in the party as a person who, apart from promoting a tolerant society, warned against the threat posed by Muslim radicalism. For many years, the leader of the Green party was Cem Özdemir, of Turkic origin, a declared opponent of political Islam and the Islamists currently ruling Turkey[51]. So far, however, the German Greens supported the government's pro-immigrant policy. They opposed the deportation of illegal immigrants and often blocked the take-off of planes with them on board.

---

[50] See P. Jendroszczyk, *Rosnący lęk przed skrajną prawicą*, "Rzeczpospolita" of 26 November 2020.

[51] J. Wójcik, *Niemieccy Zieloni: „Islamizm jest zagrożeniem"*, https://euroislam.pl/niemieccy-zieloni-islamizm-jest-zagrozeniem/ [access: 18 XI 2020].

In November 2019, the government presented a bill, according to which clergymen coming to Germany from countries outside the EU must demonstrate knowledge of the German language. Although the provisions of the act apply to clergymen of all faiths, there is no doubt that the authorities want to regulate the stay of Muslim imams and preachers in this way. According to the latest data presented by the Adenauer Foundation, there are currently approx. 2,000 mosques, and 90 percent of the imams working there come from abroad. In January 2019, the German Ministry of the Interior informed that only 1,049 imams and preachers were employed in the municipalities under the Diyanet İşleri Türk-İslam Birliği, DITIB (Turkish-Islamic Union of Religious Affairs). The draft law assumed that clergy who want to live and work in Germany would have to prove within a year of their arrival in Germany that they know German well enough to be able to talk. The German interior minister stressed that the command of language is a must for integration to be effective. The government's proposal was criticised by the Greens. Their representative, Filitz Polat, expressed concern that the law would worsen the problem of the shortage of Muslim clerics of German origin. Sometimes organisations buy out already educated imams who, for various reasons, change their organisational affiliation, e.g. after the contract expires, the imams from DITIB move to an organisation called Milli Görüs (National Awareness/Vision) and undergo additional supplementary training there. In November 2019, Chancellor Angela Merkel and Minister of the Interior, Horst Seehofer, proposed that Germany educate imams themselves[52].

Austria with a population of 9 million is inhabited by 700,000 Muslims of which over 300,000 live in Vienna and its metropolitan area. For many years, the authorities pursued a liberal policy towards immigrants and Muslims. In 2014, Sebastian Kurz, the then Minister of Foreign Affairs, presented a new draft bill on Islam. It included, among others a ban on foreign funding of mosques and imams. The aim of the changes was to increase the number of imams educated in Austria and having Austrian citizenship. Islam was to be taught by imams who not only got to know the Austrian culture, but also learned about the problems of young Muslims in this country. The law explicitly stated that Austrian law had priority over the Sharia law. In addition, it required Muslim communities to present their interpretation of the faith and to translate into German the nine versions of the *Koran* that were in use. The law also prohibited imams from justifying violence in any way. Muslims immediately objected to the bill, claiming that it makes all Muslims potential bombers. At the same time, Austrian Muslims blamed the country's authorities and their politics for the radicalisation of their fellow believers (but they did not explain what exactly was their fault). Some media outlets and politicians reacted similarly, arguing that Muslim organisations easily attracted young Muslims with promises of a better life. They proposed fighting among real men,

[52] A. Rusinek, *Nurt radykalny wśród społeczności*…, p. 73; *Niemcy: imamowie będą musieli udowodnić, że znają niemiecki*, 7 XI 2019, https://www.dw.com/pl/niemcy-imamowie-będą-musieli-uwodnić-że-znają-niemiecki/a-51148977 [access: 7 XI 2019].

the possibility of being freed from sins, etc. As a result, in 2014, over 160 jihadists left Austria for Syria. The problem, as in other European countries, was the financing of Muslim associations and institutions by state entities and non-governmental organisations from abroad: Saudi Arabia, the UAE, Qatar and Turkey. In 2015, the situation worsened when hundreds of thousands of immigrants from the Middle East and Africa moved to the EU at Angela Merkel's invitation. Only in 2015, about 100,000 people came to Austria. The authorities had no idea who they were and, like the rest of the host countries, were unable to verify their identity (over 70 percent of the newcomers had no documents except for smartphones). At that time, Sebastian Kurz demanded the closure of the Balkan route and announced decisive actions against people associated with radical Islam[53].

After taking leadership of the Österreichische Volkspartei, the ÖVP (Austrian People's Party) and chancellor in 2017, Kurz suggested a massive return of immigrants to Africa and securing the EU's southern borders, which was met with severe criticism from Western states and NGOs. In June of the same year, a 50-page report was prepared, but its publication was not anticipated. The report was prepared to check that foreigners are not discriminated against in the public employment service (Arbeitsmarktservice, AMS) and in the labour market. However, the document was leaked to the media at the beginning of 2018. It did not find any discrimination against foreigners, but described the cultural and religious barriers to the integration of people whose mother tongue was not German. This regarded especially Chechens and Afghans. It was noted that the employees of the labour office were afraid to suggest the Chechens to take up employment or attend educational courses. The AMS officials were apparently intimidated. Syrians, Chechens and Afghans, according to the authors of the report, had a problem with taking up jobs in such professions as social welfare and gastronomy, because the idea of serving other people is rejected by them. Muslim men, fathers, and husbands also made it difficult to hire or educate their wives and daughters. Following the publication of this report, the politically correct media demanded the dismissal of AMS executives[54]. In mid-2018, the chancellor ordered the expulsion of several foreign-funded imams from the country and announced the closure of seven mosques. He also presented to the European Commission a solution to the problem of immigrants before they reach EU borders. He proposed the creation of closed centres for immigrants in Albania and Kosovo. There, foreigners from outside the continent would be screened and divided into those who are actually refugees and economic immigrants. The latter

[53] B. Wieliński, *Austria zwalcza islamskich agentów zagranicy*, "Gazeta Wyborcza" of 26 February 2015, https://wyborcza.pl/1,75399,17490678,Austria_zwalcza_islamskich_agentow_zagranicy.html [access: 27 II 2015]; M. Dębski, *Atak spowodowany nienawiścią wobec chrześcijańskich wartości*, "Warszawska Gazeta", 11 XII 2020, https://warszawskagazeta.pl/swiat/item/7050-atak-spowodowany-nienawiscia-wobec-chrzescijanskich-wartosci [access: 11 XII 2020].

[54] *Austria: Czeczeni ponadprzeciętnie agresywni*, 20 III 2018, https://euroislam.pl/czeczeni-ponadprzecietnie-agresywni-raport-austriackiego-urzedu-pracy-wyciekl-do-mediow/ [access: 20 III 2018].

would be deported to their countries. The Austrian plan was unofficially supported by representatives of Denmark, the Netherlands and Germany[55]. However, it remained on paper. On the other hand, Turkish citizens living in Austria and Austrians of Turkish origin were deprived of the possibility of taking driving tests in Turkish, which had been the practice so far. This was to encourage them to learn German. After the attack in the capital on 2 November 2020, in which four people died and 23 were injured, Chancellor Kurz was not politically correct and stated unequivocally that the attack was an act of Islamic terrorism caused by hatred towards the basic values of the Austrian way of life and democracy. He emphasised that this was not a war between Austrians and immigrants or Christians and Muslims, despite the fact that since 2018 there had been several attacks on churches by young Muslims[56].

On the16 of December, the government proposed changes to the law known as the "anti-terrorist package". Despite earlier announcements, however, it lacked the explicit prohibition of the functioning of political Islam and provisions on the possibility of extending the imprisonment of terrorists after they served their sentence. Instead, alternative measures were proposed in the form of electronic monitoring of persons convicted of terrorist offenses after their release from prison. The provision was to be religiously neutral and apply to the perpetrators of all terrorist offenses, regardless of the type of religious or political motivation. It was emphasised that the goals of their fight against Islamism remained unchanged, and the law was only adapted to the requirements of the constitution. Integration Minister Susanne Raab said that whoever wanted to introduce sharia courts in Austria had to take into account the fact that they would face a criminal court. A debate began in Austria as to whether it is necessary to specify religious extremism in the law at all. Constitutionalist Heinz Mayer recalled that there were provisions in the criminal law on subversive movements that can be used in such cases. However, Raab said an "anti-terrorist package" in this form was necessary. She defended the precise regulation because it is a (...) *criminal offense, the aim of which is to create a new social order based on religion*[57]. Interior Minister Karl Nehammer confirmed the necessity to continue the fight against Islamism, but also pointed to the need to combat right-wing extremism. He announced changes in the provisions on symbols that will also apply to extreme right-wing organisations. Symbols of both the far-right Identitarian movement, the Islamic State and the Turkish Partiya Karkerên Kurdistanê, PKK (Kurdistan Workers' Party), considered terrorist, would be banned. The acceleration of the path of deprivation of dual citizenship, however, leaves no doubt as to the intentions of the legislators, as it

[55] T. Orszulak, *Austria zamknie siedem meczetów i wydali imamów. Sebastian Kurz idzie na wojnę z islamem*, 8 VI 2018, https://wiadomosci.wp.pl/austria-zamknie-siedem-meczetow-i-wydali-imamow-sebastian-kurz-idzie-na-wojne-z-islamem-6260497626355329a [access: 8 VI 2018].

[56] T. Wójcik, *Mordercy, ISIS i pustosłowie*, "Tygodnik Solidarność" 2020, no. 46.

[57] According to experts and lawyers, the act of terrorism is not an "ordinary" criminal offense and requires a special legal regulation.

would concern almost all Muslim radicals. Associations and mosques disseminating extreme views could be closed quickly in the event of terrorist propaganda appearing in them. Raab also wanted information about imams and mosques. Registers would be created with an indication of people and objects to which special attention should be paid. Compared to the previous law, the government would tighten its control over the funding of religious organisations even further, making it impossible to circumvent the ban on funding their activities through charitable associations and foundations. A lifetime ban on the possession of a weapon by persons convicted of a terrorist offense and a ban on working in security related professions would also be introduced[58]. On 1 January 2021, the regulation concerning all imams in Austria to register in the Islamic Religious Community came into force. At the same time, Austrian EU Minister Karolin Edstadier appealed to the EU to follow the example of Vienna and introduce compulsory registration of all teaching imams in the European Community. She also drew attention to the need for increased control over the allocation of funds to Muslim organisations and institutions so that the money would not go to associations supporting radical Islam[59]. By following the changes planned in French and Austrian law, the Swiss authorities intend to introduce the most drastic anti-terrorist law in the West. It would also apply to minors, which would violate the European Convention on Human Rights. But the Swiss government is determined to introduce the new rules, despite the harsh criticism of the UN Human Rights representative, who had already condemned the actions of the authorities for withdrawing Swiss citizenship from a Syrian citizen in early 2020. This was the first such case since World War II. If the changes in the law could not be passed in a referendum by February 2021, radicalised persons suspected of posing a terrorist threat would be placed under house arrest without a court order[60].

In 2017, Myndigheten för samhällsskydd och beredskap, MSB (Swedish Civil Contingencies Agency) published a report, *Muslimska brödraskapet i Sverige* (*Muslim Brotherhood in Sweden*). This report stated that Muslim organisations officially operating in Sweden create their own parallel society and have connections with the Muslim Brothers, which poses a challenge to the country's social cohesion. The author of the study, Magnus Norell, a political scientist and expert on terrorism, pointed out that the Muslim Brothers are agitating for a transformation in Sweden towards an Islamic society. The expert claimed that girls should receive special care. Since a Muslim is bound by other separate religious rules than other citizens. According to the report, the Muslim Brothers influence the Stockholm branches of the following charities: Islamic Relief, Studieförbundet Ibn Rushd (Ibn Ruszda Swedish Student Union),

---

[58] J. Wójcik, *Austria przedstawia pakiet antyterrorystyczny*, 17 XII 2020, https://euroislam.pl/austria-przedstawia-pakiet-antyterrorystyczny/ [access: 17 XII 2020].

[59] J. Kowalkowska, *Austria chce unijnego rejestru imamów*, "Gazeta Polska Codziennie" of 9 January 2021.

[60] L. Bias, *Die Schweiz ist im Begriff, das härteste Antiterror-Gesetz des Westens einzuführen*, 23 XI 2020, https://www.swissinfo.ch/ger/-die-schweiz-ist-im-begriff--das-haerteste-anti-terror-gesetz-des-westens-einzufuehren- /46168700 [access: 23 XI 2020].

Islamiska unionen (Islamic Union) and the Sveriges unga muslimer, SUM (Swedish Islamic Youth association). The document emphasises that these organisations receive millions of Swedish Kronas in subsidies from the state. These are various types of grants awarded by local governments and central offices for cultural, educational and integration activities. Norell argued that the Muslim Brothers extend influence in political parties, NGOs, academic institutions and other civil society organisations. He also accused the political elite of a conspiracy of silence dictated by political correctness and the alleged, in his opinion, fight against racism and Islamophobia. The Muslim brothers had the support of the left-wing parties and the Greens. In 2016, the organisation received 1.36 million Swedish Krona (142,000 Euros) for its activities and additional funding for an anti-racism project. It can be concluded that the political and religious activity of the Muslim Brothers in Europe has been built into the model of integration and can be interpreted as standard work for social dialogue. Norell emphasised, however, that in Sweden, the Muslim Brothers could count on the support of some circles supporting multiculturalism, left-wing parties and the Greens. The report stated that SUM members travelled to the battlefront in Syria and participated in the attempted assassination of Swedish artist Lars Vilks, the creator of the Muhammad caricature. The organisation also promotes violence and hatred towards other religions on its social networking site[61].

The Norell report was severely criticised by a group of Swedish religious scholars. In an open letter, they accused the author of, inter alia, no factual basis and equal treatment of the entire group of Swedish Muslims. Anneli Bergholm Söder, the representative of the MSB, who commissioned the report, stated in a statement for the media that the document would be analysed and the author was responsible for its content[62]. Norell was probably right because SUM did not receive a government subsidy in 2017 due to (...) *the lack of respect for democratic ideas*. Myndigheten för ungdoms-och civilsamhällesfrågor, the MUCF (The Swedish Agency for Youth and Civil Society) did not award them a grant the following year. In 2018, the Polish community organisation, the Congress of Poles in Sweden, was also deprived of subsidies. MUCF judged that the activities of the Congress were contrary to democratic ideas. In support of such a conclusion, examples of views expressed in the pages of "Goniec Katolicki" ("Catholic Courier"), a periodical published together with the "Słowo Kongresu" ("Word of the Congress"), were provided. According to Swedish officials, in 2016–2017, "Goniec Katolicki" published (…) *generalizing and damaging statements about Muslims, which described this group as a threat to society*. There were also opinions in the newspaper that (...) *Islam must be fought, not negotiated with*. The articles used inappropriate terms

[61] M. Czarnecki, *Skandynawia halal. Islam w krainie białych nocy*, Warszawa 2019, pp. 127–129.

[62] *Muzułmańskie organizacje tworzą własne społeczeństwo. Mocny raport Szwedzkiej Agencji Ochrony Cywilnej*, 3 III 2017, https://wiadomosci.wp.pl/muzulmanskie-organizacje-tworza-wlasne-spoleczenstwo-mocny-raport-szwedzkiej-agencji-ochrony-cywilnej-6097105667277953a [access: 3 III 2017].

such as "race" and "Negro"[63]. In February 2021, the Gothenburg authorities decided to withhold funding from the Ibn Ruszda Swedish Student Union due to the organisation's ties to the radical Milli Görus group and the Muslim Brothers[64].

The following two years slightly changed the attitude towards political correctness promoted in Sweden. The media revealed that at the beginning of 2019, over 19 percent of the entire population living in Sweden were immigrants, with the majority coming to the country in the last 20 years. In addition, it turned out that as much as 90 percent of Moroccan 'teenagers' who applied for asylum in the past seven years were male adults. Only recently have politicians started to notice that all assumptions about the integration policy turned out to be utopia. In September 2020, Mats Loefving, Deputy Chief of the Swedish Police, and Edi Mord, Chief of Police in Guthenburg, spoke openly about the threats posed by immigrants. They provided the public with information for which they would have been accused of racism two years earlier and lost their jobs. It turned out that there are at least 40 family gangs from Muslim countries organised in Sweden, similar to criminal clans in Germany. Their members came to the country for the sole purpose of organizing and carrying out criminal activities. They mainly earn money from drug trafficking, assaults and extortion. In the years 2018–2019, about 30 men per year are killed in mafia scores. Muslim customs apply in the clans. Their members reject integration, they do not want to be part of Swedish society. Crime clans have a completely different culture and are difficult to combat using standard police procedures. Politicians have only now begun to work on changes in the law that would permit, among others, interrogating gang members, despite the fact that a serious crime has not yet occurred, and without obtaining the prosecutor's consent, which until now was necessary. For now, the criminal clans are doing very well. They are favoured both by the law, which in Sweden has not been adapted to the changing reality, and the exceptional leniency of the Swedish law towards juvenile offenders (they enjoy complete impunity). Immigrants in Sweden still exercise many privileges, including a Swedish law which allows defendants to choose the most convenient time for serving a prison sentence. The accused leaves the courthouse and vanishes, whereas the police do not have the power and resources to be after the convict[65].

---

[63] *Muzułmańska organizacja bez dotacji od szwedzkiego państwa*, 11 IV 2018, https://religie.wiara.pl/doc/4633953.Muzulmanska-organizacja-bez-dotacji-od-szwedzkiego-panstwa [access: 11 IV 2018].

[64] *Göterborg wstrzymuje finansowanie islamistów*, https://euroislam.pl/goteborg-wstrzymuje-finansowanie-islamistow/ [access: 25 II 2021].

[65] M. Dębski, *Muzułmański potop w Szwecji*, "Warszawska Gazeta", 20 XI 2020, https://warszawskagazeta.pl/swiat/item/ 7050-muzułmański-potop-w-szwecji [access: 20 XI 2020].

Conclusions

The immigration crisis has a strong impact on politics in Europe, becoming a driving force for movements and parties that negate the current political order, including those that do not hide their xenophobic slogans and ideologies. Angela Merkel, under the catchphrases of openness and multiculturalism, opened the borders to immigrants, but at the same time caused an increase in xenophobia, from which the EU and Germany seemed to have managed to break free. Europe finds itself in a dangerous situation with xenophobic movements on the one hand and radical Islam on the other. Each of these formations legitimises its existence and methods of operation by the existence of the other, and also tries to polarise society and create a situation that will force citizens to take sides. Paradoxically, Chancellor Merkel's decision to admit immigrants has significantly increased the risk of such a scenario, which is why the German authorities perceive both Islamic and right-wing extremism as posing the same threat to state security.

The terrorist attacks in October and November 2020 in France and Austria put the EU on alert once again, but this time the rhetoric of the political class and the media changed. For the first time, the attacks were associated with political Islam, and not with maladjusted, unbalanced people or enemies of society and democracy, which resulted from political correctness that did not allow terrorism to be combined with Islam. Anti-European (especially anti-French and anti-Austrian) statements of politicians from Muslim countries, often vulgar and full of hatred, demonstrated how important this change of narrative turned out to be. President Macron also became a target of the Arab street because he dared to express his opinion on the motivations of the bombers, and also announced that he would take measures to counteract the export of anti-Western ideas from Muslim countries to the EU in the future. It is worth adding that Al-Jazeera TV turned out to be an ally of Muslim politicians. It released a 3-part film entitled *Blood and Tears: French Decolonisation*, which tried, inter alia, to explain that the source of the attacks in France was the trauma of the Algerians during the national liberation war, their discrimination and racism of the French. Similar opinions were also expressed by experts, incl. Asma Barlas from New York or Ludwika Włodek, author of the recently published book: *Gorsze dzieci republiki. O Algierczykach we Francji*[66] (*Worse children of the Republic. About Algerians in France),* whose statements the author of the article drew attention to.

Changes in the law and tightening of regulations may not be enough to change the situation. It could be beneficial to redefine the policy of multiculturalism and integration, not to mention the assimilation of Muslim minorities. If the interpretation

[66] PAP, *Ekspertka o przyczynach islamizcji migrantów we Francji: dżihad, rasizm i dyskryminacja*, 1 XII 2020, https://www.pap.pl/aktualnosci/news%2C767547%2Cekspertka-o-przyczynach-islamizacji-migrantow-we-francji-dzihad-rasizm-i [access: 1 XII 2020]; A. Barlas, *On freedom of speech and* '*Islamist separatism*', Aljazeera, 11 XI 2020, https://www.aljazeera.com/opinions/2020/11/11/on-freedom-of-speech-and-islamist-separatism [access: 11 XI 2020].

of the *Koran* and the Hadith cannot be changed and the dogmas of Islam cannot be thoroughly reformed, perhaps efforts should be made to change the consciousness of Muslim minorities in Europe. In addition, the area of norms and values can be defined in a restrictive way, which, while maintaining different cultures and customs, would determine the granting of the right to stay in the EU. A democratic society cannot accept immigrants who do not respect its basic principles. The solution may be to force them to adopt certain standards or return to their country of origin. The harmonious coexistence of minorities and host societies depends on sound political decisions and long-term, consistent action. They cannot be subordinated to party ideology and current political benefits, i.e. the pro-immigration policy of the left and the anti-immigration policy of the right. The decisive condition should be the newcomers' acceptance of European rights, norms and values and the ability to integrate. It is important that the EU as a whole, not individual countries, is ready to face this problem.

Putting hope in the education of imams residing in European countries as a way to solve the problem of radicalisation of Muslims is, in the author's opinion, too optimistic. Already in 2011, the first Center of Islamic Theology was established at the University of Tübingen, and a year later in Osnabrück and Frankfurt. It found that the studies were dominated by women, and many men with 5-year diplomas did not intend to work in mosques. Only a few Muslim theologians educated in Germany remained imams[67]. It is also wrong to assume that preachers would preach in the European language and imams would lead prayers in the same language. It is simply not compliant with Islam. It would be less costly and more rational to closely monitor clergymen in Europe who came from Muslim countries, and above all to have them reviewed by consular services and checked by special services before issuing a visa. Obtaining a work visa should be compulsory for foreign clerics of Muslim origin wishing to establish themselves in the EU. The validity of the visa can be limited to one or two years with the possibility of its extension, and not – as in Germany – it is valid for at least five years.

It is hoped that the French authorities will be determined enough to implement all the announced measures against Islamic radicals. Relations between the government and Muslim organisations operating in this country were not as strained as they are today. It is difficult to persuade these organisations to any cooperation. So far, the CFCM has not accepted the Charter of Civil Liberties, although it had 15 days to do so, and it is not known whether it will happen at all. The creation of the CNI also seems increasingly questionable. Thus, President Macron's flagship projects may fail to restore "separatist" districts on the outskirts of big cities to the state. Years of neglect, submission, and the admission of new immigrants, despite the failure of the integration policy, led to chaos. All it takes is a spark to open rebellion against the authorities.

---

[67] S. Ripperger, M. Matzke, *Pierwsze centrum kształcenia imamów w Niemczech*, 10 X 2011. https://www.dw.com/pl/pierwsze-centrum-kształcenia-imamów-w-niemczech/a-15449531 [access: 10 X 2011].

Is it justified, then, to seek an agreement with the Muslim Brothers? This grouping is deeply entrenched in many European countries and adapted to our cultural conditions. It shows special care to preserve appearances while building a correct image as an organisation in good relations with the authorities, in conducting social dialogue and in presenting itself as a movement integrated with European society. Meanwhile, slowly but systematically and persistently it is building its influence in Muslim institutions and communities as well as local authorities. For years it has controlled many associations and centres of Islam.

Therefore, answering the question posed at the beginning whether the actions taken by the authorities could have the desired effect and contribute to calming the public mood, the author believes that only temporarily. Recently the projects created by the authorities of "old" EU countries and aimed at the so-called political Islam have a pro tempore and a propaganda character. Without changing the mindset of those Muslim minorities that are negative about Europe, all integration initiatives are doomed to failure. In the near term, social tensions are likely to explode with redoubled strength.

Abstract

The 2015 immigration crisis became a driving force for movements and parties that negate the current political order, including those that do not conceal their xenophobic slogans and ideas. In retrospect, there are more and more signs that the decision to accept the uncontrolled refugee influx was more an expression of wishful thinking than a rational decision, taking into account the actual political situation. Thus, Europe finds itself in a dangerous situation with far-right movements on the one hand, and radical Islam on the other. Each of these formations legitimises its existence and methods of operation by the existence of the other side, trying to polarise society and create a situation that will somehow force citizens to opt for one of the two options. Paradoxically, Chancellor Merkel's decision to admit immigrants significantly increased the risk of such a scenario, hence the perception of Islamic and right-wing extremism by the German authorities as posing an equal threat to state security. However, it was only the recent terrorist attacks in October and November 2020 in France and Germany that changed the political narrative.

Keywords: immigration, integration, Islam, politicians, political correctness, radicalism, multiculturalism.

REMIGIUSZ ROSICKI
ORCID: 0000-0002-1187-5895

DOI: 10.4467/20801335PBW.21.018.13575

State security as exemplified by the fight against terrorism: a choice between the well-being of the individual and the well-being of the community

Introduction

The objective scope of the research problem is concerned with offences against the state and the state's reaction to the related threats. The specified research object constitutes an interest protected under the Polish criminal law. It is noteworthy that the Polish legislature adopted a narrow understanding of offences against the state. With regard to the protected interest, as it is understood *sensu stricto*, offences against the state include coup d'état, espionage, diplomatic treason, intelligence disinformation, etc. While under Polish law offences against the state are delimited by the protected interest, which the legislature found to be the determinant in the classification of offences, as well as to be the goal it set itself in the criminal policy. Whereas in the legislation adopted in other countries, or legal policy broadly conceived, including political sciences, the meaning of offences against the state is usually more broadly defined. For instance, the group of offences against the state *sensu largo* includes such acts as sabotage, subversion and various types of acts of terrorism. Hence, the objective scope of the analysis concerns offences against the state *sensu largo*, as exemplified by terrorist offences and the state's reaction to the related threats.

Noteworthily, the Polish legislature employs a category of terrorist offences that is narrower than the colloquial category of terrorist acts, or terrorism itself. To define the category of terrorist offence, the Polish legislature used the legal definition in Art. 115 §20 of the Criminal Code (as implementation of the solutions adopted within the European Union). However, it must be noted that in spite of the fact that formal and material prerequisites are indicated, the very legal definition of terrorist offences makes it possible to treat many acts penalised under the Polish criminal law as

terrorist offences.[1] In consequence, this solution may potentially breach the principle of proportionality referred to within the constitutional norms.

In a democratic state ruled by law and a liberal democracy the problematic thing is to make decisions contrary to the interpreted hierarchy of constitutional principles, which can be illustrated with the clash between such principles as dignity and the common good. The clash gains in strength as the state has recourse to – in its opinion – more effective measures, and by extension measures that result in intensive and extensive excesses in the fight against acts of terrorism. A situation like this is possible when the common good becomes more important than man's dignity, which - in highly simplified terms – can be viewed as such basic rights as life or freedom.[2]

The main purpose of this paper is to consider the acceptable scope of radical measures adopted in the fight against terrorism, while taking into account reinterpretation of the priorities in the hierarchy of constitutional principles in a democratic state ruled by law and a liberal democracy, as exemplified by the Polish law (and hence a particular type of the state's reaction to threats related to terrorist offences). A selected practical example can be furnished by one of defunct Polish rules of law, concerned with a possibility of making a discretionary decision with regard to consenting to destruction of a civil aircraft if it has been used as a means of

---

[1] Judgment of the Supreme Court of 26 June 2003, V C KN 432/01; R. Zgorzały, *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, "Prokuratura i Prawo" 2007, no. 7–8, pp. 58–79; T. Przesławski, *Cel w konstrukcji przestępstwa terrorystycznego*, "Prokuratura i Prawo" 2009, no. 5, pp. 17–28; R. Rosicki, *Information and Anti-terrorist Security of Poland. A Critical Analysis Exemplified with the Tasks and Activity of the Internal Security Agency*, "Studia Politologiczne" 2015, vol. 38, pp. 88–105; M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, Warszawa 2018, pp. 52–64; R. Rosicki, *Counter-Terrorist Security: the Example of the Special Powers of the Polish Special Services in the Field of Surveillance of Foreign Nationals*, "Przegląd Strategiczny" 2018, no. 11, pp. 263–277; A. Gasztold, P. Gasztold, *The Polish Counterterrorism System and Hybrid Warfare Threats*, "Journal Terrorism and Political Violence" 2020.

[2] Cf. P. Chalk, *West European Terrorism and Counter-Terrorism. The Evolving Dynamic*, London 1996; P. Chalk, *The Response to Terrorism as a Threat to Liberal Democracy*, "Australian Journal of Politics and History" 1998, vol. 44, no. 3, pp. 373–88; D.W. Davis, B.D. Silver, *Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America*, "The American Journal of Political Science" 2004, vol. 48, no. 1, pp. 28–46; P. Wilkinson, *Terrorism versus Democracy: The Liberal State Response*, London, New York 2006; B. Çinar, *The Relationship Between Terrorism and Liberal Democratic States*, "European Journal of Economic and Political Studies" 2010, vol. 3, no. 2, pp. 207–221; R. Rosicki, *Information and Anti-terrorist Security of Poland. A Critical Analysis Exemplified with the Tasks and Activity of the Internal Security Agency*, "Studia Politologiczne" 2015, vol. 38, pp. 88–105; B.E. Garcia, N. Geva, *Security Versus Liberty in the Context of Counterterrorism: An Experimental Approach*, "Terrorism and Political Violence" 2016, vol. 28, issue 1, pp. 30–48; L.Y. Hunter, *Terrorism, Civil Liberties, and Political Rights: A Cross-National Analysis*, "Studies in Conflict & Terrorism" 2016, vol. 39, issue 2, pp. 165–193; E. Shor, *Counterterrorist Legislation and Subsequent Terrorism: Does it Work?*, "Social Forces" 2016, vol. 95, no. 2, pp. 525–557; E. Shor et al., *Counterterrorist Legislation and Respect for Civil Liberties: An Inevitable Collision?*, "Studies in Conflict & Terrorism" 2018, vol. 41, no. 5, pp. 339–364.

terrorist attack (Art. 122a of Aviation Law).[3] Dignity and the common good have been recognised as the main constitutional principles that may determine discretion as to or a ban on special measures in the fight against terrorism, as exercised by the state. That is why on the one hand there is the priority of the well-being of the individual, and on the other hand – the priority of the well-being of the community. At the same time, on the one hand there is the position whereby priority is given to the rights and freedoms of the individual, while on the other hand there is the position whereby priority is given to the security of the community. Polarising these two priority values, and thus emphasising their opposing aspects is purposeful.

In order to elaborate the objective scope of the research problem it is legitimate to present the research question which – following appropriate reasoning – will be answered in the form of conclusions. The question that serves to elaborate the research problem is as follows: *To what extent is it possible to sacrifice the well-being of the individual (dignity, rights and freedoms) for the sake of the common good (security)?*

The analysis methodology is primarily based on the thought experiment consisting in the interpretation of the value hierarchy of the constitutional norms in a democratic state ruled by law and a liberal democracy. The two competing constitutional principles in a democratic state ruled by law and a liberal democracy are the principles of dignity and of the common good – it must be stressed, though, that this is a deliberate reduction of the problematic concerned with constitutional principles and their potential clash with other principles. Defining the ontological and epistemological position within naturalism and anti-naturalism, with regard to the subjectivity of the individual and the community, as well as the principles of dignity and the common good, will serve as the starting point for the thought experiment. Then, use will be made of the general presuppositions behind axiological essentialism with regard to the principles of dignity and the common good. With a view to argumentation based on the reinterpretation of the priority hierarchy of the constitutional principles in a democratic state ruled by law and a liberal democracy, where precedence is given to the principle of the common good, a loose reference is made to the intellectual achievements of such thinkers as Aristotle, J. J. Rousseau and C. Schmitt.

Theoretical dimension

A clash of values

In the first place there is a need to solve some fundamental ontological and epistemological problems which are connected with the subject matter addressed in the present text, i.e. the problems concerned with subjectivity of the individual and the community, as

[3] See *Aviation Law* Act of 3 July 2002 (Journal of Laws 2002 no. 130, item 1112); *Announcement by the Speaker of the Sejm of the Republic of Poland of 3 November 2005 on publication of the consolidated text of the national border protection act* (Journal of Laws 2005, no. 226, item 1944).

well as the principles of dignity and the common good. In the presented analysis both these issues are closely related; what is more, despite their dissimilarities, each one is permeated with the problematics of axiology.

The use of specific social or ethical categories involves a problem of their realness or conventionality, that is a problem of objectivism and subjectivism concerned with, for instance, knowledge and perception of reality. The idealised perspective of naturalism posits that there is a definite social reality presented by particular social and ethical categories; what is more, with the aid of suitable methods, it is possible to establish phenomena and recurring relationships between them. On the other hand, from the idealised perspective of anti-naturalism particular social and ethical categories are merely patterns subject to interpretation, and so the phenomena presented by particular categories do not exist independently, but emerge as a result of social creation, practices and above all discourse. Within the framework of idealised anti-naturalism, real cognition of social and ethical phenomena is not feasible, because they are objects of mere interpretation and play on senses.[4]

The objects of analysis in the present text are dignity and the common good, as constitutional principles whose interpreted superiority or inferiority will determine the nature of the individual or the community. Approaching the individual or collective subject in the context of naturalism or anti-naturalism gives rise to certain effects on the deliberations engaged in. One problem is concerned with the objectivity or subjectivity of existence of particular values, e.g. dignity and the common good. The assumption whereby dignity as a value is objective in character, and – what is more – exists independently will imply the existence of man's innate dignity. The assumption whereby the common good as a value is objective in character will imply the existence of an innate value – auspicious survival and development of the community. Deciding which one of the values is the priority, and by extension how the hierarchy of such values is structured, should, in the naturalist scheme of things, be objective. However, every choice and its justification will in the end have an axiological character, and so it will be merely an interpretation, a social construct. One might, then, say that when it comes to choosing values, their priority status and their hierarchy, social constructivism is indispensable.[5]

The anti-naturalist approach, based on social creation of knowledge, interpretation and play on senses, affords a possibility of reversing, in the hierarchy of values, the accepted order of protected interests, which are attributed to a democratic state ruled by law and a liberal democracy. Therefore, if we assume that the dignity of the individual is a priority in both kinds of democracy, then revising the hierarchy

---

[4] P. Furlong, D. Marsh (2010), *A Skin Not a Sweater: Ontology and Epistemology in Political Science*, in: *Theory and Methods in Political Science*, D. Marsh, G. Stoker (eds.), Basingstoke 2010, pp. 184–209; C. Parsons (2010), *Constructivism and Interpretive Theory*, in: *Theory and Methods in Political Science*, D. Marsh, G. Stoker (eds.), Basingstoke 2010, pp. 80–97; A. Grabler, *Epistemologia. Sandwiczowa teoria wiedzy*, Kraków 2019, pp. 145–149.

[5] Cf. P.L. Berger, T. Luckmann, *Społeczne tworzenie rzeczywistości*, Warszawa 2010.

results in the value of the common good coming to the fore. Of course, one might espouse the Aristotelian concept whereby the good of the individual can be realised only within the community. This would mean accepting that the common good in a democratic state ruled by law and a liberal democracy is one in which the individual's dignity must be realised. M. Piechowiak[6] is among those who are in favour of this solution, which might also be a possible resolution of the potential clash of values under the Polish constitutional order. However, such a resolution does not always resolve the problem of the clash of values in borderline situations, because one value cannot always be reconciled with another one, particularly if the existence of the community is endangered.

By way of illustration, one might point out that under the Polish constitutional order priority was given to the common good by virtue of the April Constitution, which was in force in the years 1935–1944. Already the first article of this Constitution mentions the common good. The general good is mentioned in, inter alia, Article 5, which indicates that personal values and selected freedoms are delimited by precisely this general good. Besides, Article 7 contains the provision that an individual be evaluated through the prism of the general good. This is expressed in a principle whereby an individual's entitlement to influence public matters should be conditional upon their efforts made and services rendered towards the general good. However, it must be noted that the April Constitution contains elements of the Aristotelian concept of the realisation of an individual's good within the common good, as evidenced by the contents of Article 9: "*The state aims to unite all the citizens in harmonious cooperation for the sake of the general good*." Still, this sentence can be interpreted not only in the Aristotelian, but also in the reverse, or even totalitarian spirit. Given this context, the purport of Article 10 of the Constitution is not too optimistic; it reads as follows: "*no action can stand in contradiction to the goals of the State which are articulated in its rights*" and "*in the event of opposition, the State will have recourse to measures of restraint*."[7]

The common good

M. Piechowiak distinguishes two classical traditions with regard to the conception of the common good, one that refers to Aristotle's thought, and the other that refers to N. Machiavelli's thought.[8] The distinction made by Piechowiak, in the context of

---

[6] M. Piechowiak, *Prawne a pozaprawne pojęcia dobra wspólnego*, in: *Dobro wspólne. Teoria i praktyka*, W. Arndt, F. Longchamps de Bérier, K. Szczucki (eds.), Warszawa 2003, pp. 23–65; M. Piechowiak, *Konstytucyjna zasada dobra wspólnego – w poszukiwaniu kontekstu interpretacji*, in: *Dobro wspólne. Problemy konstytucyjnoprawne i aksjologiczne*, W.J. Wołpiuk (ed.), Warszawa 2008, pp. 123–158.

[7] *The Constitutional Act* of 23 April 1935 (Journal of Laws 1935, no. 30, item 227). See also M. Piechowiak, *Filozoficzne podstawy rozumienia dobra wspólnego*, "Kwartalnik Filozoficzny" 2003, no. 31, vol. 2, pp. 5–35.

[8] M. Piechowiak, *Prawne a pozaprawne*…, pp. 23–65; M. Piechowiak, *Konstytucyjna zasada dobra*…, pp. 123–158.

the above thinkers, does not seem to be relevant on account of the fact that both Aristotle and Machiavelli wrote about the community in the context of broadly conceived *bios politikos*. What is more, successful management of the community with a view to attaining the common (supreme) good is in Aristotle's case a kind of art (Greek *techne*), while in Machiavelli it consists in skilful elimination of conflicts, and the guarantee of the people's safety is one of the ruler's virtues (Greek *areté*), i.e. proficiency or astuteness evinced in public matters. The culture has acknowledged Aristotle's adequate concept of politics as having a positive overtone, while Machiavelli's concept of politics as having an extremely negative one. This distinction appears to be erroneous, because both thinkers meant the common good. In the case of Machiavelli for that matter any necessary and pragmatic conduct on the part of the authority (Latin *necessitas*), negatively read by many interpreters, would be meaningless, if it did not serve the prosperity and existence of the community. If the community ceased to exist, the ruler would have nothing to rule. Still, there is no doubt that for Aristotle the interest of the community lies in happiness, while for Machiavelli – in propitiousness and existence. Hence, according to Aristotle the well-being of the individual is happiness that consists in acting in accordance with the soul (psychic goods), while in Machiavelli the well-being of the individual is about happiness understood in a more material sense. Still, a variety of intellectual traditions that invoke these thinkers tend to interpret the relations between the community and the individual differently on account of the very fact that they evaluate these subjects.[9]

Following Piechowiak, one should point out that the common good has at least two meanings. As regards the first one, we can speak about the common good in the subjective sense, while as regards the second one – in the objective sense.[10] Hence, in the first case we speak about propitiousness and survival, as well as the development of the community as a subject – its members, to be more precise – while in the second case, we mean the conditions for its propitiousness, survival and development. Such a division is helpful in effective deconstruction of the concept of the common good. A more interesting problem concerned with the common good is the question whether it is objective or subjective in character, as well as whether it is developed by the collective subject (a political community), or perhaps it is an effect of the development of the general

[9] N. Machiavelli, *The Prince*, Cambridge 2008; Arystoteles, *Etyka nikomachejska*, Warszawa 2012; Arystoteles, *Polityka*, Warszawa 2012. See also W. Jaeger, *Paideia: The Ideals of Greek Culture. Vol. I: Archaic Greece. The Mind of Athens*, Oxford 1946, pp. 3–14; G. Reale, *Historia filozofii starożytnej. Tom II*, Lublin 1997, pp. 473–525; W. Buchner, *Wojna i konkwista. Hiszpańska myśl polityczna Złotego Wieku*, Kraków 2007, pp. 135–160; A. Rzegocki, *Racja stanu a polska tradycja myślenia o polityce*, Kraków 2008, pp. 103–217; S. Opara, *Tyrania złudzeń. Studia z filozofii polityki*, Warszawa 2009, pp. 23–26; I. Pańków, J. Pańków, *Polityka jako sztuka skutecznego rządzenia: Niccolò Machiavelli*, in: *Koncepcje polityki*, W. Wesołowski (ed.), Warszawa 2009, pp. 127–156; F. Raimondi, »Necessità« nel Principe e nei Discorsi di Machiavelli, "Scienza & Politica" 2009, vol. 21, no. 40, pp. 27–50; H. Arendt, *Kondycja ludzka*, Warszawa 2010, pp. 41–100; E. Voeglin, *Arystoteles*, Warszawa 2011, pp. 19–153; D. Quaglioni, *Machiavelli, the Prince and the Idea of Justice*, "Italian Culture" 2014, vol. 32, no. 2, pp. 110–121.

[10] M. Piechowiak, *Prawne a pozaprawne*…, pp. 23–65.

will, which J. J. Rousseau writes about in *The Social Contract*, etc. If we were to abide by the ideas propounded by J. J. Rousseau, then the only subject in a position to lay down the content of a law – what can or cannot be done - would be the people as the only sovereign, in accordance with the rule whereby the people subject to the laws should be their author. This does not, however, mean that J. J. Rousseau does not provide for a lawgiver figure in the capacity of *spiritus movens* at the dawn of the emergent political community.[11]

The question of the community and power orients us towards the problematics addressed by C. Schmitt in his works. From the theoretical perspective, the author's concept of the political is most seminal. The situation of the community is political in character if the entire community defines its enemy. Defining a political enemy has an existential meaning, and by no means is this situation reducible to the symbolical or metaphorical. This means that the public enemy (Latin *hostis humani generis*) is the one who really threatens the existence of the entire community. Noteworthily, ascribing the public enemy status to someone is not synonymous with declaring war, as the war only unveils the ultimate consequence of the people being politically unified in line with the division. In the context of this concept, the political community can consider subjects committing acts of terrorism public enemies, but "war on terrorism" itself does not constitute the political for C. Schmitt. Therefore, it can be concluded that an exceptional or critical situation gives rise to a political unity, which can be identified with pointing to some good, and measures that the community wants to take to obviate potential danger. Hence, real power is exercised by anyone who in a critical situation has the right to determine who the enemy (*hostis*) is, and who disposes of their life and death. Extraordinary measures in the fight against terrorism can then be considered in the context of the suspension of the legal order found to be lawful. The problem that remains unresolved till this day is the question as to what should be regarded as a critical situation that entitles particular subjects or the entire political community to specific actions and to make them legally valid.[12]

---

[11] J.J. Rousseau, *Umowa społeczna,* Kęty 2002. See also Cz. Porębski, *Umowa społeczna według Jana Jakuba Rousseau*, "Etyka" 1986, no. 22, pp. 215–229; M. Blaszke, *Umowa społeczna J. J. Rousseau: polityka i racjonalność*, "Archiwum Historii Filozofii i Myśli Społecznej" 1987, vol. 32, pp. 41–74; M. Ludwisiak, *Postać Jana Jakuba Rousseau i jego wpływ na współczesnych*, "Acta Universitatis Lodziensis. Folia historica" 2007, no. 81, pp. 87–107; D. Pietrzyk-Reeves, *Podstawy zgody i dyskursu publicznego w koncepcji umowy społecznej Jana Jakuba Rousseau*, "Krakowskie Studia z Historii Państwa i Prawa" 2010, vol. 3, pp. 333–349; P. Pasterczyk, *Koncepcja umowy społecznej i natury człowieka u J.J. Rousseau w świetle teorii pożądliwości mimetycznej R. Girarda*, "Przegląd Filozoficzny – Nowa Seria" 2012, no. 4, pp. 373–387; R. Lis, *Jean Bodin, John Locke i Jean Jacques Rousseau. O paradoksie suwerenności i ludowładztwa oraz próbach jego rozwiązania*, "Studia Polityczne" 2014, no. 34, pp. 69–83.

[12] C. Schmitt, *Teologia polityczna i inne pisma*, Kraków 2000, pp. 191–250; C. Schmitt, *Teologia polityczna 2*, Warszawa 2014, pp. 21–34; C. Schmitt, *Dyktatura*, Warszawa 2016, pp. 21–46; See also R. Cristi, *Carl Schmitt and Authoritarian Liberalism*, Llandybie 1998, pp. 169–178; P. Kaczorowski, *Polityczność jako sposób egzystencji podmiotu zbiorowego. Koncepcja Carla Schmitta*, in: *Koncepcje polityki*, W. Wesołowski (ed.), Warszawa 2009, pp. 192–209; M. Freeden, *The Political Theory of*

Practical dimension

in the context of the conflict between the two different values, i.e. dignity and the common good, it is worth considering a provision in Article 122a, now defunct, of the Polish Aviation Law. The article made it possible to shoot down an aircraft if it became a means of terrorist attack. Undoubtedly, this solution is structured around a peculiar form of a state of higher necessity or necessary self-defence, which the Polish legislature contained in the general part of the Criminal Code (to some extent also the justification of ultimate need).[13] From the ethical viewpoint, the content of this legal solution exemplifies utilitarianism, if we acknowledge that the only goal is the well-being of the community or a larger group of individuals at the cost of a smaller group, or at the cost of particular individuals. Of course, such a simple conception of utilitarianism would not account for the complexity of presuppositions resulting from the assessment of social utility in accordance with the so-called utility calculus (hedonic calculus). At this point one might also reference one well-known philosophical and cognitive experiment concerned with the trolley (switch) problem. This dilemma appears to appropriately illustrate the legal construction of the solution adopted by the Polish legislature in the Aviation Law.[14]

Prior to the Constitutional Tribunal ruling of 2008, the provision in Article 122a of the Aviation Law reads as follows: "If it is required on the grounds of state security, and if the air defence command, while taking into account particularly the information communicated by the institutions providing air traffic service, finds that a civil aircraft is being used for actions against the law, and especially as a means of terrorist attack from the air, the aircraft may be destroyed in accordance with the rules specified in the national border protection act of 12 October 1990 (Journal of *Laws 2005, no. 226, item 1944)*."[15] However, the Constitutional Tribunal found the above-quoted provision to be unconstitutional on account of the following breaches of the principles, and clashes

Political Thinking, Oxford 2013, pp. 59–60.

[13] *Prawo karne materialne. Część ogólna i szczególna*, M. Bojarski (ed.), Warszawa 2017, pp. 166–186, 211–212; J. Warylewski, *Prawo karne. Część ogólna*, Warszawa 2017, pp. 323–336, 339–340, 422–424; *Prawo karne. Część ogólna, szczególna i wojskowa*, T. Dukiet-Nagórska (ed.),Warszawa 2018, pp. 175–186, 199–200, 559–560; Ł. Pohl, *Prawo karne. Wykład części ogólnej*, Warszawa 2019, pp. 291–307, 360–363.

[14] Cf. J.J. Thomson, *The Trolley Problem*, "The Yale Law Journal" 1985, vol. 94, no. 6, pp. 1395–1415; F.M. Kamm, *Harming Some to Save Others*, "Philosophical Studies" 1989, vol. 57, no. 3, pp. 227–256; P. Vardy, P. Grosch, *Etyka*, Poznań 2010, pp. 68–76; E. Awad, S. Dsouza, R. Kim et al., *The Moral Machine Experiment*, "Nature" 2018, vol. 563, pp. 59–64.

[15] The article, with such a wording of this provision, was in effect between 01 IV 2007 and 02 X 2008. *See Announcement by the Speaker of the Sejm of the Republic of Poland of 3 November 2005 on publication of the consolidated text of the national border protection act* (Journal of Laws 2005, no. 226, item 1944).

of values: (1) the principle of the right to life, (2) the principle of proportionality, (3) the principle of adequacy, (4) the principle of subsidiarity.[16]

In fact, in the Polish system of constitutional principles, the right to life is not provided with an absolute guarantee, which means that it can be protected with varying degrees of intensity. However, because of the clash of values and constitutional goods, it is posited that their restriction is possible, but in the case of a clash with values and goods of lower standing in the interpreted constitutional hierarchy no consent should be granted. In a case like this, consent to the use of special measures and means of fight against terrorism (a decision to shoot down an aircraft) would be tantamount to voluntary manslaughter. What is more, the provision would allow use of special means and methods relative to killing with a view to saving goods of lower standing in the constitutional hierarchy (e.g. goods of material character only).

Also, of great significance is the reference, made by the Polish legislature in the defunct Article 122a of the Aviation Law, to quite an abstract category of "state security," which cannot but be seen as an indeterminate phrase. This category is quite important in criminal law on account of the protected interest, with the aid of which the Polish legislature defined penalised acts, but it does not by any means materially coincide with the act mentioned in the defunct Article 122a of the Aviation Law. Therefore, the Polish law has not *de facto* developed a category of state security as a general clause that the judiciary and law-enforcement authorities might refer to in an unambiguous manner.

Likewise, the category of state security is debatable on account of the fact that a government agency would thus consent to the killing of passengers whose safety the state itself failed to guarantee, thereby allowing them to become hostages to individuals using an aircraft as a means of terrorist act. Besides, the Polish legislature indicated the conditions for deeming the aircraft as used for actions against the law in a non-transparent manner. The problem of the lack of transparency also concerns the mechanism for verifying the existing state of threat of a terrorist attack. It infringes upon the individual's freedoms and rights resulting from their dignity, and inappropriately realises the principle of proportionality with regard to the competence to their limitation. In such a reading, the content of the defunct Article 122a of the Aviation Law is in breach of the constitutional ban on the infringement of the human dignity. The constitutional norms provide that dignity is due to everyone, and so it is an essence of humanness, which means that the passengers on board of an aircraft are deprived of legal protection in order that a rescue operation can be mounted for the sake of other individuals, whereas they should also be covered by the rescue operation in the first place. Thus, it can be clearly seen that this line of reasoning cuts across the essential division into two opposing values, i.e. the well-being of the individual and the well-being of the community, by including the endangered passengers in the community.

[16] The Constitutional Tribunal Ruling of 30 September 2008, File no. K 44/07.

As mentioned before, the content of the defunct Article 122a of the Aviation Law resembles solutions concerned with the institutions of the state of higher necessity and necessary self-defence, in force under the Polish law. In the case the state of higher necessity, one should consider what kind of situation we are dealing with in regard to the clash of values. As we make liberal use of the provision concerned with higher necessity, we can consider two cases. In the first one, we can assume that in the event of a direct threat to the lives of community members, if the danger of a terrorist attack cannot be averted otherwise, and the interest sacrificed is less valuable than the interest saved, then the aircraft will be shot down, and the perpetrator will not be deemed to have committed an offence. In the second one, we can assume that in the event of a direct threat to the lives of community members, if the danger of a terrorist attack cannot be averted otherwise, and the interest sacrificed is not obviously more valuable than the interest saved, then the aircraft will be shot down, and the perpetrator will not be deemed to have committed an offence. This division is meaningful with regard to the very institution of the state of higher necessity under the Polish law, because in the case of saving one interest at the cost of another interest of lesser value, we are dealing with circumstances excluding the unlawfulness of the act. As regards saving one good at the cost of another good which is not obviously more valuable, we are only dealing with circumstances excluding guilt. With regard to the institution of the state of higher necessity, one good, which is a life, is a good of neither lesser nor greater value. Life is then a good that is not obviously more valuable, if it is necessary to save one life at the cost of another. The division of the situation into the two above-mentioned cases of shooting down aircraft, with regard to the value of life, would be meaningless, were the interpretation based on the primacy of the individual's dignity to be adopted. But if the primacy of the community's interest is adopted, life as a value becomes highly gradable, and dignity is no longer an inalienable value. There only remains the problem of the measurability of quantitative life relative to the first and the second case – both as a good saved and a good sacrificed. In a case like this it would be necessary to apply the utility calculus (hedonic calculus) in order to save one life at the cost of another.

The problem of the defunct Article 122a of the Aviation Law can also be considered through the prism of the content of the institution of necessary self-defence under the Polish criminal law. Given a loose interpretation of the provision concerned with necessary self-defence, we can consider a situation in which a person responsible for shooting down an aircraft does not commit an offence, if they ward off a direct and unlawful attack on the lives of community members – in this case, a terrorist attack involving the use of an aircraft. It is clear that under the existing interpretation of the institution of necessary self-defence, warding off the attack by shooting down an aircraft is an intensive and extensive excess, and so constitutes a violation of the conditions for necessary self-defence. As regards the intensive excess, the measures and manners applied would be too intense. As regards the extensive excess, the measures and manners applied would be non-contemporaneous with the immediacy of the terrorist attack. In the very institution of necessary self-defence,

the Polish legislature attempts to weigh the application scope for this institution in society on account of, inter alia, the dignity due to every individual. If we were to adopt the interpretation based on the primacy of the community's interest, which in this case is the primacy of security, then every subject in breach of the auspiciousness of the survival and development of the community may be treated as a public enemy. This line of reasoning, however, displays a peculiar flaw, because the use of an aircraft as a means of terrorism presupposes a possibility of killing the passengers, who are by no means consciously involved in any terrorist attack. In the scheme of the primacy of the community's interest, if the passengers constitute a part of the endangered community (e.g. because of the citizenship they hold or a different kind of affiliation with the community), this will also be problematic. In a situation like this it will be more appropriate to consider the problem of shooting down the aircraft pursuant to Article 122a of the Aviation Law as a peculiar form of the state of higher necessity rather than necessary self-defence.

Conclusion

The starting point for the analysis performed in the text is theoretical consideration concerned with such opposing categories as objectivism (naturalism) and subjectivism (anti-naturalism), dignity and the common good, the individual and the community. The text analyses offences against the state *sensu largo*, and the state's reaction to the related threats. The problematics of offences against the state is reduced to terrorist offences, and the problematics of the state's reaction is reduced to the application of special measures in the fight against terrorism. An unconstitutional provision contained in Art. 122a of the Aviation Law has been chosen as a practical example of special measures employed by the state. A special character of this provision lies in its authorisation to make a discretionary decision with regard to consenting to the destruction of a civil aircraft, if it is used as a means of terrorist attack. In order to elaborate the objective scope of the analysis, the following research question has been formulated in the text: *To what extent is it possible to sacrifice the well-being of the individual (dignity, rights and freedoms) for the sake of the common good (security)?*

There is no doubt that from the ethical viewpoint sacrificing the well-being of the individual, i.e. their dignity, rights and freedoms for the sake of the common good as expressed in the category of safety is subject to evaluation. Right from the start there is the problem of evaluating values and their hierarchy. If we adopt the anti-naturalist position, we must acknowledge that there is no objectively innate human dignity, and that it is only a social construct subject to interpretation. Such a presupposition also results in the necessity to adopt a constructivist approach to the value hierarchy, where the priorities of the constitutional principles in a democratic state ruled by law and a liberal democracy are subject to evaluation and liberal classification, frequently for instrumental reasons or on account of a choice of a new overriding characteristic, which

may be the effect of both instrumental and axiological actions. A practical example can be furnished by the relationship between the well-being of the individual and the well-being of the community, as well as the question as to the degree to which the well-being of one subject can be sacrificed for the sake of the well-being of another. The scope and degree in which the individual's well-being, e.g. their life, is taken into account and protected, constitutes an immanent part of ethical deliberation. It is frequently accepted that life is the superior value in legal systems of particular countries, but at the same time it is assumed that despite such a status, life is protected with varying degrees of intensity. This discussion allows for an evaluation of the special measures that the state – especially a democratic state ruled by law and a liberal democracy – tends to employ in the fight against terrorism. It must be clearly indicated that the content of the defunct Article 122a of the Aviation Law granted primacy to the common good (the community as the subject) at the cost of the individual good (the individual as the subject).

In 2008 the Constitutional Tribunal, while investigating the problem of the constitutionality of Article 122a of the Aviation Law, ruled that the protection of an individual life is related to the clause of the democratic state ruled by law. This means that this type of state is realised only as a community of people, even though only people are proper subjects of rights and obligations. Therefore, depriving an individual of their life is tantamount to depriving them of their rights and obligations. Even though the concept of the relation between the individual and the community goes beyond the essentialism of the two subjects, and by extension the essentialism of the two values, it points to a lack of the privileged position of the community in regard to the possibilities for limiting an individual's life in the state of higher necessity, e.g. hijacking an aircraft with a view to committing a terrorist act. Furthermore, the Constitutional Tribunal opts for the interpreted hierarchy of values that is underpinned by the supremacy of the value of human life. In the event of a clash with lower-order values, there should be no room for limiting this value. This, however, does not resolve the dilemma specified in the institution of the state of necessity, featuring two competing interests which, in relation to each other, are not values of obviously higher standing (e.g. life). Also, this does not preclude a possible construction of a legal norm based on a state of necessity construct contained in the Polish criminal law as *lex specialis*.

Therefore, one can clearly see that in the scheme of legal systems based on the principles of a democratic state ruled by law and a liberal democracy there are various kinds of restrictions with regard to the use of special measures in the fight against terrorism. Undoubtedly, every event that disturbs the community's sense of security affords a potential opportunity to use it to reinterpret the hierarchy of both ethical and constitutional values, which results in the state's unwarranted interference in the individual's goods such as dignity, rights and freedoms, and of course life itself. Conversely, such processes can be interpreted as a deliberate suspension of the legal order regarded as lawful in a political community's critical situation.

Bibliography

Arendt H., *Kondycja ludzka*, Warszawa 2010, Fundacja Aletheia.

Arystoteles, *Etyka nikomachejska*, Warszawa 2012, Wydawnictwo Naukowe PWN.

Arystoteles, *Polityka*, Warszawa 2012, Wydawnictwo Naukowe PWN.

Awad E. et al., *The Moral Machine experiment*, "Nature" 2018, vol. 563.

Berger P.L., Luckmann T., *Społeczne tworzenie rzeczywistości*, Warszawa 2010, Wydawnictwo Naukowe PWN.

Blaszke M., *Umowa społeczna J.J. Rousseau: polityka i racjonalność*, "Archiwum Historii Filozofii i Myśli Społecznej" 1987, t. 32.

Buchner W., *Wojna i konkwista. Hiszpańska myśl polityczna Złotego Wieku*, Kraków 2007, Ośrodek Myśli Politycznej.

Chalk P., *The Response to Terrorism as a Threat to Liberal Democracy*, "Australian Journal of Politics and History" 1998, no. 3.

Chalk P., *West European Terrorism and Counter-Terrorism. The Evolving Dynamic*, London 1996, Palgrave Macmillan.

Cristi R., *Carl Schmitt and authoritarian liberalism, Llandybie 1998*, University of Wales Press.

Davis D.W., Silver B.D., *Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America*, "The American Journal of Political Science" 2004, no. 1.

Dobro wspólne. Problemy konstytucyjnoprawne i aksjologiczne, Wołpiuk W.J. (ed.), Warszawa 2008, Wyższa Szkoła Zarządzania i Prawa im. Heleny Chodkowskiej w Warszawie.

Dobro wspólne. Teoria i praktyka, W. Arndt, F. Longchamps de Bérier, K. Szczucki (eds.), Warszawa 2013, Wydawnictwo Sejmowe, Fundacja "Utiriusque iuris".

Freeden M., *The political Theory of Political Thinking*, Oxford 2013, Oxford University Press.

Furlong P., Marsh D., Ercan S.A., *A Skin Not a Sweater: Ontology and Epistemology in Political Science*, in: *Theory and methods in political science*, V. Lowndes, D. Marsh, G. Stoker (eds.), Basingstoke 2010, Red Globe Press.

Gabriel-Węglowski M., *Działania antyterrorystyczne*. Komentarz, Warszawa 2018, Wolters Kluwer.

Garcia B.E., Geva N., *Security Versus Liberty in the Context of Counterterrorism: An Experimental Approach*, "Terrorism and Political Violence" 2016, issue 1.

Gasztold A., Gasztold P., *The Polish Counterterrorism System and Hybrid Warfare Threats*, "Journal Terrorism and Political Violence" 2020.

Grabler A., *Epistemologia. Sandwiczowa teoria wiedzy*, Kraków 2019, Wydawnictwo Universitas.

Hunter L.Y., *Terrorism, Civil Liberties, and Political Rights: A Cross-National Analysis*, "Studies in Conflict & Terrorism" 2016, issue 2.

Jaeger W., *Paideia: The Ideals of Greek Culture. Vol. I: Archaic Greece*. The Mind of Athens, Oxford 1946, Oxford University Press.

Kaczorowski P., *Polityczność jako sposób egzystencji podmiotu zbiorowego. Koncepcja Carla Schmitta*, in: *Koncepcje polityki*, W. Wesołowski (ed.), Warszawa 2009, Wydawnictwo Naukowe Scholar.

Kamm F.M., *Harming Some to Save Others*, "Philosophical Studies" 1989, no. 3.

Koncepcje polityki, W. Wesołowski (ed.), Warszawa 2009, Wydawnictwo Naukowe Scholar.

Lis R., *Jean Bodin, John Locke i Jean Jacques Rousseau. O paradoksie suwerenności i ludowładztwa oraz próbach jego rozwiązania*, "Studia Polityczne" 2014, no. 34.

Ludwisiak M., *Postać Jana Jakuba Rousseau i jego wpływ na współczesnych*, "Acta Universitatis Lodziensis. Folia historica" 2007, no. 81.

Machiavelli N., *The Prince*, Cambridge 2008, Cambridge University Press.

Opara S., *Tyrania złudzeń. Studia z filozofii polityki*, Warszawa 2009, MUZA.

Pańków I., Pańków J., *Polityka jako sztuka skutecznego rządzenia: Niccolò Machiavelli*, in: *Koncepcje polityki*, W. Wesołowski (ed.), Warszawa 2009, Wydawnictwo Naukowe Scholar.

Parsons C., *Constructivism and Interpretive Theory*, in: *Theory and methods in political science*, D. Marsh, G. Stoker (eds.), Basingstoke 2010, Red Globe Press.

Pasterczyk P., *Koncepcja umowy społecznej i natury człowieka u J.J. Rousseau w świetle teorii pożądliwości mimetycznej R. Girarda*, "Przegląd Filozoficzny – Nowa Seria" 2012, no. 4 (84).

Piechowiak M., *Filozoficzne podstawy rozumienia dobra wspólnego*, "Kwartalnik Filozoficzny" 2003, no. 2.

Piechowiak M, *Prawne a pozaprawne pojęcia dobra wspólnego*, in: *Dobro wspólne. Teoria i praktyka*, W. Arndt, F. Longchamps de Bérier, K. Szczucki (eds.), Warszawa 2013, Wydawnictwo Sejmowe, Fubdacja "Utiriusque iuris", s. 23–45.

Piechowiak M., *Konstytucyjna zasada dobra wspólnego – w poszukiwaniu kontekstu interpretacji*, in: *Dobro wspólne. Problemy konstytucyjnoprawne i aksjologiczne*, W.J. Wołpiuk (ed.), Warszawa 2008, Wyższa Szkoła Zarządzania i Prawa.

Pietrzyk-Reeves D., *Podstawy zgody i dyskursu publicznego w koncepcji umowy społecznej Jana Jakuba Rousseau*, "Krakowskie Studia z Historii Państwa i Prawa" 2010, vol. 3.

Pohl Ł., *Prawo karne. Wykład części ogólnej*, Warszawa 2019, Wolters Kluwer.

Porębski Cz., *Umowa społeczna według Jana Jakuba Rousseau*, "Etyka" 1986, no. 22.

Prawo karne. *Część ogólna, szczególna i wojskowa*, T. Dukiet-Nagórska (ed.), Warszawa 2018, Wolters Kluwer.

Prawo karne materialne. Część ogólna i szczególna, M. Bojarski (ed.), Warszawa 2017, Wolters Kluwer.

Przesławski T., *Cel w konstrukcji przestępstwa terrorystycznego*, "Prokuratura i Prawo" 2009, no. 5.

Quaglioni D., *Machiavelli, the Prince and the Idea of Justice*, "Italian Culture" 2014, no. 2.

Raimondi F., »*Necessità« nel Principe e nei Discorsi di Machiavelli*, "Scienza & Politica" 2009, no. 40.

Reale G., *Historia filozofii starożytnej. Tom II*, Lublin 1997, Redakcja Wydawnictw Katolickiego Uniwersytetu Lubelskiego.

Rosicki R., *Information and anti-terrorist security of Poland. A critical analysis exemplified with the tasks and activity of the Internal Security Agency*, "Studia Politologiczne" 2015, vol. 38.

Rosicki R., *Counter-Terrorist Security: The Example of the Special Powers of the Polish Special Services in the Field of Surveillance of Foreign Nationals*, "Przegląd Strategiczny" 2018, no. 11.

Rousseau J.J., *Umowa społeczna*, Kęty 2002, Wydawnictwo Antyk.

Rzegocki A., *Racja stanu a polska tradycja myślenia o polityce*, Kraków 2008, Ośrodek Myśli Politycznej.

Schmitt C., *Teologia polityczna i inne pisma*, Kraków 2000, Wydawnictwo Aletheia.

Schmitt C., *Teologia polityczna 2*, Warszawa 2014, Wydawnictwo Aletheia.

Schmitt C., *Dyktatura*, Warszawa 2016, Fundacja Augusta hr. Cieszkowskiego.

Shor E., *Counterterrorist Legislation and Subsequent Terrorism: Does it Work?*, "Social Forces" 2016, no. 2.

Shor E. et al., *Counterterrorist Legislation and Respect for Civil Liberties: An Inevitable Collision?*, "Studies in Conflict & Terrorism" 2018, no. 5.

Theory and methods in political science, D. Marsh, G. Stoker (eds.), Basingstoke 2010, Red Globe Press.

Thomson J.J., *The Trolley Problem*, "The Yale Law Journal" 1985, no. 6.

Vardy P., Grosch P., *Etyka*, Poznań 2010, Zysk i S-ka.

Voeglin E., *Arystoteles*, Warszawa 2011, Fundacja św. Mikołaja.

Warylewski J., *Prawo karne. Część ogólna*, Warszawa 2017, Wolters Kluwer.

Zgorzały R., *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, "Prokuratura i Prawo" 2007, no. 7–8.

Legal acts

Announcement by the Speaker of the Sejm of the Republic of Poland of 3 November 2005 on publication of the consolidated text of the national border protection act (Journal of Laws 2005, no. 226, item 1944).

Act of 3 July 2002 on Aviation Law (Journal of Laws 2002 no. 130, item 1112).

Constitutional Act of 23 April 1935 (Journal of Laws 1935, no. 30, item 227).

Judical decision

Constitutional Tribunal Ruling of 30 September 2008, File no. K 44/07.

Judgment of the Supreme Court of 26 June 2003, V C KN 432/01.

Abstract

The objective scope of the analysis encompasses special measures used in the fight against terrorism in the context of ethical and constitutional principles attributed to a democratic state ruled by law and a liberal democracy. A practical example of a special measure used in the fight against terrorism, and presented in the text, is furnished by the content of one of the articles in the Polish Aviation Law, which was found unconstitutional in 2008. The content of this article made it possible for an administrative authority to make a decision with regard to consenting to the destruction of a civil aircraft, if it was used as a means of terrorist attack.

The main purpose of the paper is to consider the acceptable scope of radical measures in the fight against terrorism, while taking into account the reinterpretation of priorities in the hierarchy of legal principles. In order to elaborate the objective scope of the analysis, the following research question is phrased: *To what extent is it possible to sacrifice the well-being of the individual (dignity, rights and freedoms) for the sake of the common good (security)?*

The adopted analysis methodology is based on a thought experiment consisting in the reinterpretation of ethical principles and the values of the constitutional norms in a democratic state ruled by law and a liberal democracy. With the benefit of essentialist reduction, it is posited that the two competing constitutional principles are the principle of dignity and the principle of the common good; they can be reduced to, for instance, protection of the life of an individual or of members of the community as a whole.

Keywords: terrorism, aviation terrorism, security, state of higher necessity, human rights and freedoms, common good.

Abstrakt

Zakres przedmiotowy analizy obejmuje zagadnienie szczególnych środków walki z terroryzmem w kontekście zasad etycznych i konstytucyjnych przypisanych demokratycznemu państwu prawa i demokracji liberalnej. Przykładem praktycznym szczególnego środka walki z terroryzmem zaprezentowanym w tekście jest treść jednego z artykułów polskiego Prawa lotniczego, który został uznany za niekonstytucyjny w 2008 roku. Treść artykułu dawała możliwość podjęcia decyzji przez organ administracji publicznej w zakresie wyrażenia zgody zniszczenia cywilnego statku powietrznego w sytuacji, gdy ten użyty jest jako środek ataku terrorystycznego.

Głównym celem pracy jest rozważanie zakresu dopuszczalności stosowania radykalnych środków walki z terroryzmem przy uwzględnieniu reinterpretacji priorytetów w hierarchii zasad prawnych. W celu uszczegółowienia zakresu przedmiotowego analizy zaprezentowano następujące pytanie badawcze: *W jakim zakresie możliwe jest poświęcenie dobra jednostki (godności, praw i wolności) na rzecz dobra wspólnego (bezpieczeństwa)?*

Metoda analizy opiera się na eksperymencie myślowym polegającym na reinterpretacji zasad etycznych i wartości norm konstytucyjnych w demokratycznym państwie prawa i demokracji liberalnej. Przyjęto za pomocą redukcji esencjonalnej, że dwie rywalizujące ze sobą zasady konstytucyjne, to zasada godności i zasada dobra wspólnego, które mogą być sprowadzone np. do ochrony życia jednostki lub członków wspólnoty jako całości.

Słowa kluczowe: terroryzm, terroryzm lotniczy, bezpieczeństwo, stan wyższej konieczności, prawa i wolności człowieka, wspólne dobro.

O autorach

Robert Borkowski – doktor habilitowany, profesor nadzwyczajny Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. Członek Rady Naukowej Centrum Badań nad Terroryzmem.

Paweł Gacek – doktor nauk prawnych, funkcjonariusz Komendy Miejskiej Policji w Krakowie.

Krzysztof Izak – emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Rafał Jurczak – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Andrzej Karaś – magister, laureat IX edycji ogólnopolskiego konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Maciej Aleksander Kędzierski – doktor nauk prawnych, radca prawny, emerytowany funkcjonariusz Policji.

Barbara Konior – funkcjonariuszka Agencji Bezpieczeństwa Wewnętrznego.

Mariusz Krzysztofiński – doktor habilitowany, Oddziałowe Biuro Badań Historycznych Instytutu Pamięci Narodowej w Rzeszowie.

Małgorzata Kudzin-Borkowska – magister politologii, doktorantka na Wydziale Nauk o Bezpieczeństwie Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, członek Polskiego Towarzystwa Bezpieczeństwa Narodowego.

Anna Łasińska – doktor, funkcjonariuszka Agencji Bezpieczeństwa Wewnętrznego.

Daniel Mider – doktor habilitowany nauk humanistycznych w zakresie nauk o polityce, wykładowca Uniwersytetu Warszawskiego i Szkoły Głównej Handlowej, certyfikowany informatyk śledczy.

Norbert Nowicki – magister prawa, laureat IX edycji ogólnopolskiego konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych, asystent Prokuratora Okręgowego w Białymstoku.

Paweł Pokrzywiński – absolwent Wydziału Nauk Społecznych Uniwersytetu Wrocławskiego oraz judaistyki w Instytucie Filologii Polskiej, doktorant w Instytucie Studiów Międzynarodowych Uniwersytetu Wrocławskiego.

Patryk Pucułek – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Remigiusz Rosicki – doktor habilitowany, profesor nadzwyczajny Uniwersytetu im. Adama Mickiewicza w Poznaniu, Executive Master of Business Administration (EMBA).

Tomasz Szczepański – doktor, funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Rafał Wądołowski – doktor nauk prawnych, inżynier, absolwent Wyższej Szkoły Oficerskiej w Toruniu oraz studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego, były oficer służby specjalnej.

Urszula Więckiewicz – funkcjonariuszka Agencji Bezpieczeństwa Wewnętrznego.

Ewa Aleksandra Ziemak – magister prawa, absolwentka Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego, wykładowczyni Uniwersytetu Otwartego Uniwersytetu Warszawskiego.

About the authors

Robert Borkowski – PhD with post-doctoral degree, associate professor of the Andrzej Frycz Modrzewski Krakow University, member of the Scientific Board of the Terrorism Research Center.

Paweł Gacek – PhD in law, Police officer in the Local Police Department in Cracow.

Krzysztof Izak – retired officer of the Internal Security Agency.

Rafał Jurczak – officer of the Internal Security Agency.

Andrzej Karaś – master's degree, laureate of the 9th edition of the Head of the Internal Security Agency national contest for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats.

Maciej Aleksander Kędzierski – PhD in law, legal counsel, retired police officer.

Barbara Konior – officer of the Internal Security Agency.

Mariusz Krzysztofiński – PhD with post-doctoral degree, Rzeszów Branch of the Historical Research Office of the Institute of National Remembrance.

Małgorzata Kudzin-Borkowska – Master's degree in political sciences, PhD at the Faculty of Security Studies at the Andrzej Frycz Modrzewski Krakow University, member of the Polish Association for National Security.

Anna Łasińska – PhD, officer of the Internal Security Agency.

Daniel Mider – PhD with post-doctoral degree in political sciences, lecturer at the University of Warsaw and Warsaw School of Economics, certified forensic analyst.

Norbert Nowicki – master's degree in law, laureate of the 9th edition of the Head of the Internal Security Agency national contest for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats, Assistant District Attorney in Białystok.

Paweł Pokrzywiński – graduate in social sciences at the University of Wrocław and in Jewish studies at the Institute of Polish Studies, postgraduate student at the Institute of International Studies at the University of Wrocław.

Patryk Pucułek – officer of the Internal Security Agency.

Remigiusz Rosicki – PhD with post-doctoral degree, Professor of Adam Mickiewicz University in Poznań, Executive Master of Business Administration (EMBA).

Tomasz Szczepański – PhD, officer of the Internal Security Agency.

Rafał Wądołowski – PhD in law, engineer, graduate of Military Academy in Toruń and of post-doctoral studies at the Faculty of Law and Administration at the University of Gdańsk, former special service officer.

Urszula Więckiewicz – officer of the Internal Security Agency.

Ewa Aleksandra Ziemak – master's degree in law, graduate of Law and Administration at the Cardinal Stefan Wyszyński University in Warsaw.

Informacje dla autorów czasopisma „Przegląd Bezpieczeństwa Wewnętrznego” i serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego

I. Zasady przyjmowania prac.

1. Redakcja „Przeglądu Bezpieczeństwa Wewnętrznego” przyjmuje do publikacji artykuły naukowe, recenzje oraz relacje z konferencji, dotyczące bezpieczeństwa wewnętrznego państwa i porządku konstytucyjnego. Przyjmowane są tylko materiały oryginalne, wcześniej niepublikowane i niezgłoszone do publikacji w innych czasopismach lub środkach przekazu elektronicznego (np. serwisy internetowe).
2. Przesłane publikacje nie mogą naruszać praw autorskich osób trzecich – w rozumieniu *Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych* (t.j.: DzU z 2019 r. poz. 1231, ze zm.).
3. Materiały należy przesyłać na adres redakcji: wydawnictwo@abw.gov.pl.
4. Przesyłając tekst do redakcji „Przeglądu Bezpieczeństwa Wewnętrznego”, autor wyraża zgodę na jego opracowanie redakcyjne, tj. na wykonanie redakcji merytorycznej, językowej i korekty, zgodnie z normami językowymi oraz na podstawie polskich norm wydawniczych. Wyraża także zgodę na opublikowanie informacji o artykule w naukowych bazach danych.
5. Materiały kierowane do druku w czasopiśmie „Przegląd Bezpieczeństwa Wewnętrznego” i w ramach serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego podlegają ocenie merytorycznej członków Redakcji i co najmniej dwóch recenzentów zewnętrznych.
6. Recenzje zewnętrzne mają formę pisemną i kończą się jednoznacznym wnioskiem o dopuszczeniu artykułu do publikacji (bez zmian lub po wprowadzeniu przez autora zmian sugerowanych przez recenzentów) lub jego odrzuceniu.
7. W przypadku dwóch recenzji sprzecznych Redakcja przesyła artykuł do kolejnego recenzenta. Po analizie wszystkich recenzji Redakcja podejmuje decyzję o zamieszczeniu lub niezamieszczaniu artykułu.
8. Do publikacji są kwalifikowane artykuły, które uzyskały pozytywną opinię końcową.
9. Po zakwalifikowaniu artykułu do publikacji autor lub autorzy podpisują umowę o przeniesieniu na wydawcę autorskich praw majątkowych.
10. Autorzy artykułów zakwalifikowanych do druku otrzymują honoraria.
11. W przypadku utworu stworzonego przez kilka osób każda z nich jest zobowiązana do złożenia *Oświadczenia o wkładzie poszczególnych autorów*

w powstanie publikacji (wzór oświadczenia jest dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego) i przesłania go na adres Redakcji PBW podany w pkt I ppkt 3.

12. Autorzy są zobowiązani do wypełnienia formularzy zgody na publikację materiałów przez Redakcję „Przeglądu Bezpieczeństwa Wewnętrznego" (*Formularz zgody autora na publikację artykułu w czasopiśmie „Przegląd Bezpieczeństwa Wewnętrznego* oraz *Formularz zgody autora na publikację tekstu w ramach serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego* są dostępne na stronie Agencji Bezpieczeństwa Wewnętrznego) i przesłania ich na adres Redakcji PBW podany w pkt I ppkt 3.
13. Redakcja „Przeglądu Bezpieczeństwa Wewnętrznego" wymaga podawania przez autorów numerów ORCID.

II. Zasady przesyłania tekstów.

1. Wszystkie teksty należy przesyłać w postaci zapisu elektronicznego (Word, Open Office).
2. Do artykułu należy dołączyć:
   a) bibliografię załącznikową,
   b) abstrakty w języku polskim i angielskim nieprzekraczające 15 wierszy wydruku komputerowego, zawierające cel i podsumowanie artykułu,
   c) słowa kluczowe w języku polskim i angielskim (w celu maksymalnie zwięzłego określenia tematyki artykułu – mają one ułatwić klasyfikację treści oraz wyszukiwanie artykułu w elektronicznych bazach danych; słowa kluczowe nie powinny być powtórzeniem tytułu)
   d) notkę o autorze (zawód lub tytuł naukowy, miejsce pracy).
3. Wszelkie ilustracje, zdjęcia oraz schematy, które autor chciałby umieścić w artykule, powinny być dostarczone w oddzielnych, oryginalnych plikach. Ich wymiary powinny być nie mniejsze, niż te, które mają być uzyskane po wydruku, oraz możliwie jak najlepszej jakości (min. 300 dpi w skali 1:1). W przypadku dostarczenia ilustracji złej jakości Redakcja zastrzega sobie prawo do ich niezamieszczania.

III. Normalizacja tekstu.

1. Marginesy: 2,5 cm z każdej strony.
2. Czcionka tekstu głównego: Times New Roman 12 pkt; interlinia 1,0.
3. Czcionka przypisów: Times New Roman 10 pkt; interlinia 1,0.
4. Objętość artykułu zgłaszanego do publikacji (wraz z bibliografią, abstraktami i słowami kluczowymi) nie może przekraczać 15 stron wydruku komputerowego w formacie A4, sprawozdania z konferencji – 3 stron, recenzji – 10 stron.

5. Tekst powinien być wyjustowany.
6. Tytuł, podtytuł i śródtytuły: Times New Roman, bold.
7. Rysunki i fotografie należy lokalizować w tekście głównym za pomocą podpisów.
8. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itp.).
9. Na końcu podpisu pod materiałem ilustracyjnym należy stawiać kropkę.
10. Nie należy stosować tzw. twardych spacji.
11. Ortografię i interpunkcję tekstu należy uwspółcześniać.
12. Wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być wyróżnione wytłuszczoną czcionką.
13. Nawiasy ukośne /…/ powinny być zamieniane na nawiasy półokrągłe (…).
14. Różne sposoby zapisu daty stosowane w tekście głównym powinny być ujednolicone do następującej formy: dzień zapisany cyframi arabskimi, miesiąc zapisany słownie, rok zapisany cyframi arabskimi (np. 3 lipca 1969 r.).
15. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymieniane w tekście po raz pierwszy.
16. Obce nazwy organizacji oraz skróty od nich utworzone należy zapisywać pismem prostym.

IV. Cytaty i wyróżniki.

1. Cytaty ze źródeł i literatury przedmiotu o długości do 5 wersów należy zapisywać kursywą, dłuższe należy wyróżniać przez wcięcie (1,0 cm z lewej i prawej strony, licząc od granic tekstu głównego) oraz odstęp dwóch wersów nad i pod przytoczeniem, druk prosty, czcionka o jeden stopień mniejsza niż w tekście głównym.
2. Listy przytaczane w całości należy wyróżniać przez odstęp dwóch wersów nad i pod przytoczeniem (nie należy stosować wcięcia ani kursywy).
3. Cytaty obcojęzyczne powinny być przetłumaczone w przypisie (tłumaczy autor tekstu).
4. Opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie półokrągłym.
5. Uzupełnienia i komentarze odautorskie itp. należy podawać w nawiasach okrągłych, drukiem prostym.
6. Wtrącone zwroty obcojęzyczne piszemy kursywą (np. à *rebours*, *sui generis*).
7. Tytuły dzieł sztuki (plastycznych, muzycznych, dramatycznych, filmowych), książek, artykułów, obrazów, konkursów, prac naukowych, nazw ustaw oraz innych aktów prawnych należy zapisywać kursywą, nazwy czasopism – w cudzysłowie. Zgodnie z uchwałą RJP z 2008 r. wszystkie wyrazy w tytułach czasopism, poza spójnikami i przyimkami występującymi wewnątrz tych tytułów, zapisuje się wielkimi literami.

8. W cudzysłowie należy zapisywać także: pseudonimy (np. kpr. „Smukły"), kryptonimy (np. krypt. „Jan") oraz nazwy instytucji występujące na końcu nazwy wielowyrazowej, często będącej rozwinięciem skrótowca (np. Związek Młodzieży Polskiej „Zet"); w nazwach jawnych organizacji politycznych (np. Polska Partia Socjalistyczna) oraz w nazwach operacji wojskowych (np. Pustynna Burza) nie stosuje się cudzysłowu.
9. Nazwy wystaw, konferencji i sesji naukowych należy zapisywać pismem prostym w cudzysłowie.
10. Cudzysłów należy zapisywać za pomocą znaku drukarskiego „" – a nie innych podobnych znaków ('', "").
11. Jeśli w obrębie jednego cudzysłowu występuje drugi cudzysłów, do jego wyodrębnienia należy stosować znak «».
12. Jeśli w tekście zapisanym kursywą występuje element wyróżniany kursywą (np. tytuł dzieła), należy go wyróżniać drukiem prostym (np. *Uwielbiała czytać książki, szczególnie często wracała do* Zbrodni i kary *oraz* Biesów).

V. Znaki interpunkcyjne i obce.

1. W zestawieniach (np. Austro-Węgry, Stronnictwo Demokratytczno-Narodowe, polsko-niemiecki) i w nazwiskach złożonych z dwóch członów (np. Jankowska-Cieślak) należy stosować dywiz; myślnika bez spacji należy używać w przypadku połączeń doraźnych, które odpowiadają nie jednemu obiektowi rzeczywistości pozajęzykowej, ale dwóm – najczęściej łączy się w ten sposób liczby (np. t. 1–2, w latach 2015–2020).
2. Obce nazwy miejsc i osób, podobnie jak inne słowa obce, należy zapisywać z użyciem liter i znaków obcych alfabetów (np. Národni divadlo, Tomáš Masaryk), chyba że stosuje się przyjętą w uzusie w przypadku niektórych słynnych postaci konwencję spolszczoną (np. Tomasz Masaryk, William Szekspir).

VI. Przypisy.

1. Znak przypisu należy umieszczać zawsze po słowie, nawiasie zamykającym lub po zamknięciu cudzysłowu, a przed znakiem interpunkcyjnym.
2. Przypisy należy rozpoczynać wielką literą, a kończyć kropką. Małą literą należy rozpoczynać jedynie przypisy dotyczące adresów stron internetowych (np. 1 https://www.abw.gov.pl/pl, 2 www.bip.abw.gov.pl).
3. Przypisy należy umieszczać na dole stron.
4. Przypisy we wstępie (posłowiu) oraz w tabelach mają numerację oddzielną od przypisów w tekście głównym.
5. W przypadku autorów podpisujących się dwojgiem imion należy podawać inicjały obu imion bez spacji między nimi (np. J.K. Bielecki).

6. Zawsze należy podawać podtytuł publikacji.
7. W przypisach konsekwentnie należy stosować następujące oznaczenia: tenże/taż, tamże, tłum., wstęp, posł., (red.), oprac., i in., t., cz., z., nr, [bmw] – brak miejsca wydania, [bdw] – brak daty wydania, [bmdw] – brak miejsca i daty wydania, zob., por., zob. szerzej: (z dwukropkiem), cyt. za: (z dwukropkiem), i nast.
8. Tomy, części, numery i zeszyty należy zapisywać cyframi arabskimi (np. t. 2, cz. 3, nr 4, z. 5).
9. Miesiące należy zapisywać cyframi rzymskimi bez kropek rozdzielających dzień, miesiąc i rok (w tekście głównym nazwę miesiąca należy zapisywać słownie).
10. Należy skracać opis w przypisie (oraz bibliografii) przez upraszczanie często skomplikowanych formuł dotyczących redakcji – do oznaczeń: oprac., red.
11. Gdy autorów (redaktorów, tłumaczy) jest więcej niż trzech, należy podać inicjał (inicjały) imienia i nazwisko alfabetycznie pierwszego z nich, dodając do niego skrót: i in.
12. Strony należy zapisywać następująco: s. 2; s. 3, 7; s. 3–5 (myślnik, nie dywiz).
13. Jeśli w przypisach tekst tego samego autora pojawia się więcej niż raz, to przy kolejnym przywołaniu tytuł należy skrócić do czytelnej postaci, dodając wielokropek i rezygnując z podawania ponownie miejsca i roku wydania.

    PRZYKŁAD:

    L. Wasilewski, *Ze wspomnień*…, s. 224–225.

14. Gdy podaje się przypis łączny dla kilku tomów lub części jakiejś publikacji, numery tomów należy zapisywać z myślnikiem, nie z dywizem. To samo dotyczy lat publikacji.

    PRZYKŁAD:

    K. Grodziska, *Polskie groby na cmentarzach Londynu*, t. 1–2, Kraków 1995–2001.

15. W przypadku dwóch lub trzech miejsc wydania (miejscowości), należy je zapisywać z myślnikami (np. Wrocław–Kraków), jeżeli jest ich więcej – należy podać tylko pierwsze z nich.
16. Jeśli imię zaczyna się dwuznakiem (np. Sz, Cz), należy zapisać tylko pierwszą literę; wyjątkiem jest Ch.

PRZYKŁAD:

C. Miłosz, *Druga przestrzeń*, Kraków 2002, Znak.
Ch. Dickens, *Wielkie nadzieje*, Warszawa 1999.

17. Cytaty w przypisach należy zapisywać pismem prostym w cudzysłowie.

VII. Struktura przypisów.

1. **Przypis archiwalny:**
pełna nazwa archiwum (gdy pojawia się po raz pierwszy) i w nawiasie formułka „dalej:" oraz proponowany skrót tej nazwy do stosowania za każdym kolejnym razem, po przecinku – nazwa zespołu, po przecinku – sygnatura, po przecinku – nazwa dokumentu (kursywą) lub jego opis (np. list, sprawozdanie) i data, po przecinku – numer karty (strony).

PRZYKŁADY:

Archiwum Instytutu Pamięci Narodowej, Oddziałowe Biuro Udostępniania i Archiwizacji Dokumentów w Krakowie (dalej: AIPN, OBUiAD w Krakowie), IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57.

APK, UWSl. (skrót, gdy wcześniej pojawiła się pełna nazwa miejsca przechowywania źródła), sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r., 5 I 1929 r., k. 57.

2. **Książka polska:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, inicjał imienia i nazwisko autora opracowania, miejsce i rok wydania, strony.

PRZYKŁAD:

B. Prus, *Lalka*, t. 1, oprac. J. Bachórz, Wrocław 1998, s. 100–200.

3. **Książka tłumaczona:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, inicjał imienia i nazwisko tłumacza, inicjał imienia i nazwisko autora opracowania, miejsce i rok wydania, strony.

PRZYKŁAD:

Ch. Taylor, *Źródła podmiotowości. Narodziny tożsamości nowoczesnej*, tłum. M. Gruszczyński i in., oprac. T. Gadacz, Warszawa 2001, s. 15–20.

4. **Książka zagraniczna:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, inicjał imienia i nazwisko tłumacza, miejsce i rok wydania, strony. Stosujemy zapis bibliograficzny polski, w tym obcobrzmiące nazwy miejsc wydania.

PRZYKŁAD:

P. Hadot, *The Veil of Isis. An Essay on the History of the Idea of Nature*, tłum. M. Chase, Cambridge–Massachusetts–London 2006, s. 40–50.

5. **Publikacja w pracy zbiorowej:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), w: *tytuł pracy* (kursywą), numer tomu, inicjał imienia i nazwisko redaktora, miejsce i rok wydania, strony.

PRZYKŁAD:

W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, s. 36.

6. **Dzieło wielotomowe:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), miejsce i rok wydania (np. 2007, jeśli wszystkie tomy zostały wydane w tym samym roku, lub 2000–2001, jeśli tomy zostały wydane w różnym czasie), 2 t. (dwa tomy; cyfry arabskie).

PRZYKŁAD:

B. Prus, *Lalka*, Warszawa 1985, 4 t.

7. **Praca zbiorowa** (dotyczy także antologii i opracowań):
Tytuł (kursywą). *Podtytuł* (kursywą), inicjał imienia (lub pełne imię) i nazwisko redaktora, miejsce i rok wydania.

PRZYKŁAD:

Historia Łodzi. Ze wspomnień mieszkańców, A. Kowalski (red.), Łódź 2001.

8. **Artykuł w książce:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), w: *tytuł zbioru* (kursywą), numer tomu, część, inicjał imienia i nazwisko redaktora (lub redaktorów), miejsce i rok wydania, strony.

PRZYKŁADY:

W. Szkłowski, *Sztuka jako chwyt*, w: *Teoria badań literackich za granicą*, t. 2, cz. 3, S. Skwarczyńska (red.), Kraków 1984, s. 20–22.

9. **Artykuł w zbiorze tego samego autora:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), w: tenże/taż, *tytuł zbioru* (kursywą), numer tomu, miejsce i rok wydania, strony.

PRZYKŁAD:

M. Janion, *Apokalipsa bez zbawienia. Tematy jeanpaulowskie*, w: taż, *Żyjąc, tracimy życie. Niepokojące tematy egzystencji*, Warszawa 2001, s. 15, 17.

10. **Artykuł w czasopiśmie polskim lub zagranicznym:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), „Tytuł Czasopisma", numer w danym roku, zeszyt ew. część (w opisie należy stosować cyfry arabskie), strony.

PRZYKŁAD:

W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13.

C.M. Bowra, *Orpheus and Eurydice*, „Classical Quarterly" 1952, nr 3–4, s. 12.

11. **Artykuł w dzienniku:**
inicjał imienia i nazwisko autora artykułu, *tytuł* (kursywą). *Podtytuł* (kursywą), „Tytuł Dziennika" i dalej data dzienna (nazwę miesiąca należy zapisywać słownie).

PRZYKŁAD:

Kowalski, *Energia wiatrowa. Nowe możliwości*, „Rzeczpospolita" z 2 marca 2020 r.

12. **Wydawnictwa internetowe:**
adresy internetowe należy zapisywać małymi literami (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym należy podać informację o dacie dostępu (w dacie miesiąc zapisuje się cyfrą rzymską).

PRZYKŁAD:

http://www.pbw.gov/abw/cat.html [dostęp: 1 XII 2011].

13. **Artykuły lub dokumenty zamieszczone na stronach internetowych:**
inicjał imienia i nazwisko autora, *tytuł artykułu* (*dokumentu*) – kursywą. *Podtytuł* (kursywą), data publikacji na stronie, adres internetowy, w nawiasie kwadratowym – informacja o dacie dostępu.

PRZYKŁAD:

EU NAVFOR Somalia – mission, http://www.eunavfor.eu/about-us/mission/ [dostęp: 20 VII 2014].

14. Nie należy stosować skrótów: op. cit., lok., cit.

VIII. Zapis nazwisk.

1. W tekście głównym nazwiska należy zapisywać następująco: za pierwszym razem pełne imię i nazwisko, później samo nazwisko (chyba że powtórzenie pełnego imienia jest uzasadnione względami stylistycznymi); poza opisami bibliograficznymi w przypisach i bibliografii nie należy stosować zapisu z inicjałem.

PRZYKŁAD:

Gabriel Narutowicz (lub Narutowicz; nie: G. Narutowicz) został prezydentem w 1922 r.

Jeśli dwie postaci noszą to samo nazwisko (np. Jan i Jędrzej Śniadeccy), w przypadku gdy nie jest oczywiste, o której z nich mowa, należy powtórzyć imię lub wskazać tę osobę za pomocą omówienia.

IX. Skróty.

1. W tekście głównym należy stosować ogólnie przyjęte skróty: np., itp., m.in. (bez spacji), rkps, mps, t., z. itd.), a także z reguły: r. (rok) i w. (wiek).
2. Za każdym razem należy przemyśleć zasadność wprowadzania skrótów nazw instytucji lub organizacji (zwłaszcza gdy będą stosowane rzadko), a szczególnie w przypadku przytaczania źródła; wprowadzanie skrótu jest interwencją w język zapisu.
3. Należy wprowadzać jeden skrót dla jednej nazwy.
4. Skróty należy stosować konsekwentnie – jeśli skrót został wprowadzony, odtąd zastępuje w tekście daną nazwę za każdym razem, gdy się ona pojawia.
5. W skrótach nie należy stosować dywizów.

   PRZYKŁAD:

   Polska Partia Socjalno-Demokratyczna Galicji i Śląska = PPSD (nie: PPS-D).

X. Bibliografia załącznikowa

1. Przy sporządzaniu bibliografii załącznikowej kolejne pozycje należy szeregować w porządku alfabetycznym. Opis każdej pozycji należy rozpocząć od nazwiska autora, po nim należy podać inicjał imienia, postawić kropkę, przecinek, a następnie według schematu przypisu – tytuł zapisany kursywą itd. (w przypadku artykułu w czasopiśmie lub w pracy zbiorowej należy podać zakres stron).

   PRZYKŁADY:

   Kowalski W., *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 12–20.

   Nowak W., *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, PWN, s. 32–47.

   Sekretna wojna. Z dziejów kontrwywiadu II RP, Z. Nawrocki (red.), Poznań 2014, Zysk i S-ka, 542 s.

2. Materiały archiwalne należy oddzielać od innych źródeł.
3. Akty prawne należy oddzielać od innych źródeł. Należy je szeregować według hierarchii przyjętej dla tego typu dokumentów, tj. w porządku:

– Konstytucja,
– Ratyfikowane umowy międzynarodowe.
– Rozporządzenia, dyrektywy i decyzje UE.
– Ustawy i rozporządzenia z mocą ustawy.
– Rozporządzenia.
– Akty prawa miejscowego.

4. Akty prawne zapisywane alfabetem niełacińskim wydzielamy podobnie jak literaturę w alfabecie niełacińskim:

Akty prawne

Ustawa z dnia…
Rozporządzenie z dnia…

Rosyjskie akty prawne

Указ Президента Российской Федерации…

Bułgarskie akty prawne

Конституция на Република България

5. Orzecznictwo należy oddzielać od innych źródeł.
6. Źródła internetowe należy oddzielać od innych źródeł.

Redakcja nie zwraca autorom nadesłanych prac, a także zastrzega sobie prawo do ich skracania, opracowania redakcyjnego, w tym adiustacji tekstów, oraz zmiany tytułów i śródtytułów.

Redakcja zastrzega sobie możliwość odmowy przyjęcia artykułu bez podania przyczyn.

Redakcja zwraca uwagę, że *ghostwriting** i *guest authorship*** są przejawami nierzetelności naukowej, a wszelkie wykryte przypadki praktyk niezgodnych z zasadami etyki obowiązującej w nauce będą demaskowane (ujawniane) i dokumentowane, włącznie z powiadomieniem odpowiednich podmiotów (instytucji zatrudniających autorów, towarzystw naukowych, stowarzyszeń edytorów naukowych itp.). W celu przeciwdziałania występowaniu tych zjawisk Redakcja wymaga od poszczególnych autorów ujawnienia wkładu w powstanie publikacji.

Redakcja informuje, że wszystkie artykuły zakwalifikowane do publikacji są weryfikowane z wykorzystaniem programu antyplagiatowego.

Wersją pierwotną (referencyjną) czasopisma jest wydanie papierowe.
„Przegląd Bezpieczeństwa Wewnętrznego" jest dostępny także na stronie internetowej Agencji Bezpieczeństwa Wewnętrznego w zakładce Wydawnictwo.

* Z *ghostwriting* mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, ale jego udział jako autora nie zostaje ujawniony lub choćby uwzględniony w podziękowaniach dołączonych do tekstu.

* Sytuacja określana też jako *honorary authorship* – osoba podana jako autor czy współautor tekstu miała znikomy udział lub wcale nie uczestniczyła w tworzeniu publikacji.