PROBLEMY WSPÓŁCZESNEJ KRYMINALISTYKI

UNIWERSYTET WARSZAWSKI
WYDZIAŁ PRAWA I ADMINISTRACJI
KATEDRA KRYMINALISTYKI
POLSKIE TOWARZYSTWO KRYMINALISTYCZNE

PROBLEMY WSPÓŁCZESNEJ KRYMINALISTYKI

UNIWERSYTET WARSZAWSKI
WYDZIAŁ PRAWA I ADMINISTRACJI
KATEDRA KRYMINALISTYKI

POLSKIE TOWARZYSTWO KRYMINALISTYCZNE

PROBLEMY WSPÓŁCZESNEJ KRYMINALISTYKI

TOM XIX

pod redakcją:
Ewy Gruzy
Tadeusza Tomaszewskiego
Mieczysława Goca

WARSZAWA 2015

Redakcja Naukowa
prof. dr hab. Ewa Gruza
prof. dr hab. Tadeusz Tomaszewski
dr Mieczysław Goc

Sekretarz Redakcji
dr Katarzyna Julia Furman

Rada Naukowa
prof. dr hab. Jerzy Kasprzak
prof. UWr. dr hab. Maciej Szostak
prof. dr Henryk Malewski (Litwa)

Recenzenci tomu
dr hab. Elżbieta Kozłowska-Żywucka
dr Wacław Brzęk

© Copyright by Uniwersytet Warszawski Wydział Prawa i Administracji
Katedra Kryminalistyki
© Copyright by Polskie Towarzystwo Kryminalistyczne

ISSN 1643-2207

„Problemy Współczesnej Kryminalistyki"
znajdują się na liście czasopism punktowanych

Opracowanie redakcyjne
Anna Kaniewska

Łamanie, druk i oprawa:
volumina.pl Daniel Krzanowski
ul. Ks. Witolda 7-9, 71-063 Szczecin
tel. 91 812 09 08
druk@volumina.pl, www.voluminamarket.pl

Dystrybucja i przyjmowanie zamówień:
Centrum Badawczo-Szkoleniowe PTK Sp. z o.o.
adres koresp. 00-018 Warszawa, ul. Zgoda 11/300
biuro@kryminalistyka.pl www.kryminalistyka.pl
tel. 22 692 43 85, faks 22 827 01 60

Przyjmowanie prac do druku:
Prace w formie elektronicznej, zgodne z wymogami regulaminu PWK,
należy wysłać na adres Sekretarza Redakcji:
redakcja.pwk@gmail.com

SPIS TREŚCI

Ewa Gruza
Wstęp 9

Bogusław Cichowicz
Nowelizacja Kodeksu postępowania karnego – nowy model postępowania.....11
Amendment of the Code of Criminal Procedure – new model of conduct

Antoni Feluś
Dekompozycja struktury graficzno-językowej jako środek ustalania przyczyn patologicznych pisma i miara jego zaburzenia
(Część III – Dekompozycja organizacji pisma na jego poziomie wyższym – linearności).....21
Decomposition of graphic and linguistic structure as a means of determining the causes of pathological handwritings and a measure of its disorder
(Part III – Decomposition of organization of handwriting on its higher linearity)

Michał Górski
Podstawy profilowania geograficznego 35
Basics of geographic profiling

Kacper Gradoń
Możliwości taktycznego wykorzystania otwartych źródeł informacji w Internecie przez organa ścigania oraz sprawców przestępstw i zamachów terrorystycznych.....43
Opportunities for the tactical use of the Internet-based open-source information by the law-enforcement agencies, criminal offenders and terrorists

Piotr Karasek
Manipulacja psychologiczna a swoboda wypowiedzi – rozważania na przykładzie techniki Reida.....63
Psychological manipulation v. freedom of expression – discussion on the permissibility of manipulative interrogation on the example of Reid's technique

Judyta Kasperkiewicz
Zakup kontrolowany metodą walki z anonimową siecią TOR 77
Sting operations as a method to fight anonymous net TOR

Diana Kazimierska
Metody weryfikacji spornych osiągnięć alpinistycznych 89
Methods of verification of disputed achievements in mountaineering

Maciej Kędzierski
Penalizacja finansowania terroryzmu w art. 165a kodeksu karnego 101
Criminalization of terrorist financing in Art. 165a of the Criminal Code

Krzysztof Krassowski
Wybrane elementy informatyzacji polskiej Policji 127
Selected elements of informatization of the Polish Police

Mateusz Kucharski
Modus operandi a wywiad przed włamaniem jako element taktyczny działania sprawców przestępstw przeciwko mieniu 139
Modus operandi and the interview conducted before burglary as a tactical crime method against property

Mariusz Michalski, Paweł Łabuz
Karnoprawna interpretacja „zakładania" zorganizowanej grupy przestępczej i „kierowania" nią 159
Criminal law interpretation of "establishment" and "targeting" of organized

Zbigniew Szachnitowski
Czy tęczówka oka będzie kolejną biometryką wykorzystywaną w polskiej kryminalistyce? 169
Will iris recognition be another biometric method used in Polish forensic science?

Sprawozdania

Katarzyna Julia Furman
Sprawozdanie z III Międzynarodowej Konferencji Naukowej „Miejsce Zdarzenia" 183

Mieczysław Goc, Katarzyna Julia Furman
Komunikat z obrad VI Sympozjum Kryminalistycznego Polskiego Towarzystwa Kryminalistycznego 185

Henryk Malewski
XI Międzynarodowa Konferencja Naukowo-Praktyczna „Kryminalistyka i ekspertologia sądowa: nauka, studia, praktyka", Wilno, 25–27 czerwca 2015 r. 189

Komunikaty 197

Uchwała II Kongresu Nauk Sądowych 199

Regulamin przyznawania nagród Polskiego Towarzystwa Kryminalistycznego w Konkursie im. Prof. Tadeusza Hanauska Na Pracę Roku z Dziedziny Kryminalistyki 201

Regulamin Konkursu Na Nagrodę Profesora Brunona Hołysta dla Wyróżniających się Młodych Kryminalistyków.....205

Zakres badań Polskiego Towarzystwa Kryminalistycznego.....207

Regulamin publikowania prac w „Problemach Współczesnej Kryminalistyki" ...209

Procedura recenzowania prac w „Problemach Współczesnej Kryminalistyki".....211

WSTĘP

Oddajemy w ręce Czytelników kolejny punktowany tom, jeszcze ciągle jednym punktem za publikację. Miło mi poinformować, że podjęliśmy starania o podwyższenie liczby przyznanych punktów, ale do zamknięcia niniejszego numeru nie otrzymaliśmy decyzji Ministerstwa Nauki i Szkolnictwa Wyższego, stąd też nadal czekamy na pozytywną decyzję.

W XIX tomie „Problemów Współczesnej Kryminalistyki" znajdują się opracowania znanych i uznanych autorytetów w nauce i praktyce kryminalistycznej, jak i tradycyjnie napisane przez uczestników seminarium doktorskiego prowadzonego w Katedrze Kryminalistyki Uniwersytetu Warszawskiego.

Zgodnie z przyjętą zasadą prezentujemy teksty w porządku alfabetycznym nazwisk ich Autorów.

Jest to kolejny tom „Problemów Współczesnej Kryminalistyki", w którym kwalifikujemy prace do druku, a podstawą tej kwalifikacji są pozytywne opinie dwóch recenzentów, powołanych przez redaktorów naukowych periodyku.

Życząc miłej lektury, zachęcamy wszystkich zainteresowanych do przesyłania prac do kolejnego punktowanego i jubileuszowego wydania „Problemów Współczesnej Kryminalistyki".

prof. dr hab. Ewa Gruza

Bogusław Cichowicz

NOWELIZACJA KODEKSU POSTĘPOWANIA KARNEGO – NOWY MODEL POSTĘPOWANIA

Amendment of the Code of Criminal Procedure – new model of conduct

Wstęp

Od 1 lipca 2015 r. wchodzi w życie nowelizacja Kodeksu postępowania karnego[1]. Jest ona efektem pracy Komisji Kodyfikacyjnej Prawa Karnego, powołanej w końcu 2009 r. i działającej przy Ministrze Sprawiedliwości. Wprowadza istotne zmiany w postępowaniu karnym, m.in. poprzez wzmocnienie zasady kontradyktoryjności, zmianę zakresu władzy dyskrecjonalnej sądu, ograniczenie podmiotów posiadających inicjatywę dowodową do stron procesu, a co za tym idzie, faktyczne pozbawienie sądu możliwości przeprowadzania dowodów „z urzędu". W artykule omówione zostaną najistotniejsze dla kryminalistyki zmiany przepisów kodeksu.

Ratio legis nowelizacji

Komisja Kodyfikacyjna, po przeanalizowaniu funkcjonalności i efektywności obecnego modelu postępowania karnego, przy zauważalnym wzroście przestępczości i pojawieniu się nowych *modus operandi*, uznała, iż model ten wyczerpał swoje możliwości.

Efektem tego niekorzystnego zjawiska jest nadmierna przewlekłość postępowania i długotrwałość tymczasowego aresztowania, na co zwrócił Polsce uwagę Trybunał Praw Człowieka w Strasburgu w rezolucji tymczasowej CM/ResDh (2008/75).

Komisja Kodyfikacyjna przyjęła, że najważniejszymi przyczynami tego niekorzystnego stanu są:

- odejście od kontradyktoryjności postępowania sądowego na rzecz inkwizycyjnego wyjaśniania faktów sprawy, a w konsekwencji nieprawidłowego rozłożenia ciężaru odpowiedzialności za wynik procesu,
- nadmierny formalizm wielu czynności, które nie zapewniając gwarancji procesowych uczestnikom postępowania, nadmiernie je wydłużają,
- zbędne angażowanie sądu w czynności, które mogłyby być wykonane przez czynnik pozasądowy,

[1] Ustawa z 27 września 2013 r. o zmianie ustawy Kodeks postępowania karnego oraz niektórych ustaw (DzU z 25 października 2013 r., poz. 1247).

– nieprawidłowe stosowanie standardów konstytucyjnych, które w świetle orzeczeń Trybunału Konstytucyjnego zapewniają realizację podstawowych praw jednostki[2].

Komisja wyznaczyła następujące cele, które miała osiągnąć nowelizacja:

– przemodelowanie postępowania jurysdykcyjnego w kierunku większej kontradyktoryjności, która stwarza najlepsze warunki do wyjaśnienia prawdy materialnej i najlepiej służy poszanowaniu praw uczestników postępowania,
– przemodelowanie – w zakresie niezbędnym dla zbudowania modelu kontradyktoryjnej rozprawy – postępowania przygotowawczego, zwłaszcza w zakresie celów, do których osiągnięcia postępowanie to zmierza,
– usprawnienie i przyspieszenie postępowania, dzięki stworzeniu prawnych ram szerszego wykorzystania konsensualnych sposobów zakończenia postępowania karnego i w szerszym zakresie wykorzystaniu idei sprawiedliwości naprawczej, także dzięki nowemu ujęciu instytucji mediacji,
– usunięcie „fasadowości" postępowania, dzięki nowemu określeniu sposobu procedowania, opartemu na rezygnacji z szeregu czynności niesłużących ani wyjaśnieniu prawdy w procesie, ani realizacji zasady sprawiedliwej represji,
– ukształtowanie na nowo podstaw stosowania środków zapobiegawczych, w sposób zapobiegający ich nadmiernemu wykorzystywaniu w praktyce procesowej, a zarazem lepiej gwarantujący osiągnięcie podstawowego ich celu, jakim jest zapewnienie prawidłowego przebiegu postępowania, a także lepiej chroniący gwarancje procesowe oskarżonego oraz w szerszym niż dotychczas zakresie umożliwiający dochodzenie odszkodowania i zadośćuczynienia za szkody i krzywdy, wyrządzone wykonywaniem tych środków w toku postępowania,
– ograniczenie przewlekłości postępowania, dzięki ukształtowaniu modelu postępowania odwoławczego w sposób umożliwiający szersze orzekanie reformatoryjne, a tym samym ograniczający kasacyjność tego postępowania, przyczyniającą się do przedłużenia postępowania karnego,
– odciążenie sędziów, prezesów sądów i przewodniczących wydziałów przez ukonstytuowanie możliwości podejmowania decyzji o charakterze porządkowym i technicznym (a także mniej ważkich decyzji merytorycznych) przez referendarzy sądowych, a dzięki temu umożliwienie wykorzystania czasu sędziów w bardziej efektywny sposób,
– uzyskanie pełnej zgodności rozwiązań kodeksowych ze standardami ujawniającymi się na tle orzecznictwa Trybunału Konstytucyjnego oraz Europejskiego Trybunału Praw Człowieka,
– usunięcie oczywistych i ujawnionych w orzecznictwie sądowym usterek obecnej regulacji[3].

[2] *Uzasadnienie rządowego projektu ustawy o zmianie ustawy Kodeks postępowania karnego oraz niektórych ustaw* (Druk Sejmowy nr 870), s. 1.

[3] Tamże, s. 2–3.

Przedstawione wyżej cele regulacji ustawodawca osiągnął dzięki zmianie brzmienia odnośnych przepisów kodeksu. Jest to przeważająca metoda techniki legislacyjnej, zastosowana w trakcie procesu legislacyjnego.

W dalszej części zostaną omówione zmiany istotne dla istoty modelu postępowania karnego i jego funkcjonowania na przykładzie wybranych przepisów kodeksu. Są one ważne również z punktu widzenia kryminalistyki jako nauki zapewniającej w ramach przepisów proceduralnych środki do osiągnięcia celów postępowania karnego.

Nowe brzmienie wybranych przepisów Kodeksu postępowania karnego

Pierwszą chronologicznie w ujęciu kodeksowym zmianą dokonaną przez ustawę nowelizującą jest nowe brzmienie art. **2 § 1 pkt 2**, w którym określone są cele postępowania karnego. W nowelizacji tego przepisu ustawodawca przyjął, że celem postępowania karnego jest takie ukształtowanie postępowania, aby sprawca przestępstwa został wykryty i pociągnięty do odpowiedzialności karnej, a osoba, której nie udowodniono winy, nie poniosła tej odpowiedzialności[4].

Na pozór jest to niewielka zmiana. Tymczasem ustawodawca przyjął definicję osoby niewinnej, czyli osoby, której nie udowodniono winy. Definicja ta będzie funkcjonowała w zakresie całego kodeksu. Z powyższą zmianą wiąże się zmiana treści art. **5 § 2** kodeksu, statuującego zasadę domniemania niewinności. Ustawodawca nadał temu przepisowi całkowicie nowe brzmienie. Dotychczas niedających się usunąć wątpliwości nie można było rozstrzygać na niekorzyść oskarżonego. Po nowelizacji, aby zrealizować zasadę *in dubio pro reo*, na korzyść oskarżonego należy rozstrzygać wątpliwości, których nie usunięto w toku postępowania[5]. W przepisie tym ustawodawca nie wskazał, na kim ciąży obowiązek usunięcia ewentualnych wątpliwości. Odpowiedź znajduje się w treści znowelizowanego art. 167 kodeksu, który zostanie szerzej omówiony poniżej.

Z analizy treści znowelizowanego brzmienia art. 5 § 2 wynika, że obowiązek ten nie będzie ciążył na sądzie, który nie jest – co do zasady – obowiązany do przeprowadzania dowodów „z urzędu". Dzięki temu to oskarżyciela będzie obciążać ta powinność (w sensie materialnym także obrońcę).

Nowym brzmieniem art. 5 § 2 ustawodawca przesądził także, iż wątpliwości podlegające rozstrzygnięciu na korzyść oskarżonego mogą dotyczyć jedynie kwestii dowodowych, a nie prawnych. Sprawa ta była dotąd różnie unormowana, zarówno w doktrynie, jak i orzecznictwie. Zakłada się bowiem, że wątpliwości co do interpretacji prawa muszą być usunięte w każdym przypadku w drodze wykładni, a powinność ta spoczywa właśnie na sądzie. Niemniej jednak do czasu ukształtowania się praktyki sądowej i linii orzecznictwa, powstałych pod rządami tego znowelizowanego przepisu, aktualne pozostają nadal dotychczasowe poglądy teorii i praktyki.

Rzeczą istotną jest także, że ustawodawca, nowelizując ten przepis i przesuwając na strony ciężar usunięcia wątpliwości, użył określenia „wątpliwości, których

[4] Art. 2 § 1 pkt 2 w brzmieniu nadanym przez art. 1 pkt 1 ustawy powołanej w przypisie 1.

[5] Art. 5 § 2 w brzmieniu nadanym przez art. 1 pkt 2 ustawy powołanej w przypisie 1.

nie usunięto". Zastąpił tym samym dotychczasowe określenie „niedających się usunąć wątpliwości". Jest to istotna zmiana, albowiem implikuje ona podejście sądu do tych wątpliwości. Sąd, zamiast przyjąć *a priori*, że istnieją wątpliwości, których nie usunięto przy wykorzystaniu dostępnych środków dowodowych, będących w jego dyspozycji, będzie tylko „biernym" obserwatorem działań stron, zmierzających do usunięcia tych wątpliwości, wykazanych przez drugą stronę.

Takie zadanie stawia przed sądem znowelizowany art. **167** kodeksu. Uzasadnienie nowelizacji tego przepisu zawiera się w stwierdzeniu, że „sąd będzie pełnił rolę »biernego« arbitra, który po przeprowadzeniu przez strony dowodów, uprzednio przez nich wnioskowanych i dopuszczonych przez sąd, wyda sprawiedliwe rozstrzygnięcie"[6].

W dotychczasowym brzmieniu art. 167, określającym podmioty, którym przysługuje inicjatywa dowodowa, poprzez stwierdzenie, iż „dowody przeprowadza się na wniosek stron, podmiotu określonego w art. 416 albo z urzędu"[7], została wprowadzona bardzo istotna zmiana, zarówno w konstrukcji tego przepisu, jak i w warstwie merytorycznej.

Od 1 lipca 2015 r. strony będą mogły przeprowadzać przed sądem tylko te dowody, które uprzednio zostały dopuszczone przez prezesa sądu, przewodniczącego lub sąd. Obligatoryjnie sąd będzie przeprowadzał dowód w granicach tezy dowodowej tylko w przypadku niestawiennictwa się strony, na której wniosek został dopuszczony, a także w wyjątkowych wypadkach, uzasadnionych szczególnymi okolicznościami. Fakultatywnie sąd może dopuścić dowód „z urzędu", jeżeli uzna, że zachodzą wyjątkowe wypadki, uzasadnione szczególnymi okolicznościami[8].

Rozwiązanie przyjęte w tym przepisie, mające bardzo istotne znaczenie dla zasad prowadzenia postępowania dowodowego, uznać należy, oględnie rzecz ujmując, za nietrafne. Z praktycznego punktu widzenia ustawodawca pozostawił decyzję co do zasadności dopuszczenia dowodu, wnioskowanego przez stronę, prezesowi sądu, przewodniczącemu, czyli organom administracyjnym sądu, i sądowi orzekającemu. Tym samym nie został spełniony jeden z celów nowelizacji, czyli odciążenia w pracy prezesów sądów i przewodniczących wydziałów.

Ustawodawca ograniczył inicjatywę dowodową sądu tylko do wyjątkowych przypadków, nałożył natomiast obowiązek przeprowadzenia dowodu w granicach tezy dowodowej w razie niestawiennictwa się strony wykazującej inicjatywę dowodową oraz w wyjątkowych wypadkach. W tym przepisie ustawodawca dwukrotnie używa określenia „wyjątkowe wypadki, uzasadnione szczególnymi okolicznościami", pozostawiając je do uznania sądu, słusznie przy tym opierając się na roztropności i doświadczeniu sądu.

Nie oznacza to jednak, że w praktycznym stosowaniu znowelizowany przepis art. 167 nie będzie budził wątpliwości interpretacyjnych. Uzasadnienie nowelizacji tego

[6] *Uzasadnienie rządowego projektu*…, op. cit., s. 5.

[7] Art. 167 Kodeksu postępowania karnego w brzmieniu obowiązującym do dnia 30 czerwca 2015 r.

[8] Art. 167 w brzmieniu nadanym przez art. 1 pkt 51 ustawy powołanej w przypisie 1.

przepisu nie zawiera merytorycznej *ratio legis* zmiany dotychczasowego brzmienia artykułu.

Konsekwencją wprowadzenia wzmocnionej zasady kontradyktoryjności procesu jest także nowelizacja art. **366 § 1** kodeksu. W myśl tego artykułu przewodniczący kieruje rozprawą i czuwa nad jej prawidłowym przebiegiem[9]. Tym samym przewodniczący został zwolniony z obowiązku baczenia, „aby zostały wyjaśnione wszystkie okoliczności sprawy, a w miarę możliwości także okoliczności sprzyjające popełnieniu przestępstwa", tak jak regulował to art. 167 przed jego nowelizacją. W ten sposób poza sferą procesu pozostaje jego rola prewencyjna.

Nowelizując ten przepis, ustawodawca wyznaczył sędziemu rolę „administratora" procesu, co w powiązaniu z funkcją wyznaczoną przez znowelizowany art. 167 w bardzo znacznym stopniu zmieniło, a nawet ograniczyło rolę sędziego w procesie.

Powstaje w tym miejscu pytanie, w jaki sposób zostaną spełnione cele procesu, wyznaczone w art. 2 kodeksu. Obawiam się, że przez długi czas zarówno judykatura jak i orzecznictwo nie udzielą odpowiedzi na to pytanie.

Ustawodawca, nowelizując przepisy działu V kodeksu, oprócz omówionego art. 167 dokonał innych, istotnych zmian w tym dziale. Został bowiem rozszerzony katalog zakazów dowodowych. Katalog ten objął dowody pochodzące z tzw. zatrutego drzewa. Zakaz ten dotyczy przeprowadzania i wykorzystywania dowodu uzyskanego do celów postępowania za pomocą czynu zabronionego, określonego w art. 1 § 1 Kodeksu karnego[10]. Nowelizacja wprowadziła także zakaz uzyskiwania dowodu z zeznań mediatora co do faktów, o których dowiedział się podczas prowadzenia mediacji, z wyjątkiem informacji o przestępstwach określonych w art. 240 § 1 Kodeksu karnego[11]. Tym samym mediator został wyłączony z mocy prawa jako źródło dowodowe, analogicznie jak obrońca (adwokat i radca prawny) i duchowny. *Ratio legis* tego rozwiązania wiąże się z podkreśleniem znaczenia mediacji w procesie karnym.

Zmiana przepisów postępowania dopuszcza możliwość wykorzystania w procesie karnym prywatnych opinii biegłych, uzyskanych poza tym procesem. Możliwość taką ustawodawca zawarł w znowelizowanym przepisie art. **393 § 3** Kodeksu postępowania karnego[12].

Takie opinie, jak również oświadczenia, publikacje, listy i notatki, na wniosek stron, mogą być odczytywane w trakcie procesu. Co prawda w tym przepisie nie ma określenia „opinia prywatna", ale konstrukcja art. 393 pozwala przyjąć, że określenie to zawiera się zarówno w pojęciu „opinia biegłych" (art. 393 § 1), jak i „dokumenty prywatne" (art. 393 § 3).

Zastosowanie w praktyce tego przepisu będzie powodowało poważne trudności merytoryczne i interpretacyjne. Chodzi o tzw. moc dowodową prywatnej opinii biegłego, czyli wiarygodność tej opinii, którą oceniał będzie sąd. Ponieważ od

[9] Art. 366 § 1 w brzmieniu nadanym przez art. 1 pkt 118 ustawy powołanej w przypisie 1.
[10] Art. 168a dodany przez art. 1 ust. 52 ustawy powołanej w przypisie 1.
[11] Art. 178a dodany przez art. 1 ust.55 ustawy powołanej w przypisie 1.
[12] Art. 393 § 3 w brzmieniu nadanym przez art. 1 pkt 130 ustawy powołanej w przypisie 1.

1 lipca br., w założeniu ustawodawcy, w procesie karnym będzie obowiązywała zasada kontradyktoryjności w najszerszym jej znaczeniu, na sali sądowej dojdzie do sytuacji „zderzenia się" dwóch, a może nawet więcej opinii biegłych.

Można wyobrazić sobie następującą sytuację. Z jednej strony sąd będzie miał do dyspozycji opinię biegłego sądowego, z drugiej zaś stronę opinię „prywatnego" biegłego. Nie neguję wiedzy i doświadczenia tych biegłych, ale nie wyobrażam sobie, aby opinii biegłego, np. z zakresu badania pisma ręcznego, który badania te prowadzi od lat w certyfikowanej pracowni kryminalistycznej, została przeciwstawiona opinia osoby, która takimi badaniami zajmuje się sporadycznie. Oczywiście, wybór biegłego należeć będzie do strony, wnioskującej dopuszczenie przez sąd dowodu z opinii, sporządzonej przez wybraną przez siebie osobę (biegłego).

Mam nadzieję, że ustawodawca, nowelizując art. 393, przyjął założenie, iż określenie „opinia prywatna" dotyczy zasięgnięcia opinii wyspecjalizowanego biegłego na własny koszt i na własne ryzyko.

W innym rozumieniu pojęcia „opinia prywatna" w aspekcie zasadności nowelizacji tego przepisu może dojść do sytuacji opisanej przez naszego narodowego wieszcza w IV księdze *Pana Tadeusza*.

Otóż po zakończeniu polowania Gerwazy, mając rozstrzygnąć spór pomiędzy Sędzią a Asesorem, który z nich zabił atakującego niedźwiedzia,

„dobył tasak, rozciął pysk na dwoje,
I w tylcu głowy, mózgu rozkroiwszy słoje,
Znalazł kulę, wydobył, suknią ochędożył,
Przymierzył do ładunku, do flinty przyłożył,
A potem, dłoń podnosząc i kulę na dłoni;
Panowie – rzekł – ta kula nie jest z waszej broni
Ona z tej Horeszkowskiej wyszła jednorurki"[13].

Dzięki tej opinii z zakresu badań porównawczych broni palnej, wydanej *ad hoc*, okazało się, że wyborowym strzelcem, który jednym strzałem „położył" niedźwiedzia", był ksiądz Robak.

Niewątpliwym błędem ustawodawcy jest to, że wejście w życie ustawy nowelizującej Kodeks postępowania karnego nie zostało skorelowane z zakończeniem prac legislacyjnych nad rządowym projektem ustawy o biegłych sądowych z dnia 29 października 2014 r. Projekt ten, mimo swoich niedoskonałości merytorycznych, jest próbą unormowania wymagań stawianych biegłym sądowym[14].

Omawiając zmianę przepisów Kodeksu postępowania karnego dotyczących kwestii dowodu z opinii biegłych, nie mogę pominąć problematyki ściśle związanej z czynnościami dokonywanymi na miejscu zdarzenia i wchodzącymi w skład techniki kryminalistycznej. Ustawodawca dokonał nowelizacji art. **209**, zawartego w dziale V kodeksu. Przepis ten przewiduje w przypadku podejrzenia przestępnego

[13] A. Mickiewicz, *Pan Tadeusz czyli Ostatni zajazd na Litwie. Historia szlachecka z 1811 i 1812 roku we dwunastu księgach wierszem*, Czytelnik Warszawa 1974, s. 123–124.

[14] Zob uwagi Polskiego Towarzystwa Kryminalistycznego do rządowego projektu ustawy o biegłych sądowych na stronie internetowej Towarzystwa – zakładka „Aktualności".

spowodowania śmierci dokonanie zewnętrznych oględzin zwłok i ich otwarcia (oględziny wewnętrzne). W myśl niezmienionej treści art. 209 § 2 kodeksu zewnętrznych oględzin zwłok dokonuje prokurator lub sąd, z udziałem biegłego lekarza, w miarę możności z zakresu medycyny sądowej.

Celem zewnętrznych oględzin zwłok jest ustalenie faktu i czasu śmierci, ujawnienie obrażeń, zabezpieczenie miejsca zdarzenia i śladów kryminalistycznych. W praktyce śledczej normą jest kierowanie zwłok na sądowo-lekarską sekcję zwłok, która składa się z dwóch etapów: oględzin zewnętrznych i wewnętrznych (otwarcie) zwłok i przeprowadzaną w zakładzie medycyny sądowej. Jeżeli oględziny zwłok na miejscu zdarzenia zostały przeprowadzone zgodnie z wymogami wiedzy i zasadami kryminalistyki, to sekcja zwłok w części oględzin zewnętrznych, dokonana przez biegłego z zakresu medycyny sądowej, potwierdzała wyniki oględzin zewnętrznych, dokonanych na miejscu zdarzenia. Wewnętrzne oględziny zwłok, dokonywane przez biegłego prowadziły do szczegółowego ustalenia czasu, miejsca i przyczyny zgonu.

Przed nowelizacją art. 209 w przepisie tym istniała rozbieżność między wymogami stawianymi biegłemu, dokonującemu zewnętrznych oględzin zwłok, a wymogami stawianymi osobie, która dokonywała otwarcia zwłok. W myśl art. 209 § 4 (w brzmieniu przed nowelizacją) oględzin wewnętrznych mógł dokonać biegły (w domyśle lekarz). Dlatego też dokonano nowelizacji tego przepisu, usuwając rozbieżność z treścią art. 209 § 2 kodeksu. Według znowelizowanego art. 209 § 4 otwarcia zwłok może dokonać biegły lekarz, w miarę możności z zakresu medycyny sądowej[15].

Ratio legis tej słusznej zmiany, która doprecyzowała wymogi stawiane biegłemu, dokonującemu bardzo istotnych dowodowo czynności zewnętrznych i wewnętrznych oględzin zwłok, jest wynikiem przyjęcia następującego poglądu. Projektodawca zmiany tego przepisu stwierdził, iż „zmiana przepisu ma na celu podkreślenie, że otwarcia zwłok winien dokonywać w miarę możności, a więc przede wszystkim, biegły będący lekarzem z zakresu medycyny sądowej. W dotychczasowym stanie prawnym przyjmuje się ogólnie, że otwarcia zwłok dokonuje biegły lekarz bez żadnego dookreślenia specjalności tego lekarza, co nie zmusza organów ścigania do poszukiwania w miarę szybko biegłego z zakresu medycyny sądowej, a w konsekwencji nierzadko tej czynności dokonuje inny lekarz, co może i prowadzi niekiedy do błędnych ustaleń faktycznych. Rozwiązanie obecne jest tym bardziej nieprawidłowe, że w przypadku zwykłych oględzin zwłok przyjmuje się, iż dokonuje się ich z udziałem w miarę możności lekarza z zakresu medycyny sądowej. Tym bardziej zatem wymóg taki powinien być wyraźnie zapisany przy otwarciu zwłok, czyli sekcji”[16].

W tym miejscu uczynię następującą uwagę. Projektodawcy nowelizacji tego przepisu, jak wynika z zacytowanego wyżej fragmentu uzasadnienia projektu, pominęli dotychczasową praktykę organów ścigania, które w każdym przypadku śmierci budzącym wątpliwości zarządzały sądowo-lekarskie oględziny zwłok, dokonywane w zakładzie medycyny sądowej przez biegłego z zakresu medycyny sądowej. W razie

[15] Art. 209 § 4 w brzmieniu nadanym przez art. 1 pkt 60 ustawy powołanej w przypisie 1.
[16] *Uzasadnienie rządowego projektu*…, op. cit., s. 46.

konieczności zasięgano opinii biegłego np. z zakresu toksykologii jako specjalizacji w ramach medycyny sądowej.

Z punktu widzenia kryminalistyki, a także praktyki śledczej, wyniki sądowo-lekarskich oględzin zwłok mają olbrzymie znaczenie w dalszym toku postępowania. Ugruntowaną praktyką śledczą jest udział lekarza biegłego z zakresu medycyny sądowej w zewnętrznych oględzinach zwłok, dokonywanych na miejscu zdarzenia. Po wejściu w życie nowelizacji art. 209 kodeksu praktyka ta stanie się nakazem ustawowym.

Pozostając przy problematyce związanej z udziałem biegłego w procesie karnym, warto omówić budzącą wątpliwości nowelizację art. **202 § 5** kodeksu. W tym przepisie ustawodawca nałożył na biegłych lekarzy psychiatrów oraz biegłych psychologów dodatkowy obowiązek. Od 1 lipca 2015 r. biegli ci, wydając opinię co do stanu zdrowia podejrzanego (oskarżonego), będą musieli stwierdzić w opinii, czy jego stan zdrowia psychicznego pozwala mu na „prowadzenie obrony w sposób samodzielny i rozsądny”[17]. Zmiana tego artykułu jest konsekwencją nowelizacji art. **79 § 1 pkt 4** kodeksu. W przepisie tym ustawodawca wprowadził obowiązek ustanowienia dla oskarżonego (podejrzanego) obrońcy w przypadku uzasadnionych wątpliwości, czy stan jego zdrowia psychicznego pozwala mu na udział w postępowaniu lub prowadzenie obrony „w sposób samodzielny oraz rozsądny”[18].

Moje wątpliwości budzą określenia użyte w obydwu tych przepisach. Jest rzeczą oczywistą, że język prawny powinien charakteryzować się precyzją w konstruowaniu normy prawnej. Oznacza to, że ustawodawca ma unikać określeń nieostrych, wieloznacznych, budzących wątpliwości interpretacyjne. Negatywnym przykładem nieprawidłowego zastosowania języka prawnego jest użycie przez ustawodawcę w tych znowelizowanych przepisach określenia możliwości prowadzenia przez oskarżonego obrony „w sposób samodzielny i rozsądny”. Nie wiem, jakie kryteria przyjmą biegli, aby stwierdzić, czy obrona prowadzona przez oskarżonego jest samodzielna i rozsądna.

Przypuszczam, że decydując się na nowelizację tych przepisów, ustawodawca przyjął, iż wiedza biegłych lekarzy psychiatrów i psychologów w zakresie meandrów prowadzenia obrony jest wystarczająca do wydania opinii w tym zakresie.

W przeciwnym wypadku dojdzie do paradoksalnej sytuacji, w której uwaga biegłych będzie skupiona na aspektach obrony, a nie stanie zdrowia psychicznego oskarżonego, co jest warunkiem odpowiedzialności karnej.

Utinam falsus vates sim!

Na zakończenie omawiania nowelizacji wybranych przepisów Kodeksu postępowania karnego wskażmy jeszcze jeden przykład nowelizacji, która może mieć znaczenie dla możliwości prowadzenia efektywnej obrony, jak również z punktu widzenia kryminalistyki.

Obecnie niezbędnym elementem aktu oskarżenia jest jego uzasadnienie; w nim prokurator obowiązany jest przedstawić fakty i dowody, na których opiera oskarżenie,

[17] Art. 202 § 5 w brzmieniu nadanym przez art. 1 pkt 57 ustawy powołanej w przypisie 1.
[18] Art. 79 w brzmieniu nadanym przez art. 1 pkt 22 ustawy powołanej w przypisie 1.

jak również uzasadnienie kwalifikacji prawnej czynu, zarzucanego oskarżonemu. Analiza uzasadnienia aktu oskarżenia pozwala na ujawnienie, jeszcze przed rozprawą, taktyki oskarżenia i przyjęcie linii obrony. Natomiast nowelizacja wprowadza istotne *novum* w odniesieniu do wymogów stawianych aktowi oskarżenia.

Skutkiem zmiany przepisów w odniesieniu do art. **332** kodeksu jest rezygnacja z obligatoryjnego sporządzania uzasadnienia aktu oskarżenia. W myśl tego znowelizowanego artykułu, uzasadnienie może stanowić załącznik do aktu oskarżenia[19]. Inicjatywę w tym zakresie ustawodawca pozostawił prokuratorowi.

Mam nadzieję, że odstąpienie od sporządzenia uzasadnienia aktu oskarżenia nie będzie dotyczyło spraw skomplikowanych, wielowątkowych lub tych, w których podejrzanemu zarzucono popełnienie zbrodni. Praktyka będzie zmuszona odpowiedzieć na pytanie: w jaki sposób oskarżony może udzielić odpowiedzi na akt oskarżenia, jeżeli nie zna jego uzasadnienia?

Wnioski

Reasumując powyższe rozważania dotyczące nowelizacji Kodeksu postępowania karnego, należy podkreślić, iż generalnie spełniła ona przyjęte założenia. Praktyka, w tym i orzecznictwo, pokaże czy osiągnęła swoje cele. Nie oznacza to jednak, że nie jest ona wolna od wad w odniesieniu do poszczególnych przepisów. Niektóre z nich wskazano powyżej. Dokonując nowelizacji ustawodawca powinien niejako „przy okazji" usunąć lub zmienić te przepisy, które zawierają w sobie normy nieprecyzyjne lub dające możliwość szerokiej interpretacji.

Takim przykładem jest art. 7 kodeksu, statuujący zasadę swobodnej oceny dowodów, w myśl której organy postępowania karnego kierują się zasadami prawidłowego rozumowania, czyli logiką, w powiązaniu ze wskazaniami wiedzy i doświadczenia życiowego. O ile kryterium prawidłowego rozumowania i wiedzy jest możliwe do realizacji, o tyle doświadczenie życiowe, z uwagi na nieprecyzyjność, a co za tym idzie pojemność znaczeniową, nie powinno być elementem zasady swobodnej oceny dowodów. Kryterium to jest zbyt indywidualne i związane z podmiotem badającym. W praktyce jest ono nie do zrealizowania.

Należy przy tym pamiętać, że naruszenie zasady swobodnej oceny dowodów, jako jednej z zasad procesu karnego, może stanowić podstawę zaskarżenia wyroku (art. 438 k.p.k.). Stwierdzenie w apelacji, iż sąd I instancji naruszył tę zasadę na skutek braku swojego doświadczenia życiowego, jest argumentem łatwym do wykazania, ale trudnym do odparcia.

Tylko na marginesie zaznaczę, że ten element składowy zasady swobodnej oceny dowodów został przeniesiony do art. 7 Kodeksu postępowania karnego z 1991 r. z odpowiadającego mu art. 4 kodeksu z 1969 r. Nie zawierał go natomiast Kodeks postępowania karnego z 1928 r.

[19] Art. 332 w brzmieniu nadanym przez art. 1 pkt 102 ustawy powołanej w przypisie 1.

Przy kolejnej nowelizacji kodeksu ustawodawca powinien rozważyć zmianę art. 7 i zrezygnować z doświadczenia życiowego jako elementu zasady swobodnej oceny dowodów.

Po wejściu w życie znowelizowanych przepisów przy ocenie ich skutków i sposobu realizacji konieczne będzie uwzględnienie czynnika ludzkiego. Nie można zapominać, że przez długi czas procesy będą toczyć się częściowo według „starych" przepisów, a częściowo według znowelizowanych. Tak więc nowelizacja stawia wysokie wymagania sędziom, prokuratorom, adwokatom (od 1 lipca br. także radcom prawnym) przy stosowaniu zmienionych przepisów. Dotyczy to zwłaszcza tych przepisów, które wprowadzają radykalne zmiany w procesie. Wymagać to będzie nie tylko pogłębionej wiedzy prawniczej, ale także szerszej niż dotychczas znajomości kryminalistyki, medycyny sądowej, psychiatrii, psychologii i umiejętności odpowiedniego wykorzystania posiadanej wiedzy.

De lege ferenda ustawodawca powinien jednak rozważyć, w interesie wymiaru sprawiedliwości, kierując się nakazem stanowienia dobrego prawa, zasadami legislacji, konieczność uchwalenia nowego kodeksu jako całości. Od dnia wejścia w życie Kodeks postępowania karnego z 1997 r. był bowiem nowelizowany siedemdziesiąt sześć (sic!) razy.

Streszczenie

Od 1 lipca 2015 r. wejdzie w życie nowelizacja Kodeksu postępowania karnego z 1997 r. Wprowadza ona istotne zmiany w obecnym modelu postępowania karnego. Inicjatywa i ciężar dowodzenia zostały przerzucone na strony postępowania. W bardzo istotny sposób ograniczono prawo sądu do przeprowadzania dowodów „z urzędu". Rolą sądu będzie czuwanie nad szybkim i sprawnym przebiegiem rozprawy. Autor, dokonując analizy modelu procesu, który będzie obowiązywał od 1 lipca br., wskazuje zarówno wady, jak i zalety nowelizacji i skutki jej wprowadzenia.

Słowa kluczowe: Kodeks postępowania karnego, nowelizacja, prokurator, oskarżony, inicjatywa dowodowa, sąd, biegli

Summary

From July 2015 enters into force the amendment of the Code of Criminal Procedure from 1997. It introduces significant changes to the current model of the criminal proceedings. Initiative and the burden of command has been passed on to the parties. Was limited in a very significant way the right of the court to take evidence, 'the office'. The role of the court will be monitoring the fast and efficient conduct of the hearing. The author, analyzing the process model, which will be valid from July, indicates both the advantages and disadvantages of the amendment and the effects of its introduction.

Keywords: Code of Criminal Procedure, amendment, public prosecutor, accused initiative evidence, court, experts

Antoni Feluś

DEKOMPOZYCJA STRUKTURY GRAFICZNO-JĘZYKOWEJ JAKO ŚRODEK USTALANIA PRZYCZYN PATOLOGICZNYCH PISMA I MIARA JEGO ZABURZENIA (CZĘŚĆ III – DEKOMPOZYCJA ORGANIZACJI PISMA NA JEGO POZIOMIE WYŻSZYM – LINEARNOŚCI)

Decomposition of graphic and linguistic structure as a means of determining the causes of pathological handwritings and a measure of its disorder (Part III - Decomposition of organization of handwriting on its higher linearity)

Wydawałoby się, że linearność pisma jest – z punktu widzenia informacji odnoszącej się do takich właściwości grafologicznych, jakimi są identyfikacja kryminalistyczna oraz psychofizjologia pisma – mniej wartościowa poznawczo. Że jest mniej wartościowa w stosunku np. do organizacji pisma na jego poziomie niższym, na który składa się ciąg liter jako jednostek graficznych, od siebie niezależnych, wyizolowanych, charakteryzujących się właściwościami grafometrycznymi wraz z całą informacją odnoszącą się do jakości linii dotkniętej przyczynami patologicznymi o charakterze neurologiczno-psychiatrycznym. Nie ma nic bardziej błędnego. Wskazuje na to wzgląd językowy o budowie systemowej, przybierającej postać rozciągniętą w czasie, gdy chodzi o język mówiony, natomiast w przypadku języka pisanego – przybierającej postać rozkładu przestrzennego – postać linearności; wskazuje na to także wzgląd fizjologiczny wymagający odruchu warunkowego bardziej złożonego[1] dla realizacji linearności pisma oraz wzajemnej ciągłości charakteryzującej się wzajemnym wiązaniem elementów literowych w pojedynczy wyraz czy nawet w całe zespoły wyrazowe, przybierające postać wyrażenia, a nawet całego zdania.

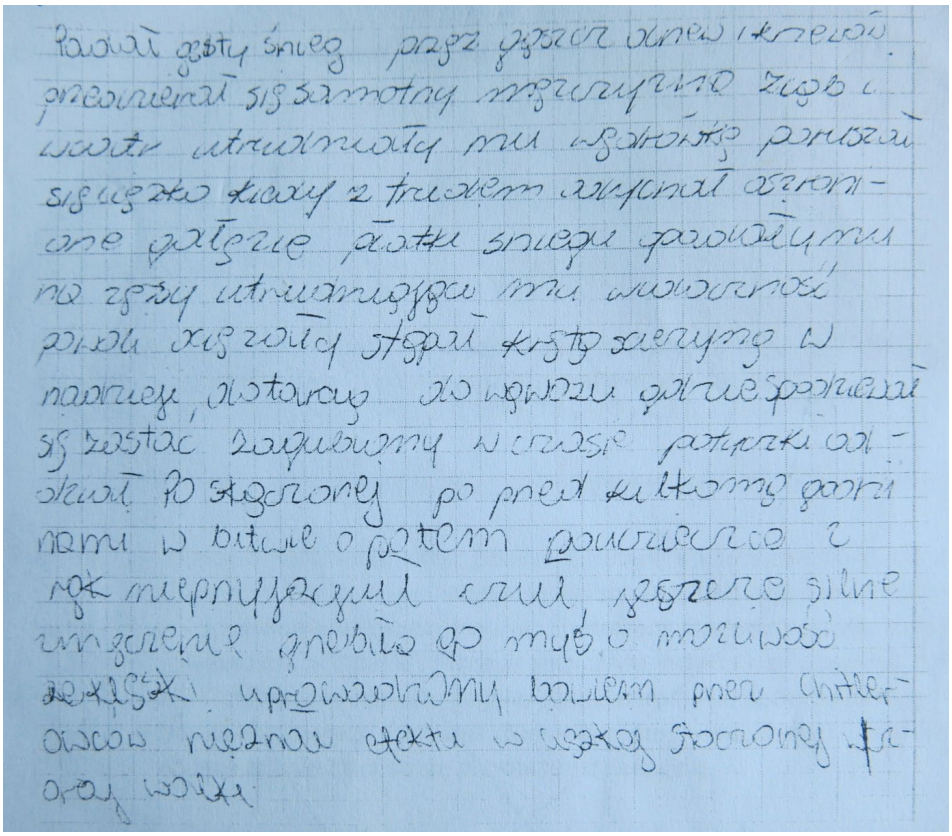
Gdy wnika się głębiej w istotę grafologiczną linearności, w jej zakres fizjologiczno-psychologiczny, wartość poznawcza w zakresie rozkładu przestrzennego, w którym mieści się także linearność, wynika z tego, że staje się ona jednoznaczną linią demarkacyjną pomiędzy strukturą graficzną zaburzoną z przyczyn neurologicznych a pismem zaburzonym wyłącznie z przyczyn psychiatrycznych, jak to się zdarza

[1] W. Chłopicki, J.S. Olbrycht, *Wypowiedzi na piśmie jako objawy zaburzeń psychicznych*, PZWL, Warszawa 1959, s. 51, 44, 37, 35, 14, 13.

np. w schizofrenii „czystej", tzn. bez „nałożenia się" na nią chorób o podłożu neurologicznym, co może mieć miejsce m.in. w wieku starczym[2]. Tego rodzaju stwierdzenie – z kryminalistycznego punktu widzenia – ma znaczenie przede wszystkim o walorach identyfikacyjnych, rozciągniętych na cały zespół chorób o podłożu neurologicznym oraz o podłożu psychicznym w zakresie chorób niepostępujących (np. psychopatie) i chorób postępujących (np. psychozy schizofreniczne). Z powyższego można wnosić, że rozkład przestrzenny pisma, w tym przede wszystkim linearność, może się przyczynić w znacznym stopniu do głębszego zrozumienia i zarazem rozeznania w strukturze graficznej pisma patologicznego z zaburzeniami o podłożu neurologicznym oraz psychiatrycznym – w charakterystyce tzw. cech swoistych, w poszukiwaniu ich właściwości jakościowo-ilościowych, uzależnionych od takiej czy innej jednostki chorobowej. Już na tym etapie postępowania badawczego można wnosić, że „cechy swoiste" o charakterze patologicznym co do ich swoistości są uzależnione nie tylko od takiej czy innej jednostki chorobowej (zespół chorób neurologicznych oraz psychicznych), ale także od ich stopnia zaburzenia[3].

[2] Tamże, s. 14, 75, 85.

[3] Zob. np. A. Feluś, *Dekompozycja struktury graficzno-językowej jako środek ustalania przyczyn patologicznych pisma i miara jego zaburzenia (część I)*, „Problemy Współczesnej Kryminalistyki" 2011, t. XV, s. 57–84; także: W. Chłopicki, J.S. Olbrycht, op. cit., s. 80–83.



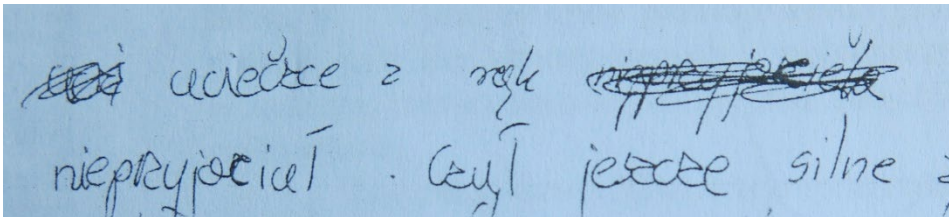
Fot. 1. Rękopis został sporządzony przez licealistę dotkniętego wszystkimi trzema dysfunkcjami – dysgrafią, dysortografią oraz dysleksją. Rozkład przestrzenny pisma w szerokim tego słowa znaczeniu nie zawiera zjawisk patologicznych. Brak widocznych zaburzeń.

Źródło: M. Całkiewicz, *Kryminalistyczne badania patologicznego pisma ręcznego*, Monografie Prawnicze Akademii Leona Koźmińskiego, Warszawa 2009, s. 141.

Chcąc poznać zjawisko rozkładu przestrzennego pisma – z uwzględnieniem przede wszystkim jego linearności będącej następstwem bardziej złożonych odruchów warunkowych – wykorzystano materiał poglądowy zawarty w rozprawach doktorskich: Anny Konopackiej[4], Mirosława Sójki[5], Magdaleny Białas[6]; w monografiach

[4] A. Konopacka, *Obraz pisma u osób z guzem mózgu. Studium kryminalistyczne* (rozprawa doktorska), WPiA Uniwersytetu Śląskiego, Katowice 2008.
[5] M. Sójka, *Epizod depresyjny i jego obraz w piśmie ręcznym* (rozprawa doktorska), WPiA Uniwersytetu Śląskiego, Katowice 2006.
[6] M. Białas, *Pismo osób z otępieniem typu alzheimerowskiego* (rozprawa doktorska), WPiA Uniwersytetu Śląskiego, Katowice 2006.

W. Chłopickiego i J.S. Olbrychta[7], Moniki Całkiewicz[8], w pracy magisterskiej Sylwii Ławrentjew[9] oraz w zbiorach własnych autora niniejszego artykułu.



Fot. 2. Rękopis licealisty dotkniętego dysgrafią oraz dysortografią. Widoczne niewielkie zaburzenia linearności, przesunięcia względem linii podstawowej wyrazu czy nawet względem linii podstawowej całego wiersza. Występują także zakłócenia w odległościach pomiędzy poszczególnymi wyrazami, są one nierównomierne.

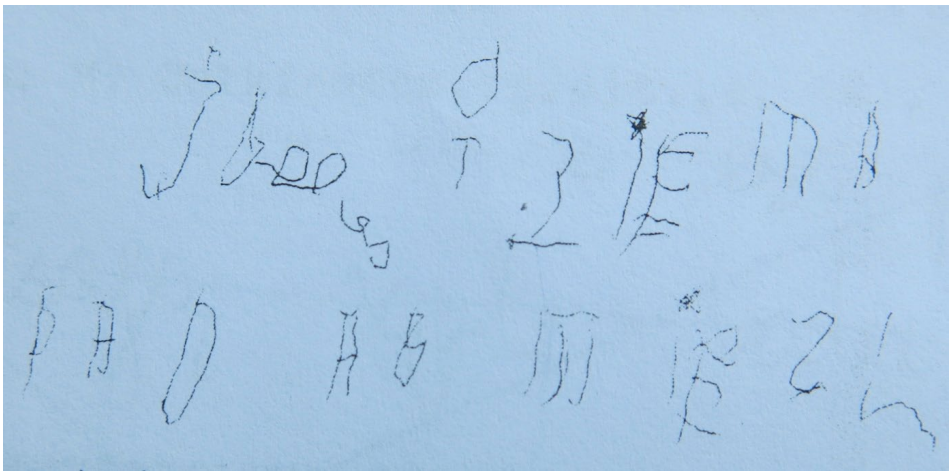
Źródło: M. Całkiewicz, op. cit., s. 123.

Wymieniony materiał badawczy, chociaż zawiera struktury graficzne o podłożu patologicznym, który może dostarczyć pewnych informacji co do podjętego w tym artykule tematu i wnosić pewne wartości poznawcze, jednak jest daleki od doskonałości. W licznych przypadkach jest on fragmentaryczny, zawiera np. jeden wiersz, a nawet jeden wyraz, i stąd też pod względem ilościowym jako krótki, pozbawiony większej liczby wierszy, został wyeliminowany. Nie mógł dostarczyć właściwych informacji co do badanego przedmiotu, zakreślonego do rozkładu przestrzennego pisma – do zbadania np. odległości pomiędzy poszczególnymi wierszami, a nawet do zbadania układu wierszy względem podłoża lub też linii podstawowej wiersza czy linii podstawowej wyrazu. Oceniając zatem materiał badawczy z punktu widzenia ilościowo-jakościowego, należy go uznać za nie całkiem obiektywny w kontekście całokształtu rozważanych tu właściwości graficznych, związanych z szeroko pojętą linearnością, czyli z rozkładem przestrzennym struktury graficznej o cechach patologicznych. Oczywiście, taki stan rzeczy odbija się niekorzystnie na wynikach badań. Mogą one nie być całkowicie obiektywne w odniesieniu do stanu faktycznego będącego następstwem zaburzeń struktury graficznej, spowodowanych chorobami neurologicznymi oraz psychicznymi.

[7] W. Chłopicki, J.S. Olbrycht, op. cit.

[8] M. Całkiewicz, *Kryminalistyczne badania patologicznego pisma ręcznego*, Monografie Prawnicze Akademii Leona Koźmińskiego Warszawa 2009.

[9] S. Ławrentjew, *Znamiona grafizmu osób dotkniętych chorobą Parkinsona* (praca magisterska), Katedra Kryminalistyki WPiA Uniwersytetu Śląskiego, Katowice 2010 (wymienione w przypisach 4, 5, 6, 9 rozprawy zostały opracowane pod kierunkiem naukowym prof. dr. hab. T. Widły i jako maszynopisy znajdują się w Bibliotece WPiA Uniwersytetu Śląskiego w Katowicach).

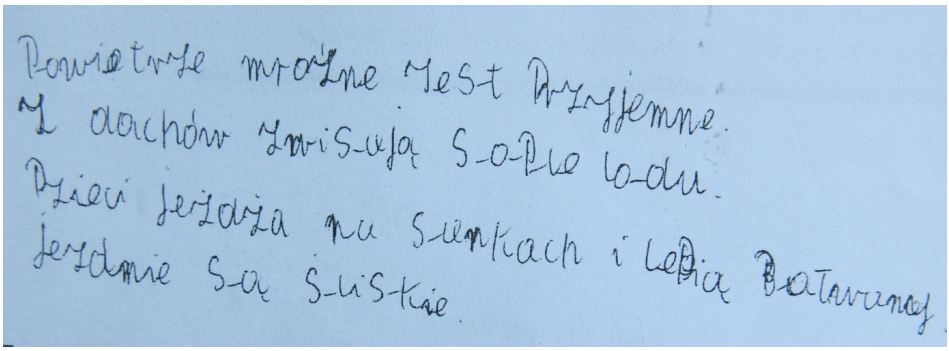


Fot. 3. Rękopis 16-letniego chłopca dotkniętego dysgrafią nabytą (zatrzymanie krążenia, niedotlenienie mózgu). Widoczne znaczne zakłócenia we wszystkich zjawiskach rozkładu przestrzennego: w linearności, w układzie liter, wyrazów i wierszy względem linii podstawowej tych jednostek graficznych. Widoczne są także zakłócenia w odległościach pomiędzy tymi elementami graficzno-językowymi.

Źródło: M. Całkiewicz, op. cit., s. 144.

Dodatkowym mankamentem – z punktu widzenia metodologicznego – jest brak definicji dla niektórych pojęć związanych z szeroko pojętą linearnością. Chodzi tu głównie o właściwości grafometryczne – o odległości istniejące pomiędzy poszczególnymi literami, wyrazami i wreszcie pomiędzy poszczególnymi wierszami, a nawet łączące się z zaburzeniami związanymi ściśle z samą linearnością w znaczeniu wąskim – w prowadzeniu wiersza w wyznaczonym kierunku, uzależnionym od charakteru struktury językowej, która w przypadku języka pisanego ma rozkład przestrzenny, co powoduje, że poszczególne wiersze układają się poziomo względem nie tylko podłoża, ale także względem linii podstawowej wiersza, a nawet wyrazu. Z metodologicznego punktu widzenia powstaje zatem problem, kiedy właściwości te są pozbawione charakteru patologicznego, a kiedy są już następstwem chorobowym. Brak definicji w tym zakresie powoduje pewną dowolność w interpretacji tych zjawisk graficznych. Potrzebne w tym względzie byłyby definicje np. o charakterze projektującym i zarazem regulującym lub konstruktywnym[10]. Takich definicji – na dzień dzisiejszy – brak, co również sprawia, że uzyskane dane ilościowe w niniejszych badaniach mogą być nieco zafałszowane. A nawet są.

[10] Z. Ziembiński, *Logika praktyczna*, Wydawnictwo Naukowe PWN, Warszawa 1994, s. 64.



Fot. 4. Rękopis sporządzony przez 20-letniego chłopca z upośledzeniem umysłowym w stopniu umiarkowanym. Widoczne zakłócenia, chociażby niewielkie, we wszystkich właściwościach graficznych rozkładu przestrzennego.

Źródło: M. Całkiewicz, op. cit., s. 181.

Poczynione zastrzeżenia co do materiału badawczego i innych zagadnień metodologicznych nie są aż tak daleko idące, by nie dostarczały cennych informacji w zakresie zaburzeń linearności pisma, spowodowanych chorobami neurologicznymi oraz psychicznymi. Nawet tak skromny materiał badawczy w świetle przeprowadzonej analizy opisowej pozwala na sformułowanie dosyć jednoznacznych wniosków w zakresie rozkładu przestrzennego „swoistych cech" wywołanych chorobami wspomnianymi wyżej. Nie jest to zresztą żadnym zaskoczeniem, jeżeli się zważy, że stwierdzone różnice są spowodowane odmiennymi przyczynami: w przypadku chorób neurologicznych są następstwem „organicznych uszkodzeń układu nerwowego"[11], natomiast w przypadku chorób psychicznych wynikają z „chorobliwych zmian psychicznych osobowości ludzkiej, a więc dotyczą zarówno życia intelektualnego, jak i uczuciowo-popędowego jednostki"[12].

Z przywołanych powyżej cytatów należałoby zatem wnosić, że analiza opisowa badanego w tym artykule materiału potwierdza tylko to, co już wcześniej w przedmiotowych rozważaniach ustalono. Chociaż potwierdzenie wcześniej uzyskanych wyników jest w tym przypadku cenne z punktu widzenia naukowego, to jednak przeprowadzona analiza opisowa przedmiotowych zaburzeń w tym miejscu ma dodatkowe walory poznawcze. W tej analizie został uwzględniony nie tylko medyczny punkt widzenia, sprowadzony do zasadniczych przyczyn zakłóceń w strukturze graficznej, w wyniku których pojawiają się „cechy swoiste" w przedmiotowym materiale badawczym, ale także – co w tym przypadku jest istotne – punkt widzenia grafologiczny. Sprowadza się on do tych szczegółów identyfikacyjno-grafologicznych, które w ekspertyzie kryminalistycznej pisma ręcznego mają niejako dodatkowy walor poznawczy – walor identyfikacyjny w zakresie stwierdzenia relacji jednorodności zaistniałej

[11] W. Chłopicki, J.S. Olbrycht, op. cit., s. 14.
[12] Tamże, s. 15.

pomiędzy materiałem kwestionowanym i porównawczym. Problem w tym, że w relacjach pojęć o zakresie szerszym, np. „linearność" lub „rozkład przestrzenny", w grę wchodzą także pojęcia o zakresie węższym. „Linearność" to nie tylko wiersz biegnący od lewej do prawej krawędzi podłoża, wzdłuż linii poziomej, ale także układ znaków literowych w stosunku do linii podstawowej wyrazu, a nawet całego wiersza. To również przesunięcia tych znaków ku górze lub w dół od linii podstawowej lub też brak tych przesunięć. W zakresie tym mieszczą się też właściwości grafometryczne odnoszące się do odległości pomiędzy poszczególnymi literami, wyrazami, a także pomiędzy poszczególnymi wierszami o zróżnicowanym układzie względem podłoża, np. układzie wznoszącym, opadającym czy najczęściej wymienianym – tzn. poziomym. Każde z tych pojęć o zakresie węższym wchodzi w zakres pojęć o zakresie szerszym[13], takich jak „linearność" względnie „rozkład przestrzenny" struktury graficznej. Chodzi tu nie tylko o zakresowość wymienionych pojęć, ale także i o to, że każde z nich ze względu na zawartą treść odnosi się do ściśle oznaczonego desygnatu, do jego cech zarówno konstytutywnych[14], jak i konsekutywnych. Jednym słowem, pojęcia te wzbogacają informacyjnie pojęcia nadrzędne, jakimi są pojęcie „linearności" oraz „rozkładu przestrzennego". Z punktu widzenia identyfikacyjnego, ze względu na wzbogaconą informację, przyczyniają się do prawidłowego opiniowania odnoszącego się do nie tylko do wskazania osoby, ale także do jej właściwości fizjologiczno-psychologicznych. To zaś może mieć znaczenie prawne, może się bowiem odnosić do zdolności np. testowania, darowizny lub zawierania innych umów cywilnoprawnych.

Tab. 1. Dane ilościowo-jakościowe zaburzeń w linearności struktury graficznej pisma, uzyskane z populacji dotkniętej chorobami o podłożu neurologiczno-psychicznym, objętymi w badaniach prac doktorskich, monografiach oraz innych publikacjach

L.p.	Jednostka chorobowa oraz wielkość próby	u.w. wzgl.p.	u.l.w. l.p.w.	u.l.w.l.p. wyrazu	o.p. literami	o.p. wyrazami	o.p. wierszami
1	depresja epizodyczna (40)	b.z. (100%)	b.z. 37 (92,5%) z. 3 (7,5%)	b.z. (100%)	b.z. (100%)	b.z. (100%)	b.z. (100%)
2	schizofrenia (5)	b.z. (100%)	b.z. (100%)	b.z. (100%)	b.z. (100%)	b.z. (100%)	b.z. (100%)

[13] Z. Ziembiński, op. cit., s. 38–41.
[14] Tamże, s. 29–32.

3	oligofrenia (20)	b.z. 3 (15%) z. 17 (85%)	b.z. 3 (15%) z. 17 (85%)	b.z. 18 (90%) z. 2 (10%)	b.z. 5 (25%) z. 15 (75%)	b.z. 7 (35%) z. 13 (65%)	b.z. 3 (15%) z. 17 (85%)
4	dysgrafia rozwojowa (24)	b.z. 21 (85%) z. 3 (15%)	b.z. 18 (75%) z. 6 (25%)	b.z. 18 (75%) z. 6 (25%)	b.z. 19 (79%) z. 5 (21%)	b.z. 20 (83%) z. 4 (17%)	b.z. 21 (87,5%) z. 3 (12,5%)
5	dysgrafia nabyta (5)	b.z. 3 (60%) z. 2 (40%)	b.z. 1 (20%) z. 4 (80%)	b.z. 1 (20%) z. 4 (80%)	b.z. 2 (40%) z. 3 (60%)	b.z. 2 (40%) z. 3 (60%)	b.z. 5 (100%)
6	otępienie typu alzheimerowskiego (38)	b.z. 18 (47%) z. 20 (53%)	b.z. 9 (24%) z. 29 (76%)	b.z. 8 (24%) z. 30 (79%)	b.z. 16 (42%) z. 22 (58%)	b.z. 28 (74%) z. 10 (26%)	b.z. 3 (8%) z. 35 (92%)
7	choroba Parkinsona (20)	b.z. 20 (100%)	b.z. 8 (40%) z. 12 (60%)	b.z. 5 (25%) z. 15 (75%)	b.z. 10 (50%) z. 10 (50%)	b.z. 17 (85%) z. 3 (15%)	b.z. 3 (15%) z. 17 (85%)
8	guzy mózgu (33)	b.z. 15 (54,5%) z. 18 (54,5%)	b.z. 16 (48,5%) z. 17 (51,5%)	b.z. 16 (48,5%) z. 17 (51,5%)	b.z. 22 (66,7%) z. 11 (33,3%)	b.z. 20 (60,7%) z. 13 (39,3%)	b.z. 18 (54,5%) z. 15 (45,5%)

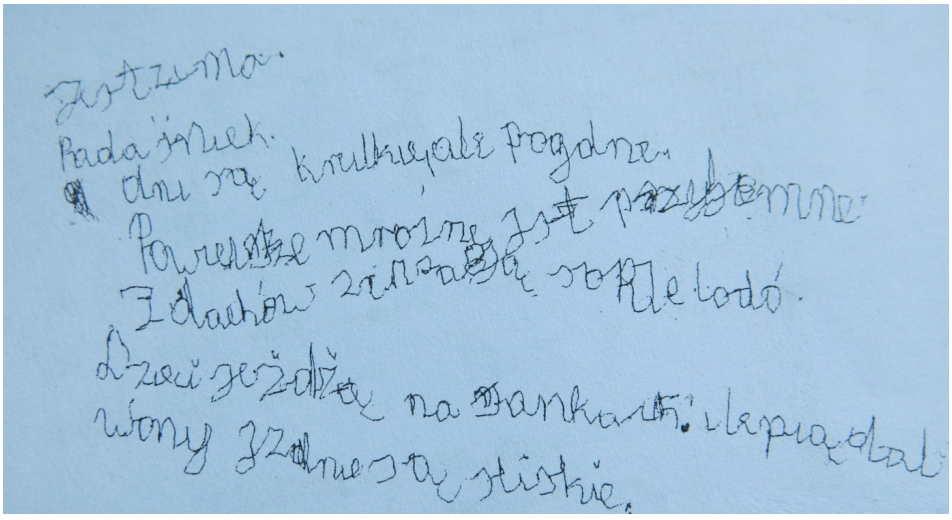
Objaśnienie skrótów:

1. u.w.wzgl.p. – układ wiersza względem podłoża;
2. u.l.w.l.p.w. – układ linii (wiersza) względem linii podstawowej wiersza;
3. u.l.w.l.p. wyrazu – układ linii (wiersza) względem linii podstawowej wyrazu;
4. o.p. literami – odległości pomiędzy poszczególnymi literami;
5. o.p. wyrazami – odległości pomiędzy wyrazami;
6. o.p. wierszami – odległości pomiędzy wierszami;
7. b.z. – bez zakłóceń;
8. z. – zakłócenia.

Do danych ilościowo-jakościowych zamieszczonych w tab. 1 należy się odnosić z rezerwą z przyczyn podanych już wcześniej. Jednak nie należy ich bagatelizować, przede wszystkim z punktu widzenia jednostki chorobowej i – oczywiście – z punktu widzenia badań identyfikacyjnych. Główną przyczyną tak wyrażonego stanowiska

krytycznego jest brak zdefiniowania szeregu pojęć[15] odnoszących się – ogólnie rzecz traktując – do rozkładu przestrzennego pisma, który w kontekście literatury uchodzi za właściwość trudną do naśladowania[16]. Wedle stanowiska, że właściwość ta jest trudna do naśladowania, jej wartość poznawcza znacznie wzrasta w kontekście ingerencji odruchu warunkowego fałszerza w odruch warunkowy tej osoby, której pismo lub podpis ma się stać przedmiotem fałszerstwa. Wprawdzie w kontekście omawianych tu zagadnień jest to szczegół, jednak o tyle ważny, że nie należy o nim zapominać.

Wracając do zasadniczych trudności – do braku zdefiniowania niektórych pojęć związanych z rozkładem przestrzennym pisma, co ma bezpośredni niekorzystny wpływ na zakwalifikowanie danego zaburzenia, czy ma ono jeszcze charakter naturalnego odruchu warunkowego w postaci nawyku graficznego, czy też jest już następstwem przyczyn patologicznych określonej jednostki chorobowej (najczęściej neurologicznej lub psychicznej), należy zauważyć, że poczynione zaszeregowanie przedmiotowych właściwości może mieć charakter subiektywny. Może być on bowiem uzależniony od doświadczenia wiążącego się z identyfikacją kryminalistyczną człowieka na podstawie pisma ręcznego.



Fot. 5. Rękopis sporządzony przez 11-letniego chłopca po usunięciu guza mózgu. Widoczne zakłócenia we wszystkich właściwościach graficznych rozkładu przestrzennego.

Źródło: M. Całkiewicz, op. cit., s. 152.

[15] A. Feluś, *Odchylenia materialne w piśmie osobniczym – Z zagadnień grafologicznych i ekspertyzy pismoznawczej*, „Prace Naukowe Uniwersytetu Śląskiego", Katowice 1979.

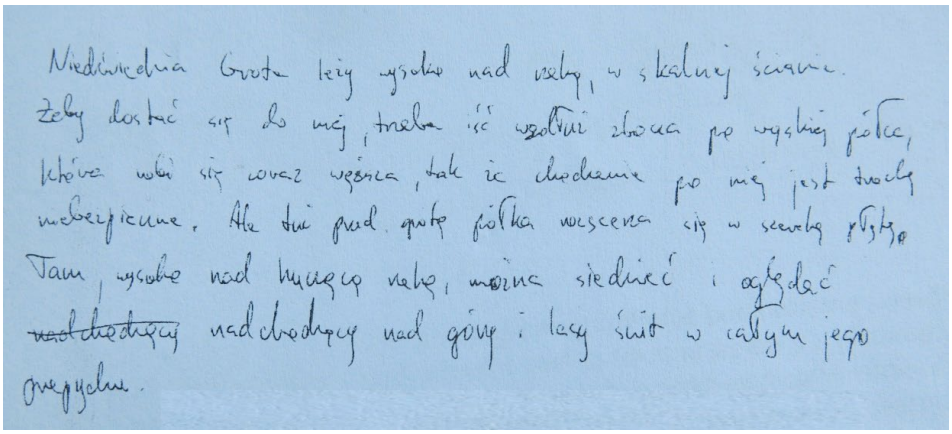
[16] P. Halder-Sinn, *Trudności naśladowania cech przestrzennych w piśmie ręcznym*, w: Z. Kegel (red.), *Problematyka dowodu z ekspertyzy dokumentów*, Katedra Kryminalistyki Wydziału Prawa, Ekonomii i Administracji Uniwersytetu Wrocławskiego, Wrocław 2002, t. I, s. 208–212.

Wprawdzie stanowisko badawcze nacechowane subiektywizmem poznawczym w opisywanym przedmiocie rozkładu przestrzennego pisma nie musi się odnosić do wszystkich właściwości graficznych wchodzących w zakres tego pojęcia, ale wyłącznie do takich zaburzeń, które w tym przypadku – na rzecz niniejszych rozważań – można by nazwać zaburzeniami nieistotnymi, tzn. takimi, które ze względu na swe parametry przede wszystkim jakościowo-ilościowe nie „narzucają się" ekspertowi jako „swoiste właściwości". Dla przykładu można tu podać np. odległości pomiędzy poszczególnymi literami, wyrazami czy nawet wierszami albo takie właściwości, które odnoszą się do wzajemnego układu podstaw literowych względem linii podstawowej wyrazu lub wyrażenia czy nawet całego wiersza. Ze względu na podane właściwości stan zaburzeń może być – w niektórych przypadkach – faktycznie trudny do jednoznacznego zaszeregowania takiej cechy, do oceny, czy jest już ona pochodzenia patologicznego, czy też jeszcze nie.

Ponieważ przedstawiony opis zjawiska rozkładu przestrzennego nie może uchodzić za zadowalający z powodu niedookreśloności wyrażenia „zaburzenie nieistotne", należałoby to wyrażenie doprecyzować. Nazwać je zaburzeniem przypadłościowym, cechą konsekutywną[17], drugorzędną, wynikającą ze swoistych okoliczności, w jakich dana struktura graficzna powstała[18], a nie zaś zaburzeniem pochodzenia patologicznego, będącym następstwem dysfunkcji systemu nerwowego z całym układem kostno-stawowym, włącznie z zaburzeniami psychicznymi. W takim kontekście poznawczym zaburzenie wynikające z okoliczności, w jakich dana struktura została sporządzona, będzie mieć wyłącznie charakter przypadłościowy, łatwy do rozpoznania w kontekście bezstronnego materiału porównawczego, pochodzącego ze ściśle określonego etapu rozwoju ontogenetycznego człowieka. Takie właśnie zaburzenie przypadłościowe jako cecha drugorzędna nie będzie mieć obrazu trwałego. Jej nietrwałość zostanie zdefiniowana w kontekście bezstronnego materiału porównawczego.

[17] Z. Ziembiński, op. cit., s. 30.

[18] T. Widła, *Wpływ pozycji pisarskiej na grafizm*, w: *Materiały VII Wrocławskiego Sympozjum Badań Pisma Ręcznego*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 1997.



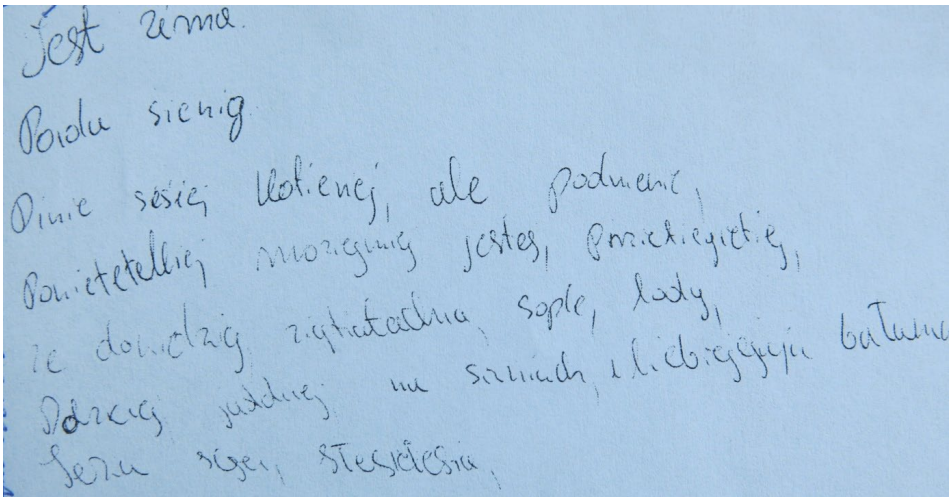
Fot. 6. Rękopis sporządzony przez 27-letniego mężczyznę cierpiącego na schizofrenię przewlekłą. Brak zakłóceń graficznych we wszystkich właściwościach rozkładu przestrzennego.

Źródło: M. Całkiewicz, op. cit., s. 243.

Inny obraz graficzny będzie mieć natomiast zaburzenie o podłożu patologicznym, chorobowym. Będzie zaburzeniem o cesze konstytutywnej. W związku z tym będzie mieć obraz graficzny stały, nie do usunięcia w świetle właściwego materiału porównawczego, o którym wspomniano wyżej. Zatem w kontekście tego, co dopiero powiedziano, można podać definicję zaburzenia w rozkładzie przestrzennym, mającego charakter patologiczny, a nie przypadłościowy, będący następstwem tego, że odruch warunkowy nie powtarza się z dokładnością matematyczną, albo też wynikający z doraźnych okoliczności, w jakich dana struktura graficzna powstała[19]. Można zatem powiedzieć, że zaburzenie w rozkładzie przestrzennym pisma (lub podpisu) ma charakter patologiczny wówczas, kiedy jego obraz graficzny jest trwały, niezmienny do czasu, kiedy przyczyna tego zaburzenia ustąpi.

W kontekście powyżej przedstawionej definicji zagadnienie rozkładu przestrzennego jest bliższe z punktu widzenia poznawczego, chociaż nie do końca. Wprawdzie podana definicja wyjaśnia, kiedy mamy do czynienia z faktycznym zaburzeniem patologicznym rozważanej właściwości struktury graficznej pisma, nie zaś z zakłóceniem doraźnym, przypadłościowym, o czym decyduje różnica gatunkowa w postaci trwałego zaburzenia obrazu graficznego linii, odnosi się więc wyłącznie do stałości tego zjawiska graficznego, a nic nie mówi o nim z punktu widzenia ilościowego badanej cechy jako „swoistej przypadłości".

[19] S. Podgajny, *Wpływ tempa kreślenia i pozycji pisarskiej na obraz podpisów własnoręcznych*, „Zeszyty Metodyczne", nr 27, Wydawnictwo CLK KGP, Warszawa 2003.



Fot. 7 . Rękopis sporządzony przez 35-letnią kobietę cierpiącą na schizofrenię przewlekłą oraz dotkniętą upośledzeniem umysłowym w stopniu umiarkowanym.

Źródło: M. Całkiewicz, op. cit., s. 256.

Z tym zaś jest większy kłopot. Wydaje się, że problem, chociaż nie do końca, mogłaby przypuszczalnie rozwiązać definicja regulująca lub konstruktywna[20], oparta na informacji pochodzącej z właściwego materiału badawczego – z próby badawczej pozyskanej od osób zdiagnozowanych co do jednostki chorobowej oraz jej zaawansowania. Pomocą w tym względzie mogłaby być norma związana z tym zjawiskiem graficznym, nakazująca piszącemu prowadzić wiersz poziomo, od lewej do prawej krawędzi podłoża, w ściśle określonych odległościach pomiędzy nimi samymi, a także pomiędzy elementami graficznymi (literami) wchodzącymi w skład poszczególnych jednostek leksykalnych lub zdaniowych. Nawiązuje to w jakimś stopniu do obowiązujących niegdyś norm kaligraficznych w nauce pisma ręcznego. Narzucone odgórnie reguły mające za zadanie utrzymać w porządku harmonicznym cały obraz struktury graficznej, by pismo było nie tylko czytelne, ale także estetyczne, zostały już dawno zarzucone. Jednak i w czasie obowiązywania tychże reguł odruch warunkowy nie dał się całkowicie „ujarzmić" rygorystycznymi przepisami i w miarę stopniowego ich osłabiania, a następnie całkowitego zarzucenia, w ten sposób wyzwolony odruch rzeźbił z upływem czasu zwiększoną ekspresję graficzną nie tylko w obrębie niższego systemu struktury graficznej, tzn. na poziomie literowym, ale także na poziomie systemu wyższego – w ich wiązaniu literowym, nadając mu charakter linearny, nierozerwalnie związany z rozkładem przestrzennym pisma na podłożu.

Znając kontekst wynikający z definicji klasycznej mówiącej o zaburzeniu w rozważanym zakresie jako o zjawisku patologicznym, przybierającym trwały obraz graficzny o cesze jakościowej, oraz właściwość odruchu warunkowego, decydującą

[20] Z. Ziembiński, op. cit., s. 46.

o tym, że jest indywidualny, chociaż nie powtarza się z dokładnością matematyczną[21], można będzie lepiej zrozumieć trudności w rozgraniczeniu, co w rozkładzie przestrzennym jest zaburzeniem pochodzenia patologicznego – skutkiem takiej czy innej choroby – a co obrazem graficznym przypadłościowym, drugorzędnym, wynikającym przede wszystkim z charakteru odruchu warunkowego oraz zewnętrznych czy nawet wolicjonalnych okoliczności towarzyszących każdorazowej czynności pisania.

Powyższa świadomość poznawcza wynikająca zasadniczo z dwóch źródeł naukowych – definicji klasycznej oraz istoty odruchu warunkowego – przy dysponowaniu właściwym materiałem badawczym pochodzącym od osób zdiagnozowanych medycznie pod względem jednostki chorobowej oraz jej zaawansowania – może się stać podstawą do zdefiniowania zjawiska patologicznego związanego z rozkładem przestrzennym struktury graficznej, które najprawdopodobniej charakteryzuje się nie tylko aspektem jakościowym, ale także ilościowym. Przypuszczalnie można by to osiągnąć za pomocą definicji regulującej lub konstruktywnej, o czym wspomniano już wyżej.

Skoro jednak, na dzień dzisiejszy, warunki podane powyżej nie są spełnione w sposób należyty, tzn. taki, który nie budziłby żadnych zastrzeżeń metodologicznych, uzyskane wyniki badań, zawarte w poszczególnych rubrykach tab. 1, chociaż są obarczone subiektywizmem poznawczym, jak zaznaczono wcześniej, nie są bezwartościowe w kontekście zaburzeń struktury graficznej pisma. Przede wszystkim dowodzą, że i ten aspekt struktury graficznej dotyka choroba, powodując w nim zaburzenia o zróżnicowanym aspekcie zarówno jakościowo-ilościowym, jak i pod względem pozostałych właściwości będących wynikiem czynności psychofizycznej w postaci struktury graficzno-językowej, uzależnionej od tego dwojakiego aspektu kondycji ludzkiej.

Na szczególną uwagę zasługuje fakt, że takie choroby o podłożu psychicznym jak m.in. depresja epizodyczna albo schizofrenia „czysta”[22] nie wywołują prawie żadnych zakłóceń w rozkładzie przestrzennym pisma, choroby o podłożu neurologicznym zaś – w zależności od stanu chorobowego – powodują znaczne zaburzenia we wszystkich aspektach tego rozkładu[23], począwszy od układu wierszy względem podłoża aż po odległości pomiędzy tymi jednostkami graficznymi. We wskazanych przypadkach opisywane zjawisko graficzne prawie w 100% pozostaje bez żadnych zakłóceń. Nieco inny obraz tego zjawiska przedstawia się w strukturze graficznej będącej pochodną chorób neurologicznych. Dane w tab. 1 wskazują, że struktura graficzna jako pochodna ściśle określonej jednostki chorobowej o etiologii neurologicznej powoduje zaburzenia jakościowo-ilościowe w strukturze graficznej pisma, w zakresie niemal wszystkich aspektów rozkładu przestrzennego. Odsetki tych zaburzeń wynoszą od 15% do 93%, w przypadku choroby Alzheimera oraz guza mózgu są one najwyższe, sięgają od 26% do 93%. Także w dysgrafii nabytej pozostają wysokie,

[21] Z. Ziółkowski, *Znaczenie zaburzeń pisma w przebiegu pląsawicy mniejszej*, PWN Oddział w Poznaniu, Bydgoszcz 1970.

[22] W. Chłopicki, J.S. Olbrycht, op. cit., s. 14–19.

[23] Ibidem.

sięgają od 40% do 80%. Natomiast w dysgrafii rozwojowej odsetki zakłóceń są najniższe i mieszczą się w przedziale od 12,5% do 25%[24].

Uzyskany opis ilościowy zaburzeń o charakterze patologicznym w strukturze graficznej pisma, sprowadzonej w tym miejscu do rozkładu przestrzennego w szerokim tego słowa znaczeniu, ma interesujący wkład poznawczy jako samodzielna jednostka zaburzeniowa, wchodząca w skład pojęcia pisma patologicznego, zaburzonego przyczynami neurologiczno-psychiatrycznymi. Taki stan rzeczy ma znaczenie zarówno w identyfikacji kryminalistycznej, jak i w sytuacji stawiania diagnozy, o ile potrzeba taka by zaistniała.

Streszczenie

Artykuł poświęcony jest jednej z cech analizowanych w badaniach pisma ręcznego – tzw. linearności pisma. Autor zwraca uwagę na wartość poznawczą tej cechy, szczególnie w analizie pisma patologicznego.

Słowa kluczowe: badania pisma ręcznego, pismo patologiczne, cechy pisma ręcznego

Summary

Article is devoted to one of the feature of handwriting – so-called: „linearity of handwriting". Author pays attention to the importantce of that feature, particularly in analysis of pathological handwriting.

Keywords: handwriting analysis, pathological handwriting, feature of handwriting

[24] M. Całkiewicz, op. cit., s. 99–107; zob. także s. 98.

Michał Górski

PODSTAWY PROFILOWANIA GEOGRAFICZNEGO

Basics of geographic profiling

Profilowanie geograficzne jest to zbiór metod mających na celu przybliżanie prawdopodobnego miejsca zamieszkania sprawcy danego przestępstwa bądź przestępstw. Metoda ta została opracowana między innymi przez Kima Rossmo i po raz pierwszy zastosowano ją w sprawie zniknięć prostytutek z ulic Vancouver. Geograficzne zależności zauważone przez Rossmo pozwoliły stwierdzić, że w tym mieście grasuje seryjny zabójca, a co więcej, przybliżyć jego miejsce zamieszkania[1]. Po aresztowaniu Roberta Picktona sierżant policji z Vancouver przyznał, że niechęć policjantów do metody proponowanej przez Rossmo mogła przyczynić się do spowolnienia śledztwa, jednocześnie umożliwiając sprawcy dokonywanie kolejnych zabójstw[2]. Pickton w więzieniu pochwalił się współwięźniowi, że dokonał 49 zabójstw, przy czym oskarżony był o 26, natomiast skazany za 6 zdarzeń.

Metody profilowania geograficznego opierają się na wykorzystaniu analiz statystycznych dostępnych zdarzeń opisujących zależności kierujące postępowaniem sprawców, ze szczególnym uwzględnieniem zachowań przestrzennych, takich jak np. odległość pokonana od miejsca zamieszkania sprawcy do miejsca zdarzenia[3]. Taka analiza umożliwia wskazanie najbardziej prawdopodobnego miejsca zamieszkania nieznanego sprawcy. Stosowanie reguł prawdopodobieństwa w praktyce śledczej pozwala na optymalizację dochodzenia poprzez wskazywanie najlepszych obszarów poszukiwań. Zaczynając od takich wyznaczonych obszarów i kierując się do miejsc o mniejszym prawdopodobieństwie, śledczy maksymalizują szanse znalezienia sprawcy danych przestępstw. W konsekwencji stosowanie takiego podejścia może znacząco ograniczyć koszty.

Niestety nawet w literaturze specjalistycznej zdarza się, że zasady profilowania geograficznego opisywane są błędnie. W książce *Serial Crime*[4] metody oparte na rozkładach zostały opisane w następujący sposób: „Jako przykład czerwony obszar pośrodku mapy reprezentuje 95% prawdopodobieństwa, pomarańczowy 90% i tak

---

[1] W. Petherick, R. Brogan, N. Brooks, C. Ferguson, E. Fry, D. Field, B. Woodhouse, *Serial Crime: Theoretical and Practical Issues*, Anderson Publishing Co., Cincinnati 2006.
[2] S. Chainey, J. Ratcliffe, *GIS and Crime Mapping*, John Wiley & Sons Ltd., Chichester 2005.
[3] Tamże.
[4] W. Petherick, R. Brogan, N. Brooks, C. Ferguson, E. Fry, D. Field, B. Woodhouse, op. cit.

dalej". Ogólna zasada działania przedstawiona została słusznie, jednak warto zauważyć, że we wskazanym przykładzie prawdopodobieństwo, iż sprawca znajduje się w obszarze pomarańczowym lub czerwonym, wynosi łącznie 185%, co jest niemożliwe. Co więcej, takie opisanie profilowania geograficznego daje fałszywe przekonanie o działaniu metody i w efekcie może powodować, że będą wobec niej stawiane nierealistyczne oczekiwania. Aby zrozumieć, w jaki sposób działa profilowanie geograficzne, wyobraźmy sobie prostą grę polegającą na zgadywaniu liczby oczek przy rzutach kostką. Jeśli kostka jest symetryczna i dobrze wyważona, prawdopodobieństwo trafienia wynosi 1/6 i jest takie samo dla każdej liczby oczek. Załóżmy, że w grze nie sprawdzamy sami liczby oczek, tylko pytamy osobę rzucającą kostką: „Czy wyrzucono liczbę *n*?" (gdzie *n* należy do zbioru liczb 1–6). Jeśli nie zgadliśmy za pierwszym razem, pytamy ponownie i tak do momentu, aż zgadniemy.

Po prawidłowym wskazaniu liczby oczek osoba ponownie rzuca kostką i zaczyna się nowa tura gry. Jeśli jest kilka osób zgadujących, to wygrywa ta, której udawało się zgadnąć liczbę oczek w mniejszej ilości kroków. Przy symetrycznej kostce nie ma strategii dającej przewagę i każdy ze zgadujących wykona średnio 3,5 kroku w każdej turze, aż poprawnie zgadnie wylosowaną liczbę.

Jednak wystarczy, żeby kostka była odrobinę źle wyważona, i już następują zmiany w prawdopodobieństwie. Wyobraźmy sobie kostkę, w której prawdopodobieństwo wylosowania 1 wynosi 2/6, dla każdej z liczb 2, 3, 4, wynosi 1/6, natomiast dla 5 i 6 prawdopodobieństwo wylosowania wynosi odpowiednio 2/18 i 1/18. W takiej sytuacji jeśli osoby zgadujące nie są świadome wadliwości kostki i podają liczby w losowej kolejności, prawdopodobieństwo zgadnięcia pozostaje dla nich niezmienione. Dalej każda z nich wykona średnio 3,5 kroku w każdej turze gry. Może istnieć gracz, który notował poprzednie wyniki i przeprowadził ich analizę, co doprowadziło do prawidłowego oszacowania istniejących prawdopodobieństw. Ten gracz zyskuje znaczącą przewagę nad pozostałymi, gdyż obstawia najbardziej prawdopodobne wyniki. Zatem najpierw zgaduje, czy wylosowano 1, jeśli nie pyta on o 2, 3, 4, 5 i na koniec o 6. Należy zwrócić uwagę, że kolejność liczb jest związana z prawdopodobieństwem ich występowania. Średnio ten gracz wykona 2,72 kroku w każdej turze gry, czyli prawie o jeden krok mniej od każdego innego gracza. W dalszej części tego gracza będziemy opisywać jako „sprytnego", aby odróżnić go od pozostałych losowych graczy, którzy nie biorą pod uwagę prawdopodobieństwa. Z tego przykładu wynikają cztery poniższe fakty.

Po pierwsze, gracze, którzy zgadują w przypadkowej kolejności, będą poprawnie zgadywać wynik rzutu średnio w 3,5 kroku. Co oznacza, że niezależnie od stopnia wadliwości kostki nie wykorzystują oni tego, aby uzyskać przewagę nad innymi graczami. W szczególnym przypadku kostka może mieć na każdej ścianie taką samą wartość, jednak dalej przy stosowaniu strategii losowej zgadnięcie zajmie tyle samo prób.

Po drugie, liczba, którą obstawiał „sprytny" gracz jako pierwszą (jedynka), nie daje nawet 50% szans na sukces. Jego strategia nie pozwalała trafić za pierwszym

razem (wręcz na odwrót, w 2/3 przypadków gracz ten pomyli się za pierwszym razem), jednak dalej zapewni mu zwycięstwo w opisanej grze.

Po trzecie, nawet „sprytny" gracz będzie popełniał istotne błędy i może się zdarzyć, że trafi dopiero za szóstym podejściem. Jednak będzie to zjawisko zdecydowanie rzadsze niż w przypadku innych graczy. Tak bardzo pomyli się w jednym na 18 rzutów. Pozostali, losowi gracze popełnią taki sam błąd w jednym na 6 przypadków, zatem trzy razy częściej.

Po czwarte, nie istnieje lepsza strategia gry niż ta wykorzystana przez „sprytnego" gracza, żaden gracz więc nie uzyska średnio lepszego wyniku. Natomiast prawdopodobieństwo, że zwykły gracz przez przypadek w odpowiedniej kolejności będzie sprawdzał wynik, wynosi 1/720, czyli zaledwie 0,14%.

Jaki jest związek rzucania kostką i profilowania geograficznego? Wszelkie właściwości opisanej gry przekładają się na właściwości profilowania geograficznego. Metoda ta wskazuje prawdopodobieństwo, z jakim sprawca przestępstw zamieszkuje dany obszar. Podobnie jak w przykładzie z kostką, możemy podzielić obszar poszukiwań na dowolną liczbę mniejszych obszarów, przyporządkować im prawdopodobieństwo i prowadzić poszukiwania zgodnie z tym prawdopodobieństwem. Obranie tej metody da takie same efekty jak w przypadku „sprytnego" gracza z wadliwą kostką. Średnio szybciej będzie się znajdowało rzeczywistego sprawcę przestępstwa po przeszukaniu mniejszego obszaru (mniejszej liczbie zapytań do osoby rzucającej kostką).

Wszelka inna metoda przeszukiwania obszarów będzie mniej opłacalna i będzie generować więcej błędów. Wskazanie w profilu geograficznym najbardziej prawdopodobnego obszaru nie oznacza jednak, że sprawca będzie tam mieszkał z prawdopodobieństwem graniczącym z pewnością (lub chociaż w 50%). Podobnie jak w przypadku gry, prawdopodobieństwo może być nawet dużo mniejsze, jednak wciąż będzie to obszar, od którego opłacalne będzie rozpoczynanie poszukiwań.

Może się zdarzyć, że sprawca będzie zamieszkiwał w obszarze najmniej prawdopodobnym, jednak sytuacja ta będzie rzadka. Co więcej, dzięki opracowaniom statystycznym jest możliwe wskazanie, z jakim prawdopodobieństwem popełniamy taki błąd i co ważniejsze, błąd ten będzie popełniany rzadziej niż przy zastosowaniu jakiejkolwiek innej strategii. Profilowanie geograficzne pozwala zatem priorytetyzować zadania organów ścigania w sytuacji, w której nie ma jednoznacznych podejrzanych. Zastosowanie profilu geograficznego pozwala nadać kierunek podejmowanym działaniom i dzięki temu średnio skrócić postępowania. Analogicznie do przedstawionej gry z kostką, profil informuje o wzorcach zachowań występujących wśród danego typu sprawców i pozwala tę wiedzę wykorzystać. Tak samo jak gracz, który pyta o kolejne wyniki rzutu kostką, można sprawdzać obszary o coraz mniejszym prawdopodobieństwie i kolejno je odrzucać, aż do trafienia właściwego wyniku. Odrzucenie obszaru o danym prawdopodobieństwie może nastąpić z różnych powodów. Jednym z takich powodów może być fakt, że dany teren jest po prostu niezamieszkany. W takim

przypadku należy pamiętać, że oprogramowanie do profilowania geograficznego nie bierze pod uwagę ukształtowania terenu na danym obszarze[5].

Metody profilowania można podzielić na dwa rodzaje. Do pierwszego rodzaju metod zalicza się te wskazujące jeden punkt, który ma być miejscem o najwyższym prawdopodobieństwie znalezienia sprawcy. Im dalej od tego punktu, tym mniejsze prawdopodobieństwo. Metody tego typu nazywamy centrograficznymi. Jednym z najprostszych przykładów takiej metody jest wskazywanie środka odcinka łączącego dwa najodleglejsze zdarzenia w serii. Pozostałe metody oparte na rozkładach prawdopodobieństwa i analizy statystyczne wymagają specjalistycznego oprogramowania. Każdy taki program wylicza w każdym punkcie mapy odpowiedni współczynnik, który wskazuje, z jakim prawdopodobieństwem w danym miejscu zamieszkuje sprawca. Dzięki temu uzyskujemy informacje nie tylko co do położenia miejsca o największym prawdopodobieństwie, ale także o charakterystyce rozkładu wspomnianego prawdopodobieństwa na całym obszarze objętym analizą.

W momencie aplikacji wyników analiz pojawia się często pytanie, czy aby na pewno aktualne zdarzenia należą do tej samej grupy co te brane pod uwagę przy tworzeniu modelu. Analogicznie przy grze z kostką można to przedstawić w następujący sposób. Czy kostka, którą rzucamy w aktualnej turze, jest podobna do poprzednich, na podstawie których wnioskujemy? Sprawa snajperów z Waszyngtonu jest przykładem zdarzeń, w których profil geograficzny (jak i każde statystyczne podejście) okazał się nieskuteczny (sprawcy ci działali w parze, pomimo iż standardowy profil snajpera mówił o pojedynczej osobie). Co więcej, działali oni na wyjątkowo rozległym obszarze nietypowym dla tego typu zdarzeń[6]. Utrudniało to stworzenie profilu geograficznego, który ostatecznie okazał się nierzetelny, gdyż sprawcy podróżowali i żyli jednocześnie w samochodzie, z którego oddawali strzały. Przykład ten obrazuje ostrożność, z jaką należy stosować statystyki. Trzeba mieć na uwadze, że w danym przypadku dostępne analizy mogą nie być właściwe, a w związku z tym należy być wyczulonym na wszelkie anomalie, jakie się pojawiają w danej sprawie. Profilowanie geograficzne, mimo iż oparte na analizach statystycznych, najprawdopodobniej nigdy nie będzie czysto algorytmiczną metodą i zawsze będzie konieczna kontrola ze strony świadomego użytkownika.

W trakcie wprowadzania analogii do gry w kości w pewien sposób po cichu założyliśmy, że wszystkie sprawy można rozwiązać. To założenie przejawiało się w tym, że mieliśmy możliwości sprawdzenia wszystkich możliwych opcji. W naszej grze w kości oznaczało to, że w pewnym momencie musimy zgadnąć właściwy wynik. W trakcie rzeczywistych postępowań nie ma takich możliwości. Z tego względu możemy lekko zmienić zasady gry i powiedzieć, że osoba zgadująca ma prawo w każdej turze zapytać tylko o pięć wartości wyniku rzutu; jeśli za żadnym razem nie zgadła, to sprawca uciekł. Należy zwrócić jednak uwagę, że nie zmienia to w żaden

[5] B. Snook, D. Canter, C. Bennell, *Predicting the home location of serial offenders: a preliminary comparison of the accuracy of human judges with a geographic profiling system*, „Behavioral Sciences & The Law" 2002, No. 20(1/2), s. 109–118.

[6] D.V. Canter, *Mapping Murder. Walking in Killers' Footsteps*, Virgin Books, London 2005.

sposób zasadności i sposobu działania omawianego profilowania geograficznego, gdyż nawet w takiej sytuacji jesteśmy zainteresowani tym, aby jak najmniejsza liczba sprawców nam uciekała, co znaczy, że liczbą, o którą nie będziemy pytać, jest wynik o najmniejszym prawdopodobieństwie. Wynika z tego, że nie zmieni się w żaden sposób kolejność, w jakiej pytamy rzucającego gracza o wynik. Oczywiście w 1/18 przypadków nie zgadniemy wyniku, ale będzie to zawsze rzadziej, niż gdybyśmy zrezygnowali z jakiejkolwiek innej wartości. Naturalnie, można dalej zmniejszać liczbę możliwych pytań do zadania osobie rzucającej, co przekłada się na liczbę dostępnych środków (ile opcji można sprawdzić). Za każdym razem jednak będziemy chcieli odrzucić najmniej prawdopodobną opcję, tak aby zgadnąć jak najczęściej, co w efekcie oznacza, że niezależnie od tego, ile można zadać pytań o wynik rzutu, będą one zawsze zadawane w tej samej kolejności, jeśli tylko gracz bierze pod uwagę prawdopodobieństwo. W przypadku rzeczywistych poszukiwań sprawców oznacza to, że przy ograniczonych środkach należy sprawdzać najbardziej prawdopodobne możliwości. Jak pokazał Canter na przykładzie włamań[7], profil geograficzny pozwala relatywnie szybko wyróżnić sprawy trudniejsze, które wymagają skierowania większej liczby policjantów i środków w celu rozwiązania danej sprawy. Zatem przedstawione rozumowanie sprawdza się nie tylko w uproszczonym teoretycznym modelu, ale także ma przełożenie na praktyczną skuteczność metody.

Wartość profilowania geograficznego może być najlepiej widoczna w przypadku analiz przesiewowych, kiedy cały region ma być objęty badaniami DNA. Jak wiadomo, są one kosztowne, a w takich przypadkach wykonywane w olbrzymich ilościach. Zatem ustalenie obszarów o większym prawdopodobieństwie może oznaczać, że nie będzie konieczności wykonania dziesiątek, a nawet setek niepotrzebnych badań próbek DNA. Jednak nie tylko w takich sprawach metoda profilowania geograficznego może być pomocna. Profilowanie geograficzne pozwala również szeregować podejrzanych. Canter i Hammond[8] w swoich badaniach nad seriami włamań testowali różne metody tworzenia profili. Do każdej serii zdarzeń był tworzony profil geograficzny, według którego następnie szeregowano podejrzanych. W zależności od metody, wśród pierwszych 5% podejrzanych o najwyższym wskaźniku prawdopodobieństwa znajdowało się od 46% do 72% sprawców skazanych za te zdarzenia wyrokami sądu. Bardziej skuteczne okazały się metody oparte na rozkładach, gorzej w tych badaniach wypadły metody centroidalne. Jak widać na tym przykładzie, profilowanie geograficzne może być przydatne w najbardziej typowych przestępstwach. Co więcej, autorzy badań wskazują, że otrzymane zależności pozwalają przewidywać, czy dana sprawa będzie skomplikowana i będzie wymagała dużego nakładu pracy ze strony organów ścigania, co umożliwi wcześniejsze zaplanowanie działań[9].

Profilowanie geograficzne jest także wykorzystywane w celu łączenia zdarzeń w serie. W przypadku włamań spójność przestrzenna i czasowa zdarzeń są lepszym

[7] D.V. Canter, L. Hammond, *Prioritizing burglars: comparing the effectiveness of geographical profiling methods*, „Police Practice & Research" 2007, No. 8(4), s. 371–384.
[8] Tamże.
[9] Tamże.

predyktorem istnienia związku między nimi niż *modus operandi* (sposób włamania, rodzaj użytych materiałów itp.)[10]. Profilowanie geograficzne pozwala łączyć zdarzenia włamań w serię, jednak w porównaniu z innymi przestępstwami gorzej sprawdza się w odniesieniu do wskazania miejsca zamieszkania sprawców. Mimo to stosowanie tej metody dalej pozwala optymalizować śledztwa, ma ona bowiem zdecydowaną przewagę nad innymi sposobami priorytetyzacji podejrzanych. W przypadku innego typu zdarzeń zaobserwowano podobne wyniki, wskazujące między innymi na wysoką relację między minimum a maksimum odległości pokonanej przez sprawców przestępstw seryjnych[11]. Wnioski te potwierdzono na przykład w badaniach na próbie seryjnych sprawców napaści na tle seksualnym[12]. Napastnicy zachowują stałość względem pokonanej odległości oraz do swoich zdarzeń wybierają stałe warunki środowiskowe. Wynika to ze znaczącej roli otoczenia w procesie decyzyjnym sprawców tego typu przestępstw.

Profilowanie geograficzne, podobnie jak profilowanie psychologiczne, ma swoich krytyków. Wskazuje się na nieprzydatność tej metody w niektórych zdarzeniach, np. we wspomnianej wyżej sprawie snajperów z Waszyngtonu[13]. Co więcej, zwraca się uwagę, że ta metoda wyjmuje zdarzenia z ich kontekstu, analizując same miejsca ich położenia. Kim Rossmo zauważał konieczność stworzenia profilu psychologicznego przed profilem geograficznym[14]. Mimo to jemu też zdarzało się tworzyć profile bez wcześniejszego profilu psychologicznego. Wskazuje się także, że stosowanie profilowania geograficznego nie pozwala na rozróżnienie aktywności jednego sprawcy od większej liczby sprawców działających na tym samym terenie[15]. Sugeruje to konieczność włączenia do analiz zachowań sprawców na miejscu zdarzenia.

Taka metodologia pozwala tworzyć typologie sprawców i różne skale zachowań. Umożliwia to rozróżnianie typów zdarzeń, a co za tym idzie, zawiera elementy profilowania psychologicznego. Tego typu podejście zaprezentował Fritzon w 2001 roku badaniach nad sprawcami seryjnych podpaleń. Na podstawie czterech typów podpaleń, które zostały wyróżnione we wcześniejszych badaniach[16], stworzono różne rozkłady prawdopodobieństwa pokonanej odległości[17]. W efekcie na podstawie

[10] L.W. Markson, *Linking serial residential burglary: comparing the utility of modus operandi behaviours, geographical proximity, and temporal proximity*, „Journal of Investigative Psychology and Offender Profiling" 2010, No. 7(2), s. 91–107.

[11] D.V. Canter, *Mapping Murder*..., op. cit.

[12] S. Lundrigan, S. Czarnomski, M. Wilson, *Spatial and environmental consistency in serial sexual assault*, „Journal of Investigative Psychology and Offender Profiling" 2010, No. 7(1), s. 15–30.

[13] W. Petherick, R. Brogan, N. Brooks, C. Ferguson, E. Fry, D. Field, B. Woodhouse, op. cit.

[14] Tamże.

[15] Tamże.

[16] D. Canter, K. Fritzon, *Differentiating arsonists: A model of firesetting actions and characteristics*, „Legal & Criminological Psychology" 1998, No. 3(1), s. 73.

[17] K. Fritzon, *An examination of the relationship between distance travelled and motivational aspects of firesetting behavior*, „Journal of Environmental Psychology" 2001, No. 21(1),

zachowań sprawców udało się wyróżnić różne rodzaje motywacji sprawców podpaleń, jej wpływ na pokonaną odległość, a co najważniejsze, opracować szybką i łatwą metodę oceny tej motywacji. Dzięki temu wyniki badań umożliwiają zastosowanie otrzymanych zależności w praktyce. Badania dotyczące odległości pokonywanej przez sprawców prowadzono między innymi w przypadkach podpaleń[18], włamań[19], zabójstw[20] oraz zgwałceń[21]. Istnieją też próby aplikacji tego podejścia do przewidywania miejsc położenia komórek terrorystycznych[22]. Pokazuje to, że profilowanie geograficzne może być stosowane w pracy policji i prokuratury zarówno w wyjątkowych, rzadkich zdarzeniach, jak i w odniesieniu do najbardziej pospolitych przestępstw.

Analogiczne badania nad zabójstwami prowadziło Koło Naukowe Psychologii Sądowej Wydziału Psychologii Uniwersytetu Warszawskiego. Do badań wybrano zdarzenia, do których nie doszło w rodzinie ze znaną historią przemocy domowej. Zabieg ten miał wyłączyć z badań najbardziej typowe zabójstwa, w których profilowanie nie jest potrzebne. Akta spraw pozyskiwano z Sądu Okręgowego w Warszawie. Otrzymane wyniki potwierdzają zależności wskazywane przez zagranicznych badaczy. Znaleziono zależności między zachowaniem sprawców na miejscu zdarzenia a odległością przez nich pokonaną. Pokazują one także, że choć zdarzają się pojedyncze przypadki pokonywania większych odległości, to w całej populacji jest ona mocno ograniczona. Spośród 104 zdarzeń, w których znana była odległość między miejscem zamieszkania sprawcy a miejscem zdarzenia, zaledwie do pięciu (4,81%) doszło w odległości powyżej 16 km. Oznacza to, że zdecydowana większość zdarzeń nastąpiła w okolicy miejsca zamieszkania sprawcy. Oczywiście konieczne są dalsze badania pozwalające na wnioskowanie w wybranych rodzajach zdarzeń oraz w różnego typu przestępstwach. Ważne jest także, że rozkład odległości pokonywanej przez sprawców był podobny do rozkładu wykładniczego. Oznacza to, że prawdopodobieństwo znalezienia sprawcy spada wraz ze wzrostem odległości od miejsca zdarzenia. W przypadku pojedynczych zdarzeń zatem optymalną strategią poszukiwań jest rozpoczęcie w bezpośrednim sąsiedztwie miejsca zdarzenia i powolne odchodzenie od niego. Oczywiście, należy pamiętać, że wykazane zależności dotyczą całej badanej grupy. Dla pewnych podgrup sprawców można znaleźć różne rozkłady prawdopodobieństwa, tak jak miało to miejsce w badaniach Fritzona[23].

---

s. 45–60.

[18] Tamże.

[19] L.W. Markson, op. cit., s. 91–107.

[20] H. Häkkänen, K. Hurme, M. Liukkonen, *Distance patterns and disposal sites in rural area homicides committed in Finland*, „Journal of Investigative Psychology and Offender Profiling" 2007, No. 4(3), s. 181–197.

[21] J. Warren, R. Reboussin, R.R. Hazelwood, A. Cummings, N. Gibbs, S. Trumbetta, *Crime scene and distance correlates of serial rape*, „Journal of Quantitative Criminology" 1998, No. 14(1), s. 35–59.

[22] D. Rossmo, K. Harries, *The geospatial structure of terrorist cells*, „JQ: Justice Quarterly" 2011, No. 28(2), s. 221–248.

[23] K. Fritzon, op. cit., s. 45–60.

Podsumowując, można uznać, że profilowanie geograficzne jest metodą o wysokiej skuteczności, pozwalającą optymalizować dochodzenia w szerokim spektrum zdarzeń. Istnieje jednak parę problemów związanych z tym podejściem. W polskich warunkach podstawową trudnością jest brak badań nad krajową populacją sprawców. Profilowanie geograficzne, jako metoda indukcyjna, wymaga odpowiedniej bazy informacji dotyczących wcześniejszych, rozwiązanych spraw. Korzyści płynące z odpowiednio zebranych materiałów są znaczne. Dobrze opracowane dane mogą dokładnie wskazywać śledczym optymalne metody poszukiwania sprawców, dzięki temu więc będą oni mieli do dyspozycji nie tylko własne doświadczenie, lecz także zbiorcze dane ze wszystkich podobnych spraw w całym kraju bądź na danym obszarze. Dzięki odpowiedniemu wsparciu statystycznemu możliwa będzie ocena, w jakim stopniu zdarzenia są ze sobą połączone, gdzie należy szukać sprawców bądź którego z podejrzanych należy przesłuchać jako pierwszego. Zaprezentowana metoda nie jest bezbłędna, jednak odpowiednio zastosowana może znacznie przyspieszyć poszukiwania sprawców przestępstw i zoptymalizować działania organów ścigania.

Streszczenie

Celem artykułu jest omówienie zagadnienia profilowania geograficznego, pokazanie zasad działania metody i jej podstaw. Wykorzystując analogię do gry z kostką, pokazano elementy teorii prawdopodobieństwa, która ma bezpośredni związek z użytecznością profilowania. Wskazano zarówno najważniejsze zalety, jak i największe trudności związane ze stosowaniem profili geograficznych. Przytoczono metody tworzenia profili i pokrótce omówiono ich skuteczność. Zwrócono uwagę na różnorodność zdarzeń, w których profilowanie geograficzne może być przydatne.

Słowa kluczowe: profilowanie geograficzne, profilowanie, *crime mapping*, rozkład prawdopodobieństwa, optymalizacja

Summary

The aim of this article was to describe geographic profiling, to show the principles of the method and its foundations. Using the dice game analogy elements of probability theory were discussed, which have a direct relationship with the utility of profiling. The main advantages and the greatest difficulties associated with the use of geographical profiles were shown. Methods of creating geographic profiles were described, and their accuracy and utility were compared based on previous research.

Keywords: geographic profiling, profiling, crime mapping, probability distribution, optimization

Kacper Gradoń

MOŻLIWOŚCI TAKTYCZNEGO WYKORZYSTANIA OTWARTYCH ŹRÓDEŁ INFORMACJI W INTERNECIE PRZEZ ORGANA ŚCIGANIA ORAZ SPRAWCÓW PRZESTĘPSTW I ZAMACHÓW TERRORYSTYCZNYCH

Opportunities for the tactical use of the Internet-based open-source information by the law-enforcement agencies, criminal offenders and terrorists

Pojęcie otwartych źródeł informacji ugruntowane jest w fachowej literaturze przedmiotu (kryminalistycznej, policyjnej, wojskowej, związanej z bezpieczeństwem wewnętrznym), a zakres znaczeniowy tego terminu (i jego synonimów, takich jak np. „biały wywiad" czy niejednokrotnie wykorzystywane w polskim piśmiennictwie anglojęzyczne określenie *Open Source Intelligence* – OSInt) nie budzi większych wątpliwości. Chociaż niniejsze opracowanie nie ma na celu zaprezentowania ewolucji pojęć ani historii rozwoju metod wywiadowczych, należy jednak przedstawić definicje terminu przyjęte na potrzeby dalszego wywodu. Korzystać zatem będę z przyjętej międzynarodowo siatki pojęciowej, w tym:

1. definicji NATO, według której biały wywiad (określany mianem „danych wywiadowczych ze źródeł jawnych/OSINT" – *open source intelligence/ renseignement de source ouverte*) to „dane wywiadowcze pochodzące zarówno z publicznie dostępnych informacji, jak i innych jawnych informacji o ograniczonym rozpowszechnianiu lub dostępie"[1];
2. definicji Armii Stanów Zjednoczonych, która konkretyzuje pojęcia „otwartego źródła" (definiowanego jako „osoba lub grupa osób dostarczająca informację i nieoczekująca zachowania jej prywatności") i „informacji dostępnej publicznie" (definiowanej jako „dane, fakty, instrukcje lub inne materiały opublikowane lub rozpowszechnione ogółowi społeczeństwa; dostępne na prośbę obywatela; legalnie zauważone lub usłyszane przez dowolnego przypadkowego obserwatora; udostępnione na spotkaniu otwartym dla ogółu społeczeństwa")[2].

[1] Słownik Terminów i Definicji NATO zawierający terminy wojskowe i ich definicje stosowane w NATO. AAP-6 (2014), s. 288, http://www.wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf.
[2] Open Source Intelligence ATP 2-22.9, Headquarters, Department of the Army. Army Techniques Publication FMI 2-22.9, Washington D.C. 10.07.2012, s. 1-1, http://www.fas.org/irp/doddir/army/atp2-22-9.pdf.

Warto podkreślić, że w polskiej literaturze dotyczącej tej tematyki (która notabene jest – w stosunku do zakresu zastosowań otwartych źródeł informacji – relatywnie skromna) przyjmuje się najczęściej polskojęzyczne warianty definicji zagranicznych lub pisze po prostu o „legalnym zdobywaniu informacji z przestrzeni publicznej"[3]. Co znamienne, również autorzy jedynej wydanej do tej pory w Polsce monografii poświęconej szeroko rozumianemu białemu wywiadowi unikają podawania własnej definicji problemu stanowiącego temat ich publikacji: pisząc o białym wywiadzie i *open source intelligence*, zaznaczają, że nie przyjęli jednej definicji tych terminów, a „był to zabieg celowy, aby pokazać różnorodność problemów i punktów widzenia na opisywane w pracy metody wykorzystywania otwartych źródeł informacji. (…) praca ma stanowić wstęp do dyskusji nad tymi metodami w praktyce podmiotów z sektora publicznego i prywatnego"[4].

W literaturze poświęconej klasyfikacji źródeł informacji o charakterze otwartym wymienia się najczęściej następujące lokalizacje danych:

1. media: gazety codzienne, periodyki, audycje radiowe i telewizyjne, media elektroniczne (Internet);
2. dane publiczne: raporty rządowe, dane oficjalne (budżety, dane demograficzne), wystąpienia oficjalne, debaty legislacyjne, konferencje prasowe, przemówienia;
3. źródła profesjonalne i akademickie: konferencje, sympozja, informacje korporacji zawodowych, artykuły naukowe, oświadczenia ekspertów[5].

Powyższa systematyka jest oczywiście uproszczona i można ją dowolnie rozwijać, tworząc dalsze podziały i podtypy. Przykładowo przyjęty w polskich źródłach podział wylicza:

1. media tradycyjne, w szczególności agencje prasowe, gazety, czasopisma, książki, radio (z zastrzeżeniem, że źródła te zawierają autorskie komentarze do danych w postaci wywiadów z ekspertami, analizy i śledztwa dziennikarskie);
2. Internet (media elektroniczne) – portale agencji informacyjnych, blogi, fora, portale społecznościowe, organizacje pozarządowe, think tanki i inne;
3. usługi komercyjne – informacje udostępniane przez prywatne podmioty trudniące się zbieraniem informacji;
4. inne usługi w zakresie dostarczania danych;
5. literaturę niszową – analizy, informacje z sektora akademickiego i organizacji pozarządowych, trudniejsze w dostępie ze względu na ograniczony zasięg i zakres;
6. opinie ekspertów, naukowców, uczestników zdarzeń;

[3] B. Sienkiewicz, *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego ABW. Wydanie specjalne" 2012, s. 52.

[4] W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, C.H. Beck, Warszawa 2012, s. 15.

[5] M.M. Lowenthal, *Intelligence. From Secrets to Policy*, fourth edition, CQ Press, Washington D.C. 2009, s. 103.

7. bazy zdjęć i obrazów (satelitarne obrazowanie powierzchni ziemi)[6].

Aktualnie, ze względu na dominującą we współczesnym świecie rolę mediów elektronicznych i nowoczesnych technologii informatycznych wykorzystujących bezpośrednio bądź pośrednio narzędzia internetowe lub z nimi powiązanych, coraz większą wagę zyskuje komponent internetowych źródeł informacji o charakterze białego wywiadu. Już przeszło dekadę temu podkreślano, że otwarte źródła internetowe są gwałtownie rosnącym obszarem zainteresowania instytucji wywiadowczych[7], a obecnie tendencja ta w wyraźny sposób zyskała na intensywności. Świadczy o tym m.in. potrzeba dalszych klasyfikacji usadowionych w strukturze Internetu źródeł danych. Jeszcze kilka lat temu wystarczające było uznanie „Internetu" za samoistną kategorię w szeregu otwartych źródeł informacji, jednak coraz częściej mamy do czynienia z tworzeniem bardziej szczegółowych typologii. Wymienia się zatem źródła takie jak:

1. serwisy informacyjne, portale, wortale;
2. blogi (dzienniki internetowe) – w tym pamiętniki internetowe, fotoblogi, wideoblogi, blogi muzyczne, blogi korporacyjne i organizacyjne, blogi tematyczne, mikroblogi;
3. fora internetowe i listy dyskusyjne;
4. otwarte serwisy chat i IRC;
5. serwisy społecznościowe;
6. inne rodzaje źródeł internetowych, w tym strony domowe, bazy danych, serwisy aukcyjne i z ogłoszeniami drobnymi, sieci wymiany plików i sieć głęboką[8].

Niektórzy autorzy rozbudowują katalog otwartych źródeł informacji dostępnych w Internecie, wymieniając ponad 20 podkategorii (internetowe wydania gazet i czasopism, blogi i mikroblogi, portale społecznościowe, grupy dyskusyjne, grupy informacyjne, komunikatory internetowe, serwisy typu Wiki, serwisy wideo, serwisy fotograficzne, strony internetowe organizacji pozarządowych, strony internetowe przedsiębiorców, rządowe strony internetowe, rządowe dokumenty udostępnione w ramach informacji publicznej, newslettery, reklamy internetowe, publikacje patentowe i aplikacje patentowe, rejestry domen WhoIs, internetowe stacje radiowe, telewizje internetowe, serwisy mapowe, serwisy zdjęć satelitarnych, serwisy zdjęć lotniczych)[9].

Warto zauważyć, że zaproponowane wyżej podziały nie mogą i nie powinny w żadnym razie stanowić katalogu zamkniętego – wraz z rozwojem technologii i w związku z powstaniem nowych narzędzi i usług internetowych bez wątpienia pojawią się nowe kategorie źródeł, dotychczas nieprzewidywane, a co najwyżej

[6] P. Chlebowicz, *Biały wywiad z perspektywy kryminalistyki*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 60.

[7] H. Fergusson, *Spy: A Handbook*, Bloomsbury Publishing, London 2004, s. 81.

[8] P. Maciołek, *Internet a OSINT – szanse i praktyczne zastosowania*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 225–230.

[9] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011, s. 62–63.

antycypowane w ramach analizy strategicznej trendów w budowie nowych aplikacji i platform. Jest to w gruncie rzeczy poważny problem, z którym dotychczas nie spotykaliśmy się w takiej skali i natężeniu. Obrazuje to już sam wzrost liczby urządzeń podłączonych do Internetu: w 1988 roku do sieci podłączonych było ok. sześćdziesięciu tysięcy urządzeń informatycznych (wśród nich nieliczne komputery osobiste)[10], natomiast w chwili obecnej[11] według danych firmy informatycznej CISCO na całym świecie podłączonych do Internetu jest ponad szesnaście miliardów osób, procesów logicznych i urządzeń – średnio co sekundę liczba ta rośnie o około 120 jednostek, a przewidywania CISCO mówią o ponad 50 miliardach jednoczesnych połączeń z Internetem w roku 2020. Ilustruje to licznik Cisco Connections Counter[12].

Najpopularniejsza obecnie sieć społecznościowa Facebook posiadała pod koniec pierwszego roku swojego istnienia (2004) około miliona użytkowników[13], natomiast w pierwszym kwartale 2015 roku Facebook miał już prawie półtora miliarda aktywnych użytkowników[14]. Podobny fenomen wzrostu zanotowała platforma mikroblogowa Twitter, która po pierwszym roku (2006) swojego funkcjonowania miała ok. 16 tysięcy użytkowników, a w pierwszym kwartale 2015 r. już ponad trzysta milionów[15]. Powstała w październiku 2010 r. sieć społecznościowa Instagram (obecnie własność korporacji Facebook), służąca przede wszystkim do publikowania i wymiany fotografii, miała pod koniec 2010 r. ok. miliona użytkowników, natomiast po czterech latach (grudzień 2014 r.) ich liczba wzrosła do ponad trzystu milionów[16].

Zilustrowana powyżej bezprecedensowa skala wzrostu, z jaką mamy do czynienia w przypadku Internetu i powiązanych z nim platform i technologii, niewątpliwie świadczy o tym, że w hierarchii otwartych źródeł informacji Internet zajmuje obecnie zdecydowane pierwsze miejsce, a trend ten nie wydaje się możliwy do zatrzymania czy odwrócenia (co najwyżej możemy się spodziewać jego spowolnienia). Fakt ten zauważają praktycy – funkcjonariusze organów ścigania i instytucji wywiadowczych.

Przeprowadzone przez W. Filipkowskiego na przełomie 2010 i 2011 roku badania dwóch grup funkcjonariuszy Policji nt. zagadnień związanych z białym wywiadem wykazały, że w owym czasie Internet (rozumiany jako źródło informacji w białym wywiadzie) wymieniany był (w zależności od grupy badanej) na drugim lub trzecim miejscu (po prasie i tzw. ogóle mediów) – wskazało go odpowiednio 21% i 17% respondentów. Pytania szczegółowe dotyczące przydatności informacji

[10] J. Zittrain, *The Future of the Internet and How to Stop It*, Penguin Books, 2009, s. 36.

[11] Tj. w czerwcu 2015 r. – uwaga ta jest istotna ze względu na tempo rozwoju infrastruktury sieciowej.

[12] http://blogs.cisco.com/news/cisco-connections-counter (dostęp 12.06.2015 r.).

[13] http://finance.yahoo.com/news/number-active-users-facebook-over-years--214600186--finance.html (dostęp 10.06.2015 r.).

[14] http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users--worldwide/ (dostęp 10.06.2015 r.).

[15] http://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/ (dostęp 10.06. 2015 r.).

[16] http://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/ (dostęp 10.06.2015 r.).

pozyskiwanych z Internetu przy wykonywaniu obowiązków służbowych spotkały się z dużym uznaniem respondentów (średnio ok. 88% odpowiedzi wskazywało na to, że takie informacje są „bardzo przydatne" lub „przydatne")[17]. W odniesieniu do działalności służb specjalnych monitorowanie i wyszukiwanie przez sieć internetową jest obecnie najpowszechniejszą metodą pozyskiwania przez Agencję Bezpieczeństwa Wewnętrznego jawnych źródeł i informacji[18].

W 2014 i 2015 roku przeprowadziliśmy (K. Gradoń i A. Gutkowska) wywiady i badania ankietowe związane ze zwalczaniem ekstremizmu i terroryzmu tzw. „samotnych wilków" w ramach realizowanego przez nas projektu Siódmego Programu Ramowego Komisji Europejskiej FP7 PRIME[19]. Jednym z aspektów naszych badań było zdiagnozowanie, czy informacje z białego wywiadu, ze szczególnym uwzględnieniem źródeł internetowych, stanowią istotne narzędzie pracy instytucji odpowiedzialnych za zwalczanie przedmiotowych zagrożeń. Badania przeprowadziliśmy m.in. wśród przedstawicieli polskiej Policji, Straży Granicznej i Agencji Bezpieczeństwa Wewnętrznego, policji brytyjskiej, amerykańskiej (NYPD), hiszpańskiej oraz przedstawicieli EUROPOL-u. Dodatkowo samodzielnie przeprowadziłem podobne badania na grupie 80 policjantów indyjskich (w stopniu nie niższym od pułkownika)[20]. Aktualnie kompleksowe wyniki badań poddawane są szczegółowej analizie, jednak warto zaznaczyć, że jeśli chodzi o aspekt istotności internetowych źródeł otwartych w pracy funkcjonariuszy organów ścigania, praktycznie wszyscy respondenci (97,5%) wymieniali Internet jako kluczowe miejsce pozyskiwania informacji (wśród źródeł otwartych).

Bezpośrednim dowodem na zainteresowanie organów ścigania wykorzystywaniem metod białego wywiadu w Internecie jest ogłoszenie przez Federalne Biuro Śledcze (FBI) „zapytania o informację" (*Request for Information*) dotyczącego możliwości stworzenia i dostarczenia platformy informatycznej służącej do wyszukiwania, mapowania i analizy informacji ze źródeł otwartych[21]. Dokument omawiający szczegóły takiego narzędzia (które miałoby stanowić wsparcie dla FBI SIOC – Strategic Information and Operations Center) wymienia zastosowania operacyjne i analityczne

[17] Szczegółowy opis badań wraz z analizą: W Filipkowski, *Wykorzystanie otwartych źródeł informacji. Wyniki badań ankietowych*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 135–162.

[18] B. Święczkowski, *Wykorzystanie tzw. białego wywiadu w działalności analityczno-informacyjnej Agencji Bezpieczeństwa Wewnętrznego*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 174.

[19] PRIME: Preventing, Interdicting and Mitigating Extremism: Defending Against Lone Actor Extremist Events. EC Grant Agreement n. 608354 (PRIME) FP7-SEC-2013-1.

[20] Badania przeprowadzone w dniach 27 kwietnia – 1 maja 2015 r. w SVP National Police Academy, Hajdarabad, Indie, w ramach szkolenia Mid-Career Training Programme Phase-IV „Strategy, Innovation and Management".

[21] https://www.fbo.gov/index?s=opportunity&mode=form&id=c65777356334dab8685984fa74bfd636&tab=core&_cview=1 (dostęp 10.01.2015 r.).

wymagane przez SIOC, wyliczając *explicite* monitorowanie środowisk Twitter, Facebook i MySpace[22].

Biorąc pod uwagę powyższe obserwacje, trzeba się zastanowić nad umiejscowieniem białego wywiadu w nauce kryminalistyki. Ponieważ ze względu na wykształcenie i doświadczenie zawodowe adresatów „Problemów Współczesnej Kryminalistyki" nie ma potrzeby przeprowadzenia wykładu z zakresu dziedzin i funkcji tej dyscypliny naukowej, wystarczy powiedzieć, że w aktualnej polskiej rzeczywistości prawnej wykorzystanie przez Policję i inne instytucje odpowiedzialne za zapobieganie przestępczości i jej zwalczanie metod i technik białego wywiadu to domena taktyki kryminalistycznej, realizującej jej funkcję rozpoznawczą. Warto podkreślić, że taka konstatacja znajduje poparcie środowiska naukowego (identyczna obserwacja P. Chlebowicza: „biały wywiad należałoby lokować w obszarze taktyki kryminalistycznej, przy czym jego zastosowanie odnosiłoby się przede wszystkim do realizacji funkcji rozpoznawczej"[23]). Jak pisze E. Gruza, funkcja rozpoznawcza kryminalistyki „realizowana jest przez opracowywanie metod i środków służących do uzyskiwania możliwie największej liczby informacji o miejscach, przedmiotach, osobach, taktyce aktualnych i przyszłych działań kryminalistycznych"[24]. Kluczowe jest tu pojęcie informacji, której rola w dziedzinie całej kryminalistyki – jak zauważa T. Hanausek – jest ogromna; autor ten podkreśla również stymulacyjną funkcję informacji, pisząc, że „każda informacja nie tylko przenosi cechy poznawanego przedmiotu do świadomości poznającego podmiotu, ale z reguły jest także stymulatorem działań podejmowanych przez ten podmiot w związku z jej treścią. W takich przypadkach informacja staje się także czynnikiem kształtującym treści, zakres oraz kierunek tych działań"[25]. Te obserwacje okażą się istotne w dalszej części niniejszego wywodu, przy prezentacji zakresu możliwości wykorzystania otwartych źródeł informacji – zarówno przez organa ścigania, jak i przestępców i terrorystów.

Ponieważ pojawiają się niekiedy zastrzeżenia, czy praca na otwartych źródłach informacji nie powinna być uznawana za jedną z form czynności operacyjno-rozpoznawczych, warto zwrócić uwagę na stanowisko wyrażone przez J.D. Pogorzelskiego, który w swojej analizie białego wywiadu w pracy prokuratora stwierdza, że „pozyskiwanie i analiza informacji z otwartych źródeł nie stanowią czynności operacyjno-rozpoznawczych"[26]. Pewne wątpliwości w odniesieniu do uznania metod białego wywiadu w pracy Policji za czynności operacyjno-rozpoznawcze ma W. Mą-

[22] https://www.fbo.gov/utils/view?id=7f9abf0ff0fdba171d1130ddf412aea3 (dostęp 10.01.2015 r.).

[23] P. Chlebowicz, *Biały wywiad z perspektywy kryminalistyki*, op. cit., s. 61.

[24] E. Gruza, *Historia, przedmiot i zadania kryminalistyki*, w: E. Gruza, M. Goc, J. Moszczyński (red.), *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 22.

[25] T. Hanausek, *Zarys taktyki kryminalistycznej*, Dom Wydawniczy ABC, Warszawa 1994, s. 71.

[26] J.D. Pogorzelski, *Wykorzystanie otwartych źródeł informacji w pracy prokuratora*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 186.

drzejowski, który podaje, że o ewentualnym uznaniu pracy na źródłach otwartych za czynności operacyjno-rozpoznawcze można byłoby mówić w kontekście form pozyskiwania tychże danych; zwraca uwagę na to, że „podstawowe znaczenie ma w tym wypadku kwestia jawności działań policyjnych”[27] – należy zatem rozumieć, że informacyjna czy rozpoznawcza rola białego wywiadu niekoniecznie musi przekładać się na „niejawność” czynności, a dopiero pewne szczególne warunki prowadzenia pracy na źródłach otwartych (np. kamuflowana penetracja, zastosowanie podstępu, użycie specjalistycznego oprogramowania) mogłyby sprawić, że konkretne formy wykorzystania źródeł OSInt zostałyby uznane za czynności operacyjno-rozpoznawcze. Również z perspektywy Agencji Bezpieczeństwa Wewnętrznego problematyka prowadzenia działań w oparciu o informacje ze źródeł otwartych może być postrzegana nie jako czynność operacyjno-rozpoznawcza, ale analityczno-informacyjna[28].

Powyższe omówienie posłużyć ma jako przyczynek do rozważań na temat możliwości wykorzystania otwartych źródeł informacji pochodzących z Internetu i powiązanych z siecią nowoczesnych technologii przez organa ścigania i służby wywiadowcze oraz przez sprawców przestępstw i zamachów terrorystycznych. W mojej opinii Internet staje się „polem bitwy”[29], na którym obie strony konfliktu walczą o dominację. Odchodzę przy tym od tradycyjnego pojmowania cyberprzestępczości (która w powszechnym odbiorze dotyczy zdarzeń „dziejących się” w świecie cyfrowym) na rzecz podejścia, w którym Internet jest narzędziem dokonywania przestępstw, do jakich dochodzi w świecie rzeczywistym. Ze względu na zobrazowane wyżej trendy w rozwoju samej sieci Internetu, stały wzrost liczby użytkowników, a także pojawiających się regularnie nowych aplikacji i narzędzi, będziemy bowiem zauważać dalszy wzrost skali przestępczości, w której nowe technologie wykorzystywane będą nie tylko do dokonywania czynów zabronionych w świecie wirtualnym, ale także – a z czasem: przede wszystkim – w świecie realnym. Wynika to z kilku przyczyn[30]:

1. nowoczesne technologie i Internet umożliwiają użytkownikom bezprecedensowo łatwy i szeroki dostęp do informacji i kontaktów;
2. narzędzia informatyczne dostępnie obecnie w obrocie internetowym są łatwe w użyciu, a ich wykorzystanie nie wymaga od użytkowników posiadania specjalistycznej wiedzy fachowej (lub daje możliwość skorzystania z pomocy łatwych do zrozumienia instrukcji – w tym poradników wideo pokazujących algorytmy postępowania);
3. zarówno sam Internet, jak i powiązane z nim technologie są łatwo dostępne, a jednocześnie bardzo tanie (niekiedy darmowe);

[27] W. Mądrzejowski, *Biały wywiad w Policji*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 126.

[28] Por. B. Święczkowski, op. cit., s. 165–167.

[29] K. Gradoń, *Crime science and the battlefield of the Internet. Securing the analog world from the digital crime*, „IEEE Security & Privacy Magazine”, 2013, Vol. 11 Issue No. 5 (September-October) 2013, s. 93–96.

[30] K. Gradoń, *Internet Crime*, w: M.E. Beare (red.), *Encyclopedia of Transnational Crime & Justice*, SAGE, Thousand Oaks 2012, s. 212.

4. narzędziami tego rodzaju można się posługiwać (przy minimum wiedzy fachowej) z zachowaniem relatywnie wysokiego poziomu anonimowości.

Najważniejszą jednak przyczyną, dla której twierdzę, że obserwując fenomen z perspektywy analizy strategicznej, można zakładać z ogromną dozą pewności, iż w nieodległej przyszłości zaobserwujemy przeniesienie się zauważalnej części działalności przestępczej i terrorystycznej do Internetu, są przemiany pokoleniowe. Osoby urodzone po 1980 roku nazywane były już kilka lat temu „generacją sieci”[31], jednak w owym czasie odnoszono się przede wszystkim do działalności społecznej, ekonomicznej czy kulturalnej, która w coraz większym stopniu przenosiła się do przestrzeni wirtualnej. Moim zdaniem te same problemy muszą przekładać się na przestępczość, zatem z im młodszym pokoleniem sprawców (bądź: potencjalnych sprawców) będziemy mieć do czynienia, tym większe prawdopodobieństwo tego, że Internet będzie głównym i oczywistym elementem ich „środowiska naturalnego”[32].

Celem niniejszego opracowania nie jest diagnoza socjodemograficzna czy pedagogiczna, jednak jeśli się przyjmie założenie, że obecnie Internet jest jednym z najważniejszych lub głównym miejscem zdobywania informacji[33], to oczywiste się staje, że już niedługo będziemy mieć do czynienia z pokoleniem przyzwyczajonym od najwcześniejszych lat życia (i edukacji) do intensywnego korzystania z mediów elektronicznych oraz zdobywania większości swej wiedzy i informacji w sieci. Przedstawiciele tego pokolenia, którzy na pewnym etapie rozwoju zdecydują się na zaangażowanie w działalność przestępczą, będą traktować Internet jako narzucające się narzędzie „pierwszego wyboru”, służące początkowo do zdobywania know-how, a w dalszej kolejności do przygotowania i przeprowadzenia zamierzonego i zaplanowanego przestępstwa[34]. Wynika to wprost z wymienionych wyżej przyczyn (dostęp do informacji i kontaktów, łatwość wykorzystania narzędzi, bardzo wysoka dostępność, niskie koszty, relatywnie wysoka anonimowość) i sprawia, że Internet staje się dla aktywnych bądź potencjalnych sprawców ekwiwalentem „wielofunkcyjnego noża”, łatwego w obsłudze i pomocnego w osiąganiu szerokiego spektrum zakładanych celów.

Już na początku XXI wieku zauważono, że „cyberprzestrzeń pozwala obecnie na wiele takich samych działań jak główna ulica miasta. Możemy angażować się tam w cyberzakupy, cyberrandki i cyberkształcenie. Jednakże tak jak i na głównej ulicy miasta mamy tam również do czynienia z mroczną stroną: cyberkradzieżami, cyberoszustwami i cyberniszczeniem”[35]. Przez kolejne kilkanaście lat problem ten

[31] *The net generation, unplugged*, „The Economist”, 4 marca 2010 r., http://www.economist.com/node/15582279 (dostęp: 6.07.2014).

[32] K. Gradoń, *Internet as a new criminal battleground? An essay on the future trends in crime*, „Przegląd Naukowy Disputatio” 2011, t. XII, s. 153.

[33] Por. np. M. Szpunar, *Internet – medium informacji versus dezinformacji*, „E-mentor. Dwumiesięcznik Szkoły Głównej Handlowej w Warszawie” 2007, nr 2, s. 46–51.

[34] K. Gradoń, *Internet as a new criminal battleground?...*, op. cit., s. 153.

[35] D.C. Kennedy, *In search of a balance between police power and privacy in the Cybercrime Treaty*, „Richmond Journal of Law and Technology” 2002, No. 9, s. 58.

w sposób wyraźny zyskał na znaczeniu i intensywności, a możliwości, jakie daje sprawcom przestępstw współczesna technologia, są nieporównywalnie większe od potencjału oferowanego przez sieć nieco ponad dekadę temu. Wiąże się to nie tylko z samym rozwojem techniki, ale także z pojawieniem się w latach 2001–2002 nowego fenomenu znanego pod nazwą „Web 2.0" (sieć drugiej generacji) – czyli platform i serwisów, których zawartość tworzona jest przez samych użytkowników (a nie jedynie transmitowana do nich przez jednostki zewnętrzne: administratorów stron czy redakcje mediów elektronicznych)[36]. Właśnie takie serwisy – czyli przede wszystkim media społecznościowe – stanowią obecnie główne otwarte źródło informacji.

Nick Ross, współzałożyciel i fundator Jill Dando Institute of Crime Science w University College London, jednostki przekładającej wyniki multidyscyplinarnych i empirycznych badań naukowych na praktyczne strategie kontroli i zwalczania przestępczości (nowa dyscyplina pod nazwą *Crime Science*[37]), odnosząc się do przyszłych trendów w przestępczości, pisze w alarmistycznym tonie: „Internet to miejsce, w którym w przyszłości przeprowadzane będą jedne z najstraszniejszych zbrodni. Jeśli trend (który obserwujemy) będzie dalej iść w tym kierunku, cyberprzestępczość prawdopodobnie stanie się jednym z największych zagrożeń, pomijając zarazy i wojnę atomową"[38]. Taka opinia może wydawać się nieco przesadzona, jednak jak postaram się poniżej wykazać, ryzyko zdominowania przestępczego krajobrazu przez zdarzenia powiązane w pewnym stopniu z cyberprzestrzenią i nowymi technologiami jest wysokie.

Jednym z pierwszych powszechnie znanych przykładów możliwości, jakie dają potencjalnym przestępcom pochodzące z Internetu dane jawnoźródłowe, było wielokrotne zabójstwo, którego dopuścili się w 1999 roku w liceum Columbine High School w stanie Kolorado dwaj nastolatkowie – Eric Harris i Dylan Klebold. Rozwój Internetu był w tamtych czasach na nieporównywalnie niższym – w stosunku do dzisiejszego – poziomie, jednak obaj sprawcy korzystali z dostępnych im narzędzi, zdobywając dzięki nim instrukcje budowy improwizowanych materiałów wybuchowych[39] (dostępna w sieci w formie edytowalnego pliku tekstowego tzw. „Anarchistyczna książka kucharska" i podręcznik armii amerykańskiej *TM 31-210 Improvised Munitions Handbook*), ucząc się taktyki działania oddziałów specjalnych i metod komunikacji w sytuacji frontowej (również dostępny w sieci – w formie pliku tekstowego – podręcznik Armii Stanów Zjednoczonych *US Marine Corps Jungle & Urban Warfare Manual*), jak również zapoznając się ze schematami działania służb policyjnych, ratowniczych i medycznych (oryginalnym zamiarem sprawców

[36] Por. np. T. O'Reilly, *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, 09.30.2005, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (dostęp 8.12.2014 r.).

[37] por. http://www.ucl.ac.uk/scs.

[38] N. Ross, *Crime – How to Solve It and Why So Much of What We're Told is Wrong*, Biteback Publishing, London 2013, s. 295–296.

[39] K. Gradoń, *Zabójstwo wielokrotne. Profilowanie kryminalne*, Lex Wolters Kluwer, Warszawa 2010, s. 29–35.

było spowodowanie w szkole potężnej eksplozji obliczonej na zabicie kilkuset ofiar, egzekucja osób, którym udałoby się wydostać z ruin, i wreszcie samobójstwo. Kilkadziesiąt minut później miało dojść do detonacji bomb ukrytych w samochodach zaparkowanych przy szkole, co w zamiarze zamachowców spowodowałoby śmierć kolejnych osób, które pojawiłyby się na miejscu tragedii. Plan nie powiódł się ze względu na usterki zapalników czasowych w ładunkach wybuchowych, wobec czego sprawcy wkroczyli do budynku szkoły i otworzyli ogień do uczniów i nauczycieli. Charakterystycznym elementem działania przestępców było w tym przypadku ogłaszanie w Internecie informacji wyprzedzających na temat planowanego zamachu.

Podobny schemat działania[40], rozwinięty tylko o możliwości, jakie daje Web 2.0 (czyli przede wszystkim portale społecznościowe), możemy zaobserwować również w innych atakach tego rodzaju – np. zabójstwie dokonanym w 2006 r. przez Kimveera Gilla w Dawson College w Montrealu, ataku Seung-Hui Cho na Politechnikę Stanu Virginia (2007 rok, 32 ofiary śmiertelne) czy masakrze w fińskim liceum Jokela (atak Pekki-Erica Auvinena w 2007 roku, 10 ofiar śmiertelnych). Sprawcy tych zbrodni nie tylko ogłaszali swoje plany w Internecie, ale także radykalizowali się i szkolili za pomocą dostępnych tam źródeł.

Również sprawca ataku w Oslo i na wyspie Utoya, Anders Breivik, był aktywnym użytkownikiem Internetu, a przygotowana przez niego i dokonana w 2011 roku zbrodnia została w znacznym stopniu opracowana w szczegółach właśnie dzięki otwartym źródłom informacji. Breivik nie tylko radykalizował się za pośrednictwem sieci, ale również planował zamach, uczył się technik działania i zdobywał niezbędne mu umiejętności przy użyciu metod, które moglibyśmy nazwać białym wywiadem[41].

Problem radykalizacji za pomocą Internetu traktowanego jako otwarte źródło informacji to bardzo poważny i skrajnie niebezpieczny fenomen, szczególnie istotny w ostatnich latach, kiedy to regularnie stykamy się z doniesieniami na temat szerzenia ideologii ekstremistycznej właśnie za pośrednictwem nowoczesnych technologii. Niektórzy autorzy posuwają się nawet do określania Internetu mianem „bodźca gniewu" (*rage enabler*)[42] dla podatnych na ekstremistyczne wpływy jednostek. Problematyka „radykalizacji on-line" jest zbyt szeroka, by ująć ją w niniejszym artykule, jednak warto wymienić przynajmniej publikatory takie jak wydawany przez organizację terrorystyczną Al-Kaida w formie elektronicznej magazyn „Inspire", którego głównym celem jest szerzenie ideologii islamskiego dżihadu, a także zachęcanie i szkolenie potencjalnych zamachowców oraz legitymizacja ataków[43]. Fenomen ten nabiera szczególnego znaczenia w obliczu zagrożenia kampanią salafickiej organizacji terrorystycznej Państwo Islamskie (ISIS), która wykorzystuje Internet i media

[40] Tamże.

[41] R. Pantucci, *What have we learned about lone wolves from Anders Behring Breivik?*, „Perspectives on Terrorism" 2011, Vol. 5, No. 5–6, s. 27–41.

[42] B. Forst, *Terrorism, Crime and Public Policy*, Cambridge University Press, New York, 2009, s. 190.

[43] http://www.foxnews.com/world/2010/07/01/make-bomb-kitchen-mom-featured-al-qaedas-st-english-magazine/ (dostęp 10.02.2015 r.).

społecznościowe jako jedno ze swoich podstawowych narzędzi zarówno białego wywiadu, jak i propagandy[44]. Kompleksową analizę tej formy wykorzystania Internetu przez terrorystów zawiera raport korporacji RAND pt. *Radicalisation in the Digital Era*[45].

Jak ustalono wcześniej, z perspektywy instytucji zaangażowanych w zwalczanie przestępczości kryminalnej i samych przestępców otwarte i powszechnie dostępne dane znajdujące się w Internecie (ze szczególnym uwzględnieniem sieci i portali społecznościowych) stanowią niezwykle wartościowe źródło informacji. W tym miejscu należy się więc skoncentrować na opisie wybranych możliwości, jakie oferują pod tym względem nowoczesne technologie. Starając się zachować przejrzystość wywodu, zaprezentujemy wyliczone poniżej narzędzia i techniki z punktu widzenia potencjału ich wykorzystania przez przestępców. Przyczyną takiego ujęcia tematu jest fakt, że populacja osób prywatnych, które nie są zaangażowane w działalność przestępczą (ewentualnych ofiar przestępstw) i do których danych osobowych sprawcy mają obecnie nieograniczony dostęp, jest znacząco większa niż populacja sprawców. Kieruję się zatem postulatem zasygnalizowania zagrożeń i wpłynięcia w ten sposób na zwiększenie ich świadomości, a jednocześnie realizację założeń prewencyjnej funkcji kryminalistyki, co w konsekwencji powinno się przekładać na podniesienie bezpieczeństwa. Oczywiście te same metody i techniki uzyskiwania i wykorzystywania danych pochodzących ze źródeł otwartych mogą być stosowane na poziomie analitycznym i operacyjnym przez instytucje i służby odpowiedzialne za zwalczanie przestępczości i jej zapobieganie.

Dostępne w niekontrolowany sposób dane dotyczące osób i miejsc mogą być wykorzystywane przez sprawców do typowania, wyboru i monitoringu celów ataku. Pomagają m.in. w ustaleniu, czy cel (ofiara) należy do kategorii niskiego, czy wysokiego ryzyka. Opierając się na dostępnych danych, sprawca może analizować wiek, zawód, styl życia, budowę ciała, kondycję fizyczną, możliwości samoobrony i okolicę, w której ofiara mieszka lub przebywa. W związku z tym wyróżnia się tzw. ofiary wysokiego ryzyka, przebywające w okolicach, w których są bardziej bezbronne (np. pętle autobusowe, odosobnione miejsca, parki, lasy, tereny otwarte lub okolice o dużym nasyceniu prostytucją), i sprawiające wrażenie łatwiejszego celu ataku (np. osoby bardzo młode lub w podeszłym wieku), oraz tzw. ofiary niskiego ryzyka, których zawód i styl życia sprawiają, że najczęściej nie stają się ofiarami przestępstw z użyciem przemocy (m.in. ze względu na okolice, w których mieszkają, pracują lub spędzają wolny czas)[46]. Na tej samej zasadzie sprawca może oceniać „opłacalność" ataku na konkretną osobę lub miejsce – bazując na źródłach otwartych, może

[44] http://www.geopoliticalmonitor.com/islamic-state-online-jihadist-propaganda-2-0/ (dostęp 8.03.2015 r.).

[45] I. von Behr, A. Reding, C. Edwards, L. Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, RAND Corporation, Santa Monica, CA, 2013.

[46] Jest to bezpośrednie przełożenie metod wykorzystywanych w profilowaniu kryminalnym. Por. K. Gradoń, *Zabójstwo wielokrotne*..., op. cit., s. 169.

rozpoznać stopień zamożności ofiary albo ocenić wartość konkretnych składników jej majątku.

Już podstawowe wyszukiwania w sieci pozwalają przeciętnemu użytkownikowi Internetu (a więc również sprawcom przestępstw) na poznanie danych osobowych ofiary. Umiejętność kojarzenia zespołów danych pochodzących z różnych stron i portali internetowych umożliwia stworzenie bardzo kompletnego dossier konkretnej osoby. Generalną zasadą jest, że intensywność aktywności sieciowej rozumianej jako udzielanie się czy obecność w różnych serwisach, portalach, forach dyskusyjnych i platformach społecznościowych jest wprost proporcjonalna do stopnia niekontrolowanego wycieku danych i potencjalnego zagrożenia dla osoby, której taka działalność jest udziałem. Brzmi to jak truizm, jednak większość użytkowników Internetu nie zdaje sobie z tego sprawy lub nie dopuszcza do świadomości ewentualnego ryzyka, na jakie się narażają. Przykładowo w ramach eksperymentów związanych z prowadzonymi badaniami przeprowadziłem testy penetracyjne dotyczące kilku osób (za ich zgodą), co do których wiedziałem, że są regularnymi użytkownikami Internetu. Dla celów badawczych celowo wytypowałem osoby, które nie używają serwisów mikroblogowych (Twitter) ani nie prowadzą blogów (natura tych platform sprawia, że autorzy publikowanych tam wpisów czy komentarzy częściej dzielą się z czytelnikami swoimi informacjami osobistymi). Skojarzenie danych pochodzących z kilku stron i portali społecznościowych (popularne Facebook i LinkedIn, nieco mniej powszechne Goldenline, ciesząca się niegdyś dużym uznaniem Nasza-Klasa, a także proste wyszukiwania za pomocą wyszukiwarki Google) pozwoliły mi na zebranie kompletów danych, wśród których znajdowały się imiona i nazwiska (w tym nazwiska panieńskie), daty urodzenia, aktualne i poprzednie adresy, kompletne informacje o wykształceniu na wszystkich szczeblach edukacji, adresy e-mail, numery telefonów prywatnych i służbowych, imiona i nazwiska osób bliskich (w tym nazwiska panieńskie), szczegółowe informacje o dzieciach, dane zawodowe dotyczące aktualnych i poprzednich miejsc zatrudnienia, informacje o hobby, zainteresowaniach, sposobach i miejscach spędzania wolnego czasu, regularnym planie dnia, informacje pozwalające na postawienie realistycznych założeń na temat statusu majątkowego oraz obfite zbiory fotografii „oficjalnych" i prywatnych, w tym fotografie spełniające warunki przewidziane dla zdjęć biometrycznych (w czego potwierdzeniu pomaga np. dostępne on-line narzędzie Photo Tool[47] wykorzystywane przez Departament Stanu USA przy internetowym systemie wniosków wizowych). Za zgodą dwóch wyselekcjonowanych osób przeprowadziłem na podstawie zebranych danych dalsze testy bezpieczeństwa dotyczące możliwości złamania zabezpieczeń należącej do nich poczty elektronicznej. Większość dostawców serwisów poczty e-mail oferuje swoim użytkownikom opcje pytań zabezpieczających wykorzystywanych do odzyskiwania haseł w przypadku ich zapomnienia. Najczęściej pytania zabezpieczające dostępne są z rozwijanego menu i z reguły są one zaproponowane użytkownikowi (większość serwisów pozwala co prawda na tworzenie własnych, jednak przeważająca grupa

[47] http://travel.state.gov/content/visas/english/general/photos.html (dostęp 15.03.2015 r.).

osób wybiera sugerowane pytania z przedstawionej im listy[48]). „Złamanie" pytań zabezpieczających ograniczyło się w obu przypadkach do udzielenia poprawnej odpowiedzi na te pytania, te zaś można było błyskawicznie znaleźć w wymienionych wyżej serwisach społecznościowych (pytania w rodzaju: „nazwisko panieńskie matki", „imię psa", „patron pierwszej szkoły", „nazwisko pierwszego nauczyciela"). Reset hasła do skrzynki e-mail pozwalał na zapoznanie się z jej zawartością, w tym odnalezienie elektronicznych wyciągów bankowych z pełnymi informacjami o rachunku, jak również faktur zawierających numery NIP i dane innych kont bankowych powiązanych z użytkownikiem.

Potencjał ustalania danych osobowych w Internecie jest ogromny, a wielu użytkowników, w całkowitej nieświadomości zagrożenia, udostępnia jeszcze bardziej precyzyjnie je identyfikujące materiały. Przykładowo wspomniany wyżej fotograficzny serwis społecznościowy Instagram umożliwia swoim użytkownikom umieszczanie zdjęć, które opisywane są przy użyciu słów kluczowych (tzw. hashtagów). Niektórzy użytkownicy zamieszczają w tym serwisie fotografie swoich dowodów osobistych, praw jazdy, paszportów, kart płatniczych, mandatów karnych (!), aktów notarialnych, rachunków itp. Ponieważ zamieszczone tam zdjęcia opisywane są słowami kluczowymi, ich znalezienie nie przedstawia większego problemu. Fenomen ten opisany został w grudniu 2013 r. przez serwis Niebezpiecznik.pl, który zwrócił uwagę na możliwość wykorzystania innej aplikacji (zwanej wówczas Statigram) do przeszukiwania zasobów Instagramu po słowach kluczowych[49]. Obecnie Statigram został zastąpiony nowocześniejszą wyszukiwarką Iconsquare[50], dzięki której można prowadzić efektywne wyszukiwania hashtagów Instagramu. Proste ćwiczenie (sprowadzające się wyłącznie do wymyślania „kreatywnych" słów kluczowych powiązanych z danymi osobowymi – w języku polskim i angielskim) umożliwia błyskawiczny dostęp do znacznej liczby dokumentów zawierających dane wrażliwe (niejednokrotnie ich komplety; szczególnie kuriozalny przykład to przypadek osoby, która zamieściła w serwisie Instagram fotografie awersów i rewersów swojego dowodu osobistego, prawa jazdy i karty debetowej).

Tworzenie profilu czy dossier ofiary przy użyciu otwartych źródeł informacji pozwalać może na dotarcie do informacji wrażliwych, w tym danych medycznych i szczegółów związanych ze stanem zdrowia i kondycją fizyczną. Wielu użytkowników Internetu poszukuje wstępnych porad medycznych w przestrzeni wirtualnej, a pięć z dwudziestu największych grup dyskusyjnych poświęconych takim poradom zrzesza (w Polsce) od 1 do 2,2 miliona użytkowników. Łącznie ze wszystkich grup dyskusyjnych korzysta w naszym kraju ponad 7 milionów unikalnych użytkowników[51]. Natura rozmów prowadzonych na tego typu forach i w grupach dyskusyj-

[48] http://time.com/3892793/security-questions-answer/ (dostęp 3.06.2015 r.).

[49] http://niebezpiecznik.pl/post/instagram-pelen-zdjec-dowodow-praw-jazdy-i-kart-platniczych-polakow/ (dostęp 7.05.2014 r.).

[50] http://iconosquare.com.

[51] Raport *Pacjenci w sieci* przygotowany przez Procontent Communication, Warszawa, styczeń 2012. Dostęp: http://pliki.gemius.pl/Raporty/2012/Raport_Pacjenci_w_sieci_20121.pdf.

nych sprawia, że większość uczestników posługuje się tam pseudonimami (nickami) i teoretycznie unika ujawniania swojej tożsamości. Proste przeszukanie podobnych list dyskusyjnych wskazuje jednak na to, że stosunkowo częstym zjawiskiem jest rejestrowanie się użytkowników przy użyciu adresu e-mail (niekiedy podawany przez uczestników w celu kontynuacji dyskusji na konkretny temat poza forum), ten zaś z kolei pozwala na znalezienie innych miejsc w sieci, w których dana osoba rejestrowała się przy użyciu tego samego adresu, ale już pod swoim prawdziwym imieniem i nazwiskiem. Testowy przegląd kilku medycznych grup dyskusyjnych umożliwił mi znalezienie w specjalistycznych wątkach znacznie bardziej szczegółowych informacji zdrowotnych – w tym skanów z epikryz szpitalnych, kopii wyników analiz lekarskich i badań obrazowych – w tych przypadkach udostępniający dokumenty (najprawdopodobniej ich właściciele) nie zadbali o usunięcie wyjątkowo wrażliwych danych (zarówno identyfikacyjnych, jak i ściśle osobistych, dotyczących stanu zdrowia).

Wyszukiwanie po pseudonimach/nickach, adresach e-mail lub adresach IP umożliwia osobom ukierunkowanym na zbieranie danych ze źródeł otwartych dotarcie do specyficznych informacji, które niejednokrotnie mogą być uznane za dane wrażliwe (w tym kompromitujące lub wstydliwe). Jeżeli osoba używa charakterystycznego pseudonimu (do którego jest przyzwyczajona, przywiązana), to jest możliwe, że korzysta z niego w różnych sytuacjach, tj. np. w kilku niepowiązanych ze sobą miejscach sieci. Podobny mechanizm dotyczy wykorzystywania adresów poczty elektronicznej. Takie postępowanie jest naturalną i pragmatyczną, ukierunkowaną na własną wygodę postawą, właściwą większości ludzi[52]. Znając charakterystyczny nick czy adres e-mail interesującej nas osoby, możemy spróbować znaleźć ślady jej działania na różnych stronach w Internecie, docierając niekiedy do treści, których taka osoba wolałaby nie podpisywać własnym nazwiskiem, w trosce o swoje dobre imię lub pod wpływem innych przyczyn motywacyjnych. Rzecz jasna, nie można być wówczas pewnym tożsamości autora takich treści (bazując na samym pseudonimie), jednak ocena psycholingwistyczna publikowanych treści (tj. „szczegółowa analiza pisemnej (…) wypowiedzi ich autora, zarówno od strony formy wypowiedzi, sposobu (…) pisania, jak i zawartości – treści, składni gramatycznej, częstotliwości używania określonych słów, stosowanych zwrotów i idiomów, popełnionych błędów językowych i ortograficznych”[53]) może w znacznym stopniu uprawdopodobnić hipotezę dotyczącą osoby autora i rozszerzyć naszą wiedzę na jego temat o nietypowe czy trudne do zdobycia w inny sposób informacje. Warto zauważyć, że w ten sam sposób możemy dotrzeć do profilu interesującej nas osoby w serwisach dotyczących np. recenzji wystaw, koncertów, przedstawień, filmów, restauracji czy hoteli (dzięki czemu można rozbudować „dossier” o informacje o gustach czy możliwościach finansowych i sposobach spędzania wolnego czasu) oraz do profili w serwisach aukcyjnych (takich jak eBay czy Allegro), co może pozwolić na prześledzenie historii

[52] Por. koncepcja „rachunku szczęśliwości” (*Felicific Calculus*) sformułowana przez Jeremy’ego Benthama.

[53] E. Gruza, *Wybrane działania rozpoznawczo-wykrywcze*, w: E. Gruza, M. Goc, J. Moszczyński (red.), op. cit., s. 56.

zakupów i sprzedaży i dotarcie do bardzo specyficznych szczegółów składających się na profil socjoekonomiczny danego człowieka[54].

Kolejnym problemem, który wiąże się z tematyką białego wywiadu w Internecie, jest kwestia uzyskiwania danych o geolokalizacji użytkownika. Poza rozwiązaniami niemieszczącymi się w pojęciu źródeł otwartych (zazwyczaj też nielegalnymi i często wymagającymi specjalnych umiejętności od użytkownika, czyli np. zarażenia telefonu komórkowego ofiary za pomocą złośliwego oprogramowania), aktualne rozwiązania oferowane przez Internet i powiązane z nim nowoczesne technologie pozwalają na posłużenie się oficjalnie dostępnymi i jawnymi narzędziami do zdobycia precyzyjnych informacji na temat fizycznej przestrzeni, w której znajduje się cel ataku (osoba lub miejsce).

Najprostszą metodą jest odczytanie danych geolokalizacyjnych miejsca wykonania fotografii umieszczonej przez autora w Internecie. Jeżeli zdjęcie zostało zrobione przy użyciu aparatu cyfrowego mającego na wyposażeniu włączony moduł GPS (obecnie coraz więcej zdjęć jest wykonywanych nie tradycyjnym aparatem fotograficznym, ale cyfrową kamerą umieszczoną w telefonie typu smartphone, zawierającym zazwyczaj funkcję GPS), to w pliku metadanych zdjęcia (EXIF) znajdą się dokładne współrzędne miejsca wykonania zdjęcia oraz informacje o dacie i godzinie wykonania fotografii. Można dzięki temu potwierdzić obecność osoby w danym miejscu i mieć pewność co do czasu, w jakim się tam znajdowała. Daje to duże możliwości także organom ścigania, łatwiej jest im bowiem dzięki temu wytypować potencjalne miejsca, w których może przebywać poszukiwana przez nie osoba[55].

Dane fotograficzne dostępne w Internecie (dotyczy to zarówno metadanych, jak i po prostu obiektów uwidocznionych na zdjęciach) mogą pomóc nawet w prowadzeniu operacji militarnych, czego przykładem jest precyzyjny atak lotnictwa amerykańskiego na siedzibę organizacji terrorystycznej Państwo Islamskie (ISIS) 3 czerwca 2015 roku. Atak został przygotowany dzięki prywatnym fotografiom terrorysty z ISIS; prezentował na nich samego siebie przed budynkiem, w którym mieściła się jednostka dowodzenia ISIS; fotografie te umieszczone były w jednym z serwisów społecznościowych[56]. Zbliżona sytuacja z lipca 2014 roku była nieformalnym potwierdzeniem obecności wojsk armii rosyjskiej na terytorium Ukrainy: rosyjski żołnierz wykonał swoje autoportrety i umieścił je w serwisie Instagram – metadane zdjęcia dotyczące lokalizacji geograficznej wskazywały, że w momencie zrobienia zdjęcia musiał znajdować się na Ukrainie[57]. Podobny potencjał mają metadane

[54] Badanie danych z serwisów aukcyjnych, wykraczające poza tematykę białego wywiadu, a związane raczej z pracą operacyjną, pracą dochodzeniowo-śledczą i informatyką śledczą, jest problemem zasługującym na oddzielną publikację. Por. np. „eBay Toolbar in Forensic Investigations" dostępne: http://computer-forensics.7safe.com/ebay-toolbar-in-forensic-investigations/ (dostęp: 14.12.2014 r.).

[55] Por. np. http://exifdangers.blogspot.com/ (dostęp 11.06.2015 r.).

[56] http://www.militarytimes.com/story/military/tech/2015/06/04/air-force-isis-social-media-target/28473723/ (dostęp 5.06.2015 r.).

[57] http://www.businessinsider.com/russian-soldier-ukraine-2014-7 (dostęp 10.08.2014 r.).

w wiadomościach publikowanych w serwisie mikroblogowym Twitter, powiązanych z usługą geolokalizacyjną oferowaną przez moduł Foursquare, którego użytkownicy mogą oznaczać miejsce pobytu w chwili zamieszczenia wiadomości na swoim profilu w Twitterze. Świadczy to wówczas o ich fizycznej obecności w danym miejscu, jak również o tym, że nie znajdują się np. w swoim mieszkaniu (co może pomóc przestępcom w oszacowaniu czasu, jaki mają na dokonanie włamania)[58].

Sprawcy przestępstw mogą korzystać z dostępnych im narzędzi przy przygotowaniu i planowaniu ataków. Prostą metodą rekonesansu jest użycie internetowych serwisów mapowych. W Internecie dostępne są zarówno profesjonalne ortofotomapy, jak i szczegółowe mapy topograficzne, drogowe i satelitarne. Najpopularniejsza aktualnie platforma Google Maps oferuje mapy satelitarne wysokiej jakości i dużej wiarygodności, zawierające w niektórych częściach świata renderowanie trójwymiarowe. Ogromną popularnością cieszy się funkcja Google Street View, pozwalająca użytkownikowi na zapoznanie się z fizycznym otoczeniem danego punktu na mapie (znajdującego się w polu widzenia samochodu firmy Google fotografującego okolicę) poprzez panoramiczne widoki z poziomu ulicy. Potencjał przestępczego wykorzystania Google Street View jest bardzo duży. Wymienia się[59] m.in. możliwość obejrzenia celu w ramach przygotowania ataku (np. włamania) i zorientowanie się w otoczeniu fizycznym, pod kątem obecności płotów, żywopłotów, lokalizacji kamer monitoringu, liczbie i położeniu wejść, wytypowanie kryjówek (krzaki, śmietniki), ustalenie umiejscowienia skrzynek z mediami (gaz, woda, elektryczność), określenie marki, modelu i koloru samochodu zaparkowanego na podjeździe przed domem, dokładne zmierzenie odległości od celu ataku do miejsc ewentualnej ucieczki. Wszystko to możliwe jest bez fizycznego zbliżania się do obiektu. Taką strategię zastosowali m.in. terroryści z ugrupowania Lashkar-e-Taiba, którzy dopuścili się ataków w Bombaju w listopadzie 2008 r.[60] Posługując się serwisem Google Maps, uczyli się na pamięć topografii miasta, tak aby po przybyciu na miejsce nie wzbudzać podejrzeń i nie tracić czasu na zapoznawanie się z siatką ulic[61].

Kolejnym przykładem możliwości pobierania informacji geolokalizacyjnych ze źródeł otwartych jest zdobywająca wielką popularność funkcjonalność pozwalająca na przenoszenie informacji ze sportowych zegarków biegowych[62] (Garmin, Suunto) i smartfonów (z aplikacjami sportowymi, np. Endomondo) do serwisów społecznościowych (zarówno tych powszechnych, jak i przeznaczonych specyficznie dla sportowców). Funkcja rejestracji przebiegu trasy biegowej (przy użyciu modułu GPS w zegarku i telefonie) pozwala użytkownikowi na to, by zapis przebytej trasy (oraz

[58] https://cdt.org/blog/over-sharing-and-location-awareness/ (dostęp 10.05.2011 r.).

[59] http://netsecurity.about.com/od/perimetersecurity/a/How-Criminals-Use-Google-Maps-Street-View-To-Case-The-Joint.htm (dostęp 8.06.2014 r.).

[60] K. Gradoń, *Crime science and the battlefield of the Internet*..., op. cit., s. 95.

[61] http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?_r=0 (dostęp: 27.12.2014 r.).

[62] Wszystkie obserwacje opisane w tym akapicie poczynione zostały przez autora niniejszego artykułu podczas badań własnych.

informacje o prędkości, tempie, czasie i miejscu rozpoczęcia i zakończenia treningu, a także – w przypadku urządzeń wyposażonych w funkcję pomiaru tętna – średnim i maksymalnym tętnie i spalonych kaloriach) przenieść do komputera domowego i wykorzystać go np. do analizy postępów treningowych. Wiele osób przenosi takie dane również do Internetu – na serwisy w rodzaju Run-Log[63], MapMyRun[64] czy Endomondo[65]. Korzystając z otwartych źródeł informacji (znając nazwisko, adres e-mail lub popularny pseudonim) interesującej nas osoby, możemy w tego rodzaju serwisie odnaleźć jej profil i odczytać wszystkie wymienione wyżej parametry. Dzięki temu dowiedzieć się możemy np. o regularnych trasach biegowych tej osoby, porach dnia rozpoczynania treningu i lokalizacji miejsca startu. Jeżeli mamy do czynienia z osobą uprawiającą sport w sposób regularny, prosta analiza trendów pozwolić nam może na postawienie hipotez odnośnie do tego, czy interesujący nas człowiek będzie danego dnia w określonych godzinach przebywał w konkretnych miejscach. Zazwyczaj jesteśmy też w stanie ocenić, czy punktem startu jest np. dom osoby, czy inne, przypadkowe miejsce. Umożliwia to funkcja satelitarnej warstwy mapy nakładana na elektroniczny zapis przebiegu treningu. Możemy też się domyślać, przez jak długi czas osoba będzie przebywała poza domem i którędy może się przemieszczać. Sprawcy przestępstw mogą dzięki temu wytypować czas ataku na obiekt (np. włamanie do domu pod nieobecność właściciela) lub atak na osobę (napad zaplanowany w miejscu położonym na trasie ofiary, a wygodnym i bezpiecznym dla napastnika). Nawet jeżeli sprawca nie zna tożsamości ofiary, a jedynie planuje włamanie lub napaść w konkretnej okolicy, może sprawdzić w serwisie sportowym, czy w tym rejonie przebywają zarejestrowani na danym portalu biegacze, a następnie podejrzeć ich plany treningowe i miejsca startu. Chociaż większość osób zarejestrowanych na serwisach biegowych nie podaje publicznie swojego nazwiska, tylko figuruje tam pod pseudonimem (nickiem), to biały wywiad umożliwia odnalezienie prawdziwych danych konkretnego człowieka: wiele osób aktywnych w portalach sportowych publikuje swoje fotografie z zawodów, na których zazwyczaj figurują z numerem startowym przypiętym do koszulki. Kolejne otwarte źródło danych (strona internetowa organizatora zawodów) pomaga w powiązaniu numeru startowego z imieniem, nazwiskiem, wiekiem i miastem zamieszkania sportowca. Do tego osoba posiłkująca się metodami białego wywiadu ma dzięki portalom biegowym dostęp do zdjęć interesującego ją człowieka, a niekiedy również danych medycznych lub dotyczących wydolności organizmu (VO2Max, HRMax) i kondycji fizycznej.

Opisane wyżej metody i możliwości wykorzystania Internetu i powiązanych z nim nowoczesnych technologii przez przestępców nie wyczerpują oczywiście tematu białego wywiadu i otwartych źródeł informacji. Ze względu na ograniczoną wielkość artykułu niemożliwe było zasygnalizowanie wszystkich możliwości oferowanych aktualnie przez sieć (sam temat wykorzystania otwartych źródeł do budowy, analizy i weryfikacji sieci powiązań między osobami wymagałby oddzielnej

[63] https://run-log.com/.
[64] http://www.mapmyrun.com.
[65] http://www.endomondo.com.

publikacji o porównywalnej objętości). Nowe aplikacje i serwisy udostępniające nowatorskie funkcje pojawiają się na rynku informatycznym z dużą regularnością, tak więc wymienienie wszystkich aktualnie dostępnych metod i przewidzenie kierunków ich rozwoju nie jest możliwe. Moim zamiarem było jedynie zasygnalizowanie skali zagrożenia i zwrócenie uwagi na konieczność intensyfikacji działań profilaktycznych ukierunkowanych głównie na edukację i zwiększanie świadomości społecznej na temat skali i rodzajów zagrożeń. Warto również zaznaczyć, że te same metody, z których korzystać mogą sprawcy przestępstw, są dostępne dla organów, instytucji i agencji, których zadaniem jest zwalczanie przestępczości i działalność kontrterrorystyczna, a ich funkcjonariusze powinni zdawać sobie sprawę z potencjału, jaki oferują im nowoczesne technologie, i aktywnie z nich korzystać przy wykonywaniu swoich obowiązków służbowych.

Specjaliści z zakresu bezpieczeństwa podkreślają, że bezkrytyczne dzielenie się informacjami prywatnymi w Internecie wystawia użytkowników na ogromne ryzyko. Już w początkowym okresie rozwoju Sieci 2.0 (ery portali społecznościowych) zwracano uwagę, że „użytkownicy publikują wiele danych osobistych na swój temat, w tym informacji w rodzaju tych, które wykorzystywane są przez instytucje finansowe do weryfikacji tożsamości klientów. (…) Wszystkie strony internetowe zawierające dane osobowe powinny znaleźć się w ogniu krytyki; dotyczy to także stron firmowych publikujących szczegóły biograficzne i CV pracowników. Prostym rozwiązaniem jest usunięcie wszystkich danych prywatnych ze wszystkich stron w Internecie, podważa to jednak cel istnienia tych stron: większość użytkowników portali społecznościowych znajduje przyjemność w publikowaniu informacji, w tym tych osobistych”[66]. Mimo upływu lat ostatnie zacytowane zdanie pozostaje boleśnie aktualne. Jak zauważa profesor prawa internetowego z Uniwersytetu Harvarda Jonathan Zittrain: „Gdyby Internet został zaprojektowany wokół koncepcji zapewnienia bezpieczeństwa, nigdy nie osiągnąłby tak wielkiego sukcesu, jakim cieszył się już nawet w 1988 roku. Podstawowym założeniem projektowania i wdrażania protokołu internetowego było po prostu przypuszczenie, że ludzie będą z niego korzystać w sposób rozsądny”[67]. Być może końcowa konstatacja wyda się Czytelnikom nadto brutalna, ale dopóki ludzie nie pozbędą się przywar pychy, nieroztropności i ignorancji, dopóty będą się stawać łatwymi ofiarami przestępstw – w tym przypadku: internetowych. Niestety, jestem w tym zakresie pesymistą.

Streszczenie

Artykuł prezentuje problematykę kryminalistyczną otwartych źródeł informacji (tzw. białego wywiadu) pochodzących z Internetu. Przedstawia możliwości taktycznego i strategicznego wykorzystania tych źródeł przez organa ścigania. Zwraca również uwagę na zagrożenia wynikające z niekontrolowanego dostępu do informacji i perspektyw skorzystania z nich przez sprawców przestępstw i terrorystów.

[66] A. Marshall, P. Stephens, *Identity and identity theft*, w: R. Bryant (red.), *Investigating Digital Crimes*, Wiley, Chichester 2008, s. 188–189.
[67] J. Zittrain, op. cit., s. 60.

Słowa kluczowe: biały wywiad, otwarte źródła informacji, *open source intelligence*, OSInt, Internet, cyberprzestrzeń, cyberprzestępczość, cyberterroryzm, *cyberspace*, *cybercrime*, *cyberterrorism*, sieci społecznościowe, *social networks*, policja, służby specjalne, terroryzm, przestępczość kryminalna, bezpieczeństwo

Summary

The paper presents the forensic aspects of Open Source Intelligence, specifically the Internet-based OSInt. It offers the description of the opportunities for the tactical and strategic use of such sources by the law-enforcement agencies. Additionally, it is focused on the threat assessment of the risks arising from the uncontrolled access to information and its potential illicit use by the criminal offenders and terrorists.

Keywords: open source intelligence, open source information, OSInt, Internet, cyberspace, cybercrime, cyberterrorism, social networks, police, law enforcement agencies, terrorism, crime, security.

Piotr Karasek

MANIPULACJA PSYCHOLOGICZNA A SWOBODA WYPOWIEDZI – ROZWAŻANIA NA PRZYKŁADZIE TECHNIKI REIDA

Psychological manipulation v. freedom of expression – discussion on the permissibility of manipulative interrogation on the example of Reid's technique

W żadnej mierze nie wydaje się kontrowersyjne stwierdzenie, iż zasadniczym celem postępowania karnego jest wykrycie i pociągnięcie do odpowiedzialności rzeczywistego sprawcy przestępstwa w oparciu o prawdziwe ustalenia faktyczne[1]. Realizacja tak postawionego celu wymaga oczywiście zgromadzenia wiarygodnego i jak najpełniejszego materiału dowodowego. Trudno więc wyobrazić sobie procedurę karną, w której istotnej roli dowodowej nie odgrywałyby osobowe środki dowodowe.

Zeznania świadków oraz wyjaśnienia podejrzanych (oskarżonych)[2] obejmują ich wypowiedzi procesowe i uzyskiwane są w drodze przesłuchania. Przesłuchanie stanowi zaś czynność procesowo-kryminalistyczną o charakterze dowodowym polegającą na czynnym odbiorze zeznań świadka bądź wyjaśnień podejrzanego przez uprawniony do tego organ procesowy. Zeznanie jest odbierane w sposób bezpośredni i ustny oraz utrwalane – zgodnie z wymogami ustawy procesowej[3]. Przesłuchanie można postrzegać jako czynność materialno-techniczną, *de facto* stanowiącą formę *rozmowy* ze świadkiem czy podejrzanym, która jest inicjowana i protokołowana przez uprawnioną do tego osobę. Dodajmy jednak, że przebieg rozmowy musi odpowiadać wymogom stawianym tej czynności przez ustawę procesową.

Niniejszy artykuł ma na celu prezentację taktyki przesłuchania podejrzanego, opierającej swoją skuteczność na perswazji i manipulacji psychologicznej, ale przede wszystkim ocenę dopuszczalności stosowania jej i podobnych taktyk w świetle polskiej procedury karnej.

---

[1] Por. art. 2 § 1 i 2 k.p.k.

[2] Pojęcia oskarżonego i podejrzanego mogą w pewnym zakresie być stosowane zamiennie z uwagi na treść art. 71 § 3 k.p.k. Zagadnienia opisane w niniejszym artykule będą miały jednak największe zastosowanie do podejrzanego i jego przesłuchania w postępowaniu przygotowawczym.

[3] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 106–107.

Warto już na wstępie w jasny sposób określić, jaki jest ogólny cel prowadzenia przesłuchania (niezależnie od roli procesowej przesłuchiwanej osoby, lecz ze szczególnym uwzględnieniem przesłuchania podejrzanego). Otóż w przeciwieństwie do tego, co miało miejsce w czasach minionych[4], przyznanie się podejrzanego do winy nie stanowi już „królowej dowodów" i uzyskanie go nigdy nie powinno być *per se* celem przesłuchania. Jest nim zaś uzyskanie szczerych, zgodnych z obiektywną rzeczywistością[5] wyjaśnień lub zeznań[6]. Tylko bowiem takie wypowiedzi przesłuchiwanych osób dają możliwość dokonania prawdziwych ustaleń faktycznych, a dzięki temu zrealizowania celu postępowania karnego.

Aby jednak zeznania bądź wyjaśnienia stanowiły wiarygodne źródło dowodu, muszą być pozyskane w odpowiednich warunkach, sprzyjających uzyskaniu szczerych i spontanicznych wypowiedzi. Zagwarantowaniu tych warunków służą zarówno narzędzia pozytywne (np. odpowiednia taktyka przesłuchania), jak i negatywne (np. zakazy dowodowe). Niezwykle istotna część tychże wymogów została zawarta w art. 171 k.p.k., wymienione są w nim między innymi sposoby prowadzenia przesłuchania, których stosowanie jest niedopuszczalne – zakazy te pełnią ważną funkcję gwarancyjną w procesie karnym[7].

Punktem wyjścia do dalszych rozważań powinno być pojęcie „swobody wypowiedzi" osoby przesłuchiwanej. Jest to nieodzowny warunek uzyskania wiarygodnych wyjaśnień bądź zeznań, co oznacza, że osoba ma mieć możliwość decydowania zgodnie z własną wolą o treści swoich wypowiedzi, tak by nic nie krępowało jej w ich formułowaniu[8].

Wiele wskazuje na to, iż to właśnie swoboda wypowiedzi stanowi najważniejszą dyrektywę prowadzenia przesłuchania. Już w pierwszym paragrafie art. 171 k.p.k. zawarto wskazanie, iż: „osobie przesłuchiwanej należy umożliwić swobodne wypowiedzenie się w granicach określonych celem danej czynności". Chociaż w tym kontekście chodzi bardziej o tzw. fazę swobodnej wypowiedzi w przesłuchaniu (tj. przed zadaniem pytań szczegółowych), to swoboda wypowiedzi stanowi też generalną zasadę prowadzenia przesłuchań. Konsekwencje naruszenia tej dyspozycji zostały określone w § 7 ww. artykułu: „zeznania, wyjaśnienia oraz oświadczenia złożone w warunkach wyłączających swobodę wypowiedzi lub uzyskane wbrew zakazom wymienionym w § 5 nie mogą stanowić dowodu". Wspomniany § 5 ww. artykułu

[4] Zob.: uwagi nt. procesu inkwizycyjnego w: S. Waltoś, *Proces karny: zarys systemu*, LexisNexis Polska, Warszawa 2009, s. 88.

[5] Oczywiście wyjaśnienia „szczere" nie muszą być tożsame z wyjaśnieniami „zgodnymi z obiektywną rzeczywistością". Można jednak uznać, że w sytuacji idealnego przesłuchania zakresy tych pojęć pokrywają się całkowicie.

[6] Zob. m.in.: T. Hanausek, *Kryminalistyka – zarys wykładu*, Zakamycze, Kraków 2005, s. 237.

[7] Por. S. Kalinowski, *Przebieg procesu karnego*, Państwowe Wydawnictwo Naukowe, Warszawa 1961, s. 257. Co prawda autor prowadził tam rozważania na gruncie ówcześnie obowiązującej procedury karnej, jednakże z uwagi na jednakową redakcję niektórych przepisów można uznać, iż podejście ustawodawcy do tej kwestii nie uległo zmianie od tamtego czasu.

[8] T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, LexisNexis Polska, Warszawa 2007, s. 467.

stanowi, że stosowanie przemocy fizycznej, psychicznej, gróźb, a także środków chemicznych czy hipnozy wobec przesłuchiwanej osoby jest niedopuszczalne. Można przy tym zgodzić się ze stanowiskiem, iż obowiązująca redakcja przepisu § 7 jest niefortunna. Jego literalna wykładnia prowadzi bowiem do przekonania, iż zakazy wymienione w § 5 są w pewien sposób przeciwstawne wobec wyłączenia swobody wypowiedzi. Tymczasem uznać należy, że wpływanie na wypowiedź osoby przesłuchiwanej za pomocą gróźb, przemocy czy stosowanie narkoanalizy są po prostu najbardziej skrajnymi przykładami wyłączenia swobody wypowiedzi[9] i stanowią wzorcowe przykłady takiej sytuacji. W § 7 ustanowiono po prostu generalną klauzulę niedopuszczalności uzyskiwania wypowiedzi w warunkach wyłączenia jej swobody[10].

W literaturze częściej niż definicję samej swobody wypowiedzi można odnaleźć definicje i rozważania na temat tego, czym jest stan jej wyłączenia. Nie dokonując jednak w tym miejscu wyczerpującego przedstawienia poglądów doktryny, można wskazać, iż zachodzi on wtedy, gdy istnieje nacisk na wolę osoby składającej wyjaśnienia, zeznania lub oświadczenia w procesie karnym lub gdy znajduje się ona w stanie co najmniej utrudniającym przekazanie treści, które chciałaby zawrzeć w swojej wypowiedzi. Stan taki może być związany z obiektywnym wyłączeniem zdolności podejmowania lub realizacji decyzji dotyczącej wypowiadania się (*vis absoluta*) albo z wystąpieniem istotnych dolegliwości powodujących konieczność dostosowania wypowiedzi osoby przesłuchiwanej do oczekiwań przesłuchującego (*vis compulsiva*)[11].

Orzecznictwo wypracowało pewien katalog okoliczności, które w razie ich wystąpienia należy uznać za wyłączające swobodę wypowiedzi osoby przesłuchiwanej. Zazwyczaj są to okoliczności stosunkowo oczywiste, np. związane ze stanem nietrzeźwości przesłuchiwanego czy stosowaniem przemocy fizycznej lub bezpośrednich gróźb jej użycia. Nie w każdym jednak przypadku kwestia dopuszczalności lub niedopuszczalności określonej praktyki jest tak intuicyjna.

Aby odpowiednio zilustrować tę kwestię, wskazać można na nurt w orzecznictwie zmierzający do określenia dopuszczalnych praktyk w kontekście substancji chemicznych, z którymi może mieć kontakt osoba przesłuchiwana. Przede wszystkim zdecydowanie wskazano, że o wyłączeniu swobody wypowiedzi przesądza „każdy stopień nietrzeźwości”[12]. Zarazem jednak, choć zakaz korzystania ze środków chemicznych w przesłuchaniu wprost wynika z treści art. 171 § 5 k.p.k., to pomimo jego literalnego brzmienia nie uznano za wyłączające swobodę wypowiedzi podania przesłuchiwanemu kawy czy papierosa, a nawet środków uspokajających (w rozsądnej dawce). Przypomnijmy przy tym, że za „środek chemiczny” uznać można w zasadzie każdą substancję. Uznano, iż większość „środków chemicznych” nie wpływa

[9] R. Kaczor, *Niedozwolone sposoby przesłuchania*, „Prokuratura i Prawo” 2009, nr 3, s. 116.
[10] Zob. A. Gaberle, *Dowody w sądowym procesie karnym*, Wolters Kluwer Polska, Kraków 2007.
[11] Tamże, zob. też S. Waltoś, *Swoboda wypowiedzi osoby przesłuchiwanej w procesie karnym*, „Prokuratura i Prawo” 1975, nr 10.
[12] Wyrok Sądu Najwyższego z 9 stycznia 2003 r., sygn. III KKW 316/01, OSNWSK 2003, poz. 51.

na procesy psychiczne osoby w sposób, jakiemu zapobiec ma art. 171 § 5 k.p.k.[13] Odejście od literalnej wykładni przepisu należy uznać w tym wypadku za rozsądne. Poważny wyłom w swobodzie wypowiedzi wywołuje natomiast wykorzystanie stanu uzależnienia osoby przesłuchiwanej od jakiejkolwiek substancji (nie sam fakt istnienia takiego uzależnienia)[14]. Istnieją więc sytuacje, w których właśnie długotrwałe pozbawienie przesłuchiwanego danego „środka chemicznego", chociażby nikotyny, będzie powodowało wyłączenie swobody wypowiedzi. W pewien sposób są to więc dwie strony jednego medalu – co do zasady można poczęstować świadka papierosem, lecz nie można czynić tego np. pod warunkiem wcześniejszego złożenia przez niego zeznań określonej treści[15]. Pokazuje to, że granica między praktyką dozwoloną a zakazaną nie zawsze i nie dla każdego jest oczywista.

Oczywiście pewne dolegliwości dla osoby przesłuchiwanej, wpływające na jej szeroko rozumianą swobodę (nie tylko wypowiedzi), wpisane są w naturę postępowania karnego (np. obowiązek stawiennictwa świadków, zatrzymanie podejrzanego). O ile więc dolegliwości te, nawet pochodzące ze strony organu postępowania, wynikają z prawidłowego stosowania ustawy procesowej, to nie można mówić ani o wyłączeniu, ani o ograniczeniu swobody wypowiedzi przesłuchiwanego[16]. Pogląd ten jest odpowiednio poparty także orzecznictwem sądów[17]. Problematyczna jest natomiast m.in. kwestia tego, czy dopuszczalne jest ograniczenie swobody wypowiedzi osoby przesłuchiwanej. Należy podzielić pogląd, iż odpowiednio poważne ograniczenie swobody wypowiedzi daje podstawę do wyłączenia dowodu w myśl art. 171 § 7 k.p.k. Przepis ten nie wskazuje bowiem, że niedopuszczalne wyłączenie swobody wypowiedzi musi być „całkowite"[18] – dopuszczalność dowodu uzyskanego w warunkach „ograniczenia" swobody wypowiedzi zależeć będzie od stopnia tego ograniczenia[19].

---

[13] Wyrok Sądu Apelacyjnego w Katowicach z 17 stycznia 2007 r., sygn. II Aka 421/06, KZS 2007, nr 5, poz. 79.

[14] W kontekście głodu narkotycznego zob.: wyrok Sądu Apelacyjnego w Krakowie z 17 kwietnia 2003 r., sygn. II Aka 75/03, OSA 2003, nr 10, poz. 97. Przesłuchania osób, o których wiadomo, że zażywają narkotyki, wiążą się z wieloma odrębnymi problemami. Zob. M. Bednarczyk, M. Adamczyk, *Uwagi o taktyce przesłuchania świadków zażywających narkotyki w świetle zasady swobody wypowiedzi*, w: V. Kwiatkowska-Darul (red.), *Czynności procesowo-kryminalistyczne w polskich procedurach*, Wydawnictwo Uniwersytetu Mikołaja Kopernika, Toruń 2005.

[15] Identyczna sytuacja podczas przesłuchania świadka przez policjantów została zarejestrowana i zaprezentowana w pierwszym odcinku serialu dokumentalnego *Prawdziwe psy* w realizacji Krzysztofa Langa. Palący policjant, proszony przez świadka o papierosa, zwraca się tam do przesłuchiwanej następująco: „Jak się chce zapalić, to trzeba mówić prawdę (...) jak powiesz prawdę, to będziesz palić".

[16] K. Pawelec, *Proces dowodzenia w postępowaniu karnym*, LexisNexis Polska, Warszawa 2010, s. 233.

[17] Zob. m.in. wyrok Sądu Najwyższego z dnia 26 maja 1981 r., sygn. IV KR100/81, OSNKW 1981, nr 9, poz. 52.

[18] Tamże, s. 238.

[19] K. Pawelec, op. cit., s. 238.

Wydaje się jednak, iż w tym zakresie nie można dopuszczać zbyt daleko idących odstępstw, choć należy pamiętać, że nawet stres wywołany samym faktem uczestniczenia w przesłuchaniu może spowodować, iż zdolność do wypowiadania się zgodnie ze świadomą wolą może być w pewnym stopniu ograniczona.

Dla zachowania swobody wypowiedzi istotną rolę odgrywa przyjęta przez przesłuchującego metoda przesłuchania. Stanowi ona świadomie wybrany i zastosowany przez przesłuchującego sposób postępowania wobec osoby przesłuchiwanej, który przy założeniu prawidłowego rozumienia i podejścia do czynności przesłuchania ma służyć uzyskaniu wszechstronnych i szczerych wypowiedzi[20]. Określeniem zróżnicowanych metod prowadzenia przesłuchań zajmuje się nauka kryminalistyki. Istnieje wiele taktyk prowadzenia przesłuchania – czy to podejrzanego, czy świadka – a wybór odpowiedniej z nich powinien zależeć od cech i właściwości osobistych osoby przesłuchiwanej. Można zgodzić się z poglądem, że trudniejszą i ciekawszą z punktu widzenia teorii komunikacji sytuację stanowi przesłuchanie podejrzanego. Jest tak m.in. ze względu na jego szczególne uprawnienia procesowe (m.in. prawo do odmowy składania wyjaśnień, brak odpowiedzialności karnej za składanie wyjaśnień fałszywych), a także oczywistą, diametralną rozbieżność interesów przesłuchiwanego sprawcy przestępstwa i osoby go przesłuchującej[21]. Z tego powodu szczególną uwagę często poświęca się tworzeniu metod przesłuchań odpowiednich do takiej właśnie sytuacji[22].

Na marginesie warto dodać, że zdaniem niektórych pojęcie „metody" przesłuchania, silnie związane z pojęciem „metodologii", sugeruje naukowość danego sposobu postępowania. Z tego powodu miałoby być zarezerwowane dla przesłuchań przeprowadzonych w zgodzie z ustawą procesową. W przeciwnym razie miałoby to oznaczać, że „nauka pozostaje w służbie bezprawia"[23]. Nie można jednak zgodzić się z tym idealistycznym w swej wymowie poglądem. Powszechnie znane fakty historyczne wskazują niestety, iż nauce zdarzało się „pozostawać w służbie bezprawia". Można jednak przyjąć za cytowanym autorem, że bardziej uniwersalnym pojęciem będzie „taktyka" czy też „sposób" prowadzenia przesłuchania. W przeciwieństwie do „metod" naukowa podbudowa nie jest dla nich warunkiem koniecznym.

Dla zachowania swobody wypowiedzi szczególnie groźne są takie sposoby prowadzenia przesłuchania, które opierając się na elementach naukowych, w szczególności na wskazaniach nauki psychologii, dążą do dostosowania woli przesłuchiwanej osoby do oczekiwań przesłuchującego. W tym punkcie należy wprowadzić pojęcie

[20] Zob. E. Gruza, *Ocena wiarygodności zeznań świadków w procesie karnym: problematyka kryminalistyczna*, Kantor Wydawniczy Zakamycze, Kraków 2003, s. 285.

[21] M. Tokarz, *Manipulacje komunikacyjne w praktyce: przesłuchanie podejrzanego*, w: B. Sierocka (red.), *Przełom komunikacyjny a filozoficzna idea konsensu*, seria: *Via Communicandi*, Oficyna Wydawnicza Atut, Wrocław 2003, s. 209.

[22] Zob. m.in. taktyczne metody przesłuchania podejrzanego w: T. Hanausek, op. cit., s. 241–246, zob. też.: K. Otłowski, *Podejrzany w postępowaniu karnym: studium kryminalistyczne*, Państwowe Wydawnictwo Naukowe, Warszawa 1979, s. 79–125.

[23] R. Kaczor, op. cit., s. 111–112.

„perswazji". Przez perswazję można rozumieć tłumaczenie, dowodzenie i przekonywanie o czymś osoby przesłuchiwanej. Taka forma nacisku jest co do zasady dozwolona w postępowaniu karnym[24]. Elementy perswazji występują przecież w zasadzie w każdym przesłuchaniu, a wpływanie w pewnym stopniu na procesy motywacyjne wyjaśniającego (np. przez wyrażone w wyważony sposób zachęcanie do składania wyjaśnień prawdziwych) nie jest niedozwolone[25]. Istnieje jednak oczywiście granica dopuszczalności wywierania takich nacisków.

Drugim istotnym pojęciem jest „manipulacja", którą zdefiniować można jako „działanie o charakterze niejawnym, mające na celu ukształtowanie postaw korzystnych dla manipulatora przez eliminowanie racjonalnego namysłu i decyzji wskutek oddziaływania na sferę emocjonalną lub kształtowanie fałszywego obrazu rzeczywistości"[26]. Zgadzając się z taką, stosunkowo uniwersalną definicją, należy uznać, że manipulacja stosowana podczas przesłuchania osoby jest wprost skierowana przeciwko swobodzie podejmowania decyzji – a więc przeciwko swobodzie wypowiedzi[27]. Warto zatem przyjrzeć się tym taktykom prowadzenia przesłuchań, których autorzy niekiedy wprost przyznają, iż są one „manipulacyjne", i ocenić dopuszczalność ich stosowania w świetle polskiej procedury karnej.

Aby nadać odpowiedni kontekst tym rozważaniom, należy przedstawić podstawowe założenia i zarys wspomnianych wyżej manipulacyjnych taktyk przesłuchania. Rozbudowane taktyki przeprowadzania przesłuchań podejrzanych na etapie postępowania przygotowawczego (przez policję) proponowane są przez wielu autorów. Najbardziej znane są te zaprojektowane pod auspicjami amerykańskiego Federalnego Biura Śledczego (FBI*)*. Mowa więc przede wszystkim o podręczniku autorstwa E. Inbaua, J. Reida i J. Buckleya[28], opracowanym na bazie ich wcześniejszych prac, a wydanym w 1986 r. pod tytułem *Criminal Interrogation and Confession* (wydawany był ponownie, w poprawianych wersjach[29]). Zdobył on bardzo dużą popularność wśród służb policyjnych na całym świecie[30]. Oferuje zestaw praktycznych wskazówek dotyczących prowadzenia przesłuchania podejrzanego. Charakterystyczną cechą proponowanej przez ww. autorów taktyki jest to, że za podstawowy cel przesłuchania podejrzanego uznają uzyskanie przyznania się przez niego do zarzucanego

[24] R. Markowski, *Manipulacje w postępowaniu karnym*, Oficyna Wydawnicza Impuls, Kraków 2006, s. 47.

[25] Zob. wyrok Sądu Najwyższego z 15 lipca 1979 r., sygn. V KRN 102/79 i 123/79, OSNPG 1980, nr 5, poz. 66 i OSPiKA 1981, nr 7–8, poz. 141.

[26] Definicja autorstwa A. Balickiej za: W. Chudy, *Kłamstwo jako metoda. Esej o społeczeństwie i kłamstwie*, Oficyna Naukowa, Warszawa 2007, s. 19.

[27] Tamże, s. 22.

[28] W późniejszych wydaniach do grona autorów dołączył B. Jayne.

[29] Piąte wydanie pochodzi z 2011 r. Zob.: F. Inbau, J. Reid, J. Buckley, B. Jayne, *Criminal Interrogation and Confessions*, Jones & Bartlett Learning, Burlington 2011.

[30] M. Hartwig, P. Granhag, A. Vrij, *Police interrogation from a social psychology perspective*, „Police and Society" 2005, vol. 15, no. 4, s. 380–381.

mu czynu[31] – wychodząc z założenia, że: „żaden niewinny podejrzany o przeciętnej inteligencji nie przyznałby się do popełnienia przestępstwa tylko dlatego, że przesłuchujący zadaje podchwytliwe pytania"[32]. Doprowadzić ma do tego złożony proces wykorzystujący skomplikowane mechanizmy psychologiczne, a składający się z dziewięciu etapów – kolejnych kroków dochodzenia do przyznania się podejrzanego do winy. Proponowana taktyka została wypracowana na podstawie długoletniej praktyki autorów[33]. Zarazem jest to prawdopodobnie najbardziej autorytatywna praca opisująca techniki przesłuchania[34].

Nazwana przez autorów metodą „przesłuchania w dziewięciu krokach" (skrótowo metodą „dziewięciu kroków" lub od nazwiska jednego ze współautorów „techniką Reida") stanowi jeden z centralnych elementów podręcznika. Autorzy czynią także szereg zastrzeżeń i założeń, które mają znaczenie przy ewentualnym zastosowaniu opisanej przez nich taktyki – przede wszystkim uprzedzają, że nadaje się ona do zastosowania wobec podejrzanych, co do których winy przesłuchujący nie ma wątpliwości (lub nie są one duże)[35]. Podręcznik zawiera także wiele innych wskazówek, dotyczących na przykład sposobów wykrywania kłamstwa na podstawie zachowania się podejrzanego, czy opisy pomocniczych technik towarzyszących przesłuchaniu (takich jak choćby techniki niewerbalne, mające na celu psychologiczne zbliżenie się przesłuchującego z przesłuchiwanym).

Ze względu na popularność i wpływ tego właśnie podręcznika na praktykę (w szczególności amerykańską[36]) celowe jest przedstawienie szczegółów proponowanej w nim taktyki przesłuchań. Celem poniższego opisu nie jest jednak wyczerpujące jej zaprezentowanie czy też instrukcja jej zastosowania, lecz jedynie zasygnalizowanie istotnych elementów i założeń tej taktyki. Dzięki temu możliwe będzie dokonanie rzeczywistej oceny jej charakteru.

Pierwszym z dziewięciu etapów takiego przesłuchania jest tzw. oskarżenie – należy w zdecydowany sposób postawić zarzut podejrzanemu, wyrażając przy tym postawę przekonania o jego winie (autorzy wskazują, że podejrzany powinien nie mieć wątpliwości co do tego, iż przesłuchujący go wierzy w jego winę – w przeciwnym razie trudniej będzie go nakłonić do przyznania się). Po postawieniu zarzutu – przy czym zdaniem autorów można zarzut wyolbrzymić czy wręcz zasygnalizować podejrzanemu istnienie mocnych dowodów jego winy (chociażby takie nie istniały lub nie znajdowały się w dyspozycji organu ścigania) – należy przyjrzeć się reakcji podejrzanego. Na tym etapie wolno dopuścić do zaprzeczenia przez niego

[31] Wskazuje się, że o ile przyznanie się nie uchodzi już co prawda za *królową dowodów*, o tyle w postępowaniu przygotowawczym nadal stanowi moment z wielu powodów przełomowy czy wręcz najważniejszy. W ten sposób zob.: M. Tokarz, op. cit., s. 212–213.

[32] F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 365.

[33] E. Gruza, *Psychologia sądowa dla prawników*, Wolters Kluwer Polska, Warszawa 2009, s. 127.

[34] B. Hołyst, *Psychologia kryminalistyczna*, LexisNexis Polska, Warszawa 2009, s. 1204.

[35] M. Tokarz, op. cit., s. 213.

[36] E. Gruza, *Psychologia sądowa*…, op. cit., s. 127.

swojej winy, lecz tylko raz. Później należy oskarżenie powtórzyć i zdecydowanie nie pozwalać na zaprzeczenia – psychologiczny mechanizm konsekwencji[37] powoduje bowiem, że trudniej jest wycofać się ze stanowiska, które wcześniej wielokrotnie wyrażaliśmy[38].

W drugim etapie należy zaoferować podejrzanemu taką wersję zdarzeń z jego udziałem, w której jego wina będzie w akceptowalnym dla niego stopniu zmniejszona. Można tego dokonać przez wyrażanie zrozumienia dla jego zachowania („Na twoim miejscu każdy by tak zrobił…") czy też przez przerzucenie odpowiedzialności na ofiarę („Nie dziwię się, żadna porządna kobieta by się tak nie ubrała…"). Należy znaleźć płaszczyznę porozumienia z podejrzanym i podsunąć mu możliwą do zaakceptowania przez niego wersję motywacji popełnienia przestępstwa. Zbudowany w tym momencie motyw popełnienia przestępstwa stanie się istotnym elementem późniejszego etapu przesłuchania[39].

W trzecim etapie należy uzyskać psychologiczną dominację nad przesłuchiwanym – dalej prowadzić rozmowę, nie dopuszczając do jakichkolwiek zaprzeczeń. Jak wspomniano wyżej, zaprzeczenia przesłuchiwanego są niepożądane – utrudniają uzyskanie przyznania się na późniejszym etapie i stawiają przesłuchującego w pozycji defensywnej. Autorzy „techniki Reida" wymieniają zarazem szereg zachowań podejrzanego (werbalnych i niewerbalnych), które mogą wskazywać na chęć dalszego zaprzeczania swojej winie – sugerują, aby wychwytywać takie zachowania i reagować prewencyjnie. Nakazują zarazem oceniać charakter zaprzeczeń podejrzanego: podejrzany niewinny będzie, ich zdaniem, zaprzeczał bardziej żywiołowo i spontanicznie od winnego[40].

W pewnym momencie należy przejść do etapu czwartego, w którym można pozwolić podejrzanemu tłumaczyć swoje zachowanie, lecz wszystko obracając przeciwko niemu, starając się jednocześnie skupić jego myśli na zaproponowanej mu na etapie drugim wersji (gdy przesłuchiwany stwierdzi, że np. nie zdołałby dokonać danego czynu, bo nie jest tak agresywny, możemy odpowiedzieć: „No właśnie! Co też ta kobieta musiała z Tobą zrobić, żebyś się do tego posunął…"). To wszystko może trwać stosunkowo długo, aż przesłuchiwany zacznie przejawiać stopniową apatię spowodowaną poczuciem braku wpływu na przesłuchanie. Ma on w tym czasie przekonać się, że jego zaprzeczenia nie są skuteczne, i utracić pewność siebie[41].

---

[37] R. Cialdini, *Wywieranie wpływu na ludzi: teoria i praktyka*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1996, s. 67.

[38] Por.: *Step 1 – Direct, positive confrontation*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 192–201, zob. też.: E. Gruza, *Psychologia sądowa*…, op. cit., s. 127.

[39] Por.: *Step 2 – Theme development*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 202–254, zob. też E. Gruza, *Psychologia sądowa*…, op. cit., s. 127.

[40] Por.: *Step 3 – Handling denials*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 255–275, zob. też E. Gruza, *Psychologia sądowa*…, op. cit., s. 128.

[41] Por.: *Step 4 – Overcoming objections*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 276–280, zob. też E. Gruza, *Psychologia sądowa*…, op. cit., s. 128.

Następuje wówczas piąty etap przesłuchania. W tym momencie, jak uważają autorzy taktyki „dziewięciu kroków", przesłuchiwany jest szczególnie wrażliwy. Istotne jest, aby podtrzymać jego uwagę i skupienie na temacie przesłuchania. Wskazuje się, że osoba, której uwaga jest rozproszona, zrywa komunikację. Należy wykorzystać moment osłabienia woli podejrzanego i psychologicznie zbliżyć się do niego. Stosując pomocnicze techniki niewerbalne, również opisywane przez autorów, trzeba w niedługim czasie skrócić psychologiczny dystans pomiędzy przesłuchującym i przesłuchiwanym. Może posłużyć temu na przykład zmniejszenie fizycznej odległości między nimi, połączone z przyciszeniem mowy i utrzymywaniem kontaktu wzrokowego. Jednocześnie należy powrócić do motywu popełnienia przestępstwa przedstawionego podejrzanemu na drugim etapie[42].

Krok szósty następuje, gdy podejrzany jest już stosunkowo pasywny wobec przesłuchującego. Należy wówczas wrócić do prezentowania mu usprawiedliwiających, rozgrzeszających go wersji zdarzenia, jednocześnie bacznie obserwując jego reakcje. Ponadto trzeba ponownie okazać zrozumienie dla przyczyn popełnienia przez niego przestępstwa, zarazem usilnie namawiając do skruchy[43].

W pewnym momencie trzeba przejść do swoistej ofensywy – kroku siódmego, którego istotę autorzy określają mianem „pytania-pułapki". Pytanie to jest niczym innym jak pytaniem sugerującym treść odpowiedzi (w bardzo agresywnej formie), zawierającym dwa alternatywne rozwiązania. Oba są niekorzystne dla podejrzanego, lecz przynajmniej jedno z nich powinno pozwolić mu usprawiedliwić przed sobą swoje zachowanie (nie musi to być prawda, nawet w świetle zgromadzonego materiału dowodowego – wersję można zaostrzyć po uzyskaniu wstępnego przyznania się). Pytanie może brzmieć: „Czy użyłeś noża z premedytacją, czy po prostu w nerwach podsunął ci się pod rękę?". Przesłuchanie powinno trwać do momentu, gdy podejrzany przyzna się, odpowiadając na pytanie-pułapkę w obciążający go sposób[44]. Tego rodzaju pytanie ma też na celu zasianie wątpliwości w umyśle przesłuchiwanego, tak by choć na chwilę, o ile jest faktycznie winny, zwątpił w opłacalność kłamstwa[45]. Warto zauważyć, że w świetle polskiej procedury karnej zadawanie pytań sugerujących treść odpowiedzi jest niedopuszczalne, aczkolwiek nie pociąga za sobą skutku nieważności całego przesłuchania. Nie można jednak ustrzec się przed pytaniem sugerującym, gdy wbrew dyspozycji art. 171 k.p.k. zadaje je osoba pełniąca funkcję organu procesowego (np. przesłuchujący podejrzanego policjant). Autorzy podkreślają, że nie wolno wówczas przerwać przesłuchania, gdyż uzyskane przyznanie się jest nietrwałe.

---

[42] Por.: *Step 5 – Procuremend and retention of a suspect's attention*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 281–286, zob. też E. Gruza, *Psychologia sądowa*…, op. cit., s. 129.

[43] Por.: *Step 6 – Handling the suspect's passive mood*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 287–292, zob. też E. Gruza, *Psychologia sądowa*…, op. cit., s. 129.

[44] Por: *Step 7 – Presenting an alternative question*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 293–302, zob. też E. Gruza, *Psychologia sądowa*…, op. cit., s. 129.

[45] M. Tokarz, op. cit., s. 213.

Należy wówczas przejść do etapu ósmego – uzyskania pełnego przyznania się z uzupełnieniem wszelkich koniecznych szczegółów zdarzenia, oraz dziewiątego – czyli odpowiedniej dokumentacji przesłuchania (w realiach amerykańskich przesłuchania nie protokołuje się koniecznie na bieżąco)[46].

Podsumowując przedstawioną wyżej taktykę „przesłuchania w dziewięciu krokach", można wskazać, że jest to propozycja obejmująca pewien złożony proces przesłuchania. Jej autorzy szczegółowo opisują każdy z etapów, podając także hipotetyczne reakcje podejrzanego i proponując właściwe reakcje przesłuchującego. Pomimo swojej popularności jest to taktyka wysoce kontrowersyjna i wielokrotnie krytykowana, także przez amerykańskich czy brytyjskich badaczy[47]. Przyznanie się do winy podejrzanego, o ile nastąpi, uzyskuje się przez stopniowe budowanie w nim poczucia, iż jest to najlepszym wyjściem w jego sytuacji[48]. Jest to więc rozbudowany proces, w którym wykorzystywanych jest wiele podświadomych mechanizmów psychologicznych. Wielu podejrzanych, szczególnie mniej inteligentnych, będzie całkowicie bezbronnych wobec takiej taktyki – i to niestety niekoniecznie z powodu ich faktycznej winy. Warto dodać, że przesłuchanie tym sposobem może trwać stosunkowo długo. Pytanie-pułapka (niedopuszczalne przecież, a jednak niepowodujące nieważności dowodu), stanowiące kulminacyjny moment przesłuchania, pojawia się po długim procesie psychologicznej manipulacji podejrzanym[49]. Stosowanie tej i podobnych taktyk przesłuchania krytykowane jest także przez psychologów, określających je mianem „wyrafinowanych" czy „wymuszających"[50]. Pomijając pojawiające się zarzuty dotyczące naukowej nierzetelności autorów metody „przesłuchania w dziewięciu krokach"[51], bardzo często wobec takich manipulacyjnych technik przesłuchania podnoszone są także wątpliwości natury etycznej związane ze stosowaniem podstępu i kłamstwa.

Nie ulega wątpliwości, że przy wykorzystaniu manipulacyjnych technik przesłuchań wprost zaleca się wprowadzanie w błąd podejrzanego. Należy się więc zastanowić, czy już tylko z tego powodu nie następuje wyłączenie swobody wypowiedzi przesłuchiwanego. Nie ma pełnej zgody na tym tle – można spotkać się z poglądem, że wprowadzanie podejrzanego w błąd nie jest niczym złym, gdyż sam fakt podania mu fałszywych informacji nie stanowi zmuszania go do przyznania się do winy,

[46] Por.: *Step 8 – Having the suspect orally relate various details of the offense*, w: F. Inbau, J. Reid, J. Buckley, B. Jayne, op. cit., s. 303–309, oraz: *Step 9 – Converting an oral confession into a written confession*, tamże, s. 310–328.

[47] E. Gruza, *Psychologia sądowa*…, op. cit., s. 130.

[48] Tamże, s. 129–130, za: A. Memon, A. Vrij, R. Bull, *Prawo i psychologia – wiarygodność zeznań i materiału dowodowego*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2003, s. 156–157.

[49] M. Hartwig, P. Granhag, A. Vrij, op. cit., s. 387.

[50] B. Hołyst, op. cit., s. 1201, za: P. Zimbardo, *The psychology of Police confessions*, „Psychology Today" 1967, no. 1, s. 17–27.

[51] Wskazuje się, że skuteczność bardzo wielu z technik opisywanych przez autorów uzasadniana jest w zasadzie tylko ich długoletnim doświadczeniem zawodowym i że nie mają one oparcia w badaniach naukowych. Zob. m.in.: B. Hołyst, op. cit., s. 1218–1219.

lub że jest co prawda zachowaniem nie fair, lecz dopuszczalnym z punktu widzenia swobody wypowiedzi[52]. Bardzo podobne stanowisko w tej sprawie wyraził też dawniej Sąd Najwyższy[53]. Wydaje się jednak, iż takie zapatrywania świadczą o pomyleniu „swobody wypowiedzi" z „możliwością wypowiedzenia się". Uznać należy za słuszny pogląd, iż podstęp stanowi nieetyczną, niedopuszczalną metodę śledczą[54]. Rzecz jasna nie oznacza to, że funkcjonariusze organów ścigania powinni być wobec przesłuchiwanego nadto szczerzy. Należy jednak pamiętać, że wypowiedzi przesłuchiwanej osoby złożone pod wpływem błędu nie będą w pełni wiarygodne – mogą być np. wyrazem pewnej przyjętej przez przesłuchiwanego taktyki.

Innym, bodajże najpoważniejszym problemem, na który warto zwrócić uwagę w odniesieniu do przesłuchań manipulacyjnych, jest ryzyko uzyskania fałszywego przyznania się do winy. Jak wskazano powyżej, przyznanie się do winy jest podstawowym celem tego rodzaju przesłuchań. Praktyka pokazuje, że wbrew przyjętemu założeniu w pewnych warunkach do przestępstwa przyzna się nawet niewinna osoba. Bynajmniej nie jest to zjawisko marginalne – przyznanie się oskarżonego do winy odnotowano aż w 88 z 325 (27%) spraw, w których w ramach amerykańskiego „Innocence Project" ponad wszelką wątpliwość wykazano później niesłuszne skazanie oskarżonego[55]. Podstawowym problemem jest to, iż przy tego typu agresywnych psychologicznie technikach część podejrzanych, pomimo swojej niewinności, nie jest w stanie oprzeć się woli przesłuchującego. Przyznają to, acz niechętnie, nawet sami autorzy niektórych policyjnych podręczników[56]. Nie wchodząc głębiej w rozważania nad fenomenem fałszywych samooskarżeń i ich wpływem na niesłuszne skazania, należy stwierdzić, iż problem ten istnieje i jest poważny, a wpływem manipulacyjnych technik przesłuchania na skalę tego zjawiska zainteresowało się już wielu autorów[57]. Zapewnienie swobody wypowiedzi, jak widać, istotne jest nie tylko ze względu na obowiązek humanitarnego i etycznego traktowania uczestników postępowania, lecz także ze względu na ochronę wymiaru sprawiedliwości przed fałszywym przyznawaniem się oskarżonych do winy. Z uwagi na to ryzyko stosowanie manipulacji psychologicznej w przesłuchaniu podejrzanego jest niedopuszczalne również z czysto pragmatycznego punktu widzenia.

Brak jest danych pozwalających na stwierdzenie, czy i w jakim zakresie takie techniki są stosowane w Polsce w praktyce. Zwraca jednak uwagę fakt, iż polscy

---

[52] Zob. W. Daszkiewicz, *Swoboda wypowiedzi jako przesłanka ważności dowodu w procesie karnym*, „Prokuratura i Prawo" 1979 nr 7–8, s. 74.

[53] Wyrok Sądu Najwyższego z 15 lipca 1979 r., op. cit.

[54] K. Pawelec, op. cit., s. 232, za: Z. Krasny, *Swoboda wypowiedzi podejrzanego w śledztwach dotyczących spraw aferowych*, „Problemy Prawne" 1978, nr 2, s. 246.

[55] Dane za: http://www.innocenceproject.org/causes-wrongful-conviction, dostęp dnia 10 maja 2015 r.

[56] B. Hołyst, op. cit., s. 1200–1201, za: J. Wakley, *Police Interrogations. A Handbook for Investigators*, Police Review Publication, London 1987.

[57] Zob. m.in.: G. Gudjonsson, *The Psychology of Interrogations and Confessions*, Wiley 2003, s. 173–215, 360–412, oraz: A. Memon, A. Vrij, R. Bull, *Psychologia i prawo*…, op. cit.

policjanci przechodzili w ostatnich latach szkolenia z zakresu przesłuchań tzw. metodą FBI[58], obejmującą bardzo często także opisaną wyżej metodę „dziewięciu kroków" lub jej istotne elementy, takie jak „pytanie-pułapka", opisywane również w policyjnych czasopismach[59]. Ponadto w ramach struktur polskiej policji przetłumaczono na język polski inny popularny podręcznik prowadzenia przesłuchań opracowany przez FBI. Dostarczony funkcjonariuszom policji jako materiał szkoleniowy tekst powtarza bardzo wiele z tez i agresywnych psychologicznie wskazówek omawianej wyżej techniki. Jeden z jego rozdziałów zawiera też wskazówki dotyczące programowania neurolingwistycznego, co może w pewien sposób zobrazować techniki, jakie są tam proponowane[60].

Zmierzając ku podsumowaniu, należy zastanowić się więc nad odpowiedzią na zadane wcześniej pytanie: czy manipulacyjne techniki przesłuchania są technikami niedozwolonymi i czy korzystanie z nich powoduje wyłączenie swobody wypowiedzi przesłuchiwanego w rozumieniu art. 171 § 7 k.p.k.? Opisana wyżej metoda „przesłuchania w dziewięciu krokach", stanowiąca bodaj najbardziej jaskrawy przykład taktyki manipulacyjnej, składa się z wielu kroków, zmierzających do stopniowego złamania woli podejrzanego. Swoboda wypowiedzi może więc zostać w tej sytuacji wyłączona. To, czy do tego dojdzie, zależy oczywiście od wielu czynników, takich jak inteligencja i cechy emocjonalne podejrzanego oraz umiejętności zastosowania technik manipulacyjnych i inteligencja przesłuchującego. Za manipulowaniem podejrzanym mogłyby przemawiać zapewne argumenty natury utylitarnej (w imię zasady, że cel uświęca środki), jednakże z uwagi na wspomniane wcześniej ryzyko wystąpienia fałszywych samooskarżeń nie można w pełni zgodzić się z takim stanowiskiem. Uprawnione będzie mimo to twierdzenie, że poważne ryzyko naruszenia swobody wypowiedzi, brak wiarygodności samooskarżeń uzyskanych drogą manipulacji, jak również nieetyczność taktyk manipulacyjnych, przemawiają za niedopuszczalnością ich stosowania – zarówno z racjonalnego, jak i czysto formalnego (procesowego) punktu widzenia.

Streszczenie

Wyłączenie swobody wypowiedzi stanowi jeden z zakazów dowodowych wyrażony w formie klauzuli generalnej w art. 171 § 7 k.p.k. i jedynie częściowo doprecyzowany w art. 171 § 5 k.p.k. Oprócz intuicyjnie rozpoznawanych przesłanek wyłączenia swobody wypowiedzi warto rozważyć mniej intuicyjne tego przyczyny, takie jak zastosowanie wobec podejrzanego manipulacyjnych technik przesłuchania. Istniejące manipulacyjne techniki przesłuchania opierają swoją skuteczność na różnych mechanizmach psychologicznych i stanowią poważne zagrożenie dla prawidłowo rozumianej swobody wypowiedzi podejrzanego.

Słowa kluczowe: swoboda wypowiedzi, manipulacja, przesłuchanie, technika Reida

[58] E. Gruza, *Psychologia sądowa*…, op. cit., s. 130.
[59] Zob. G. Bartuszek, *Pytamy, słuchamy*, „Policja 997", marzec 2007.
[60] Mowa o niepublikowanym podręczniku *Taktyka i technika przesłuchań* w tłum. kom. Macieja Boreckiego i kom. Pawła Tarnawskiego z Centralnego Biura Śledczego.

Summary

Polish rules of evidence prohibit the use of any witness testimony or confession which has not been in conditions of freedom of expression. There are many possible reasons of the exclusion of freedom of expression in a particular case – many of them are obvious or clearly indicated in art. 171 § 5 of the Code of Criminal Procedure. However, there are also less intuitive reasons for the exclusion of the freedom of expression such as psychological manipulation. Existing manipulative interrogation techniques use very advanced psychological coercion methods and they pose a serious threat to freedom of expression.

Keywords: freedom of expression, manipulation, interrogation, Reid's technique

Judyta Kasperkiewicz

ZAKUP KONTROLOWANY METODĄ WALKI Z ANONIMOWĄ SIECIĄ TOR

Sting operations as a method to fight anonymous net TOR

Wprowadzenie

Zagadnienie bezpieczeństwa i ochrony prywatności w cyberprzestrzeni stanowi już od kilku lat jeden z najczęstszych tematów rozważań i debat prawnych. Od czasu głośnej afery związanej z Edwardem Snowdenem (PRISM) użytkownicy Internetu dostrzegli, że trudno o anonimowość w sieci, i zdali sobie sprawę, że każdy przejaw ich działalności w sieci może stać się w pełni jawny i dostępny dla różnych instytucji państwowych. Dzięki bardzo popularnym portalom społecznościowym tym instytucjom (głównie służbom specjalnym) dużo łatwiej jest gromadzić dane o całym społeczeństwie. Szczególnie otwarty na współpracę z instytucjami państwowymi jest Facebook i dlatego też bardzo zaskakuje fakt, że ten portal dostępny jest również w anonimowej sieci TOR, gdzie przecież z założenia nie dochodzi do ujawniania prawdziwej tożsamości użytkowników i nie ma możliwości gromadzenia danych, które pozwalają przykładowo na wyświetlanie spersonalizowanych reklam. Zapewne na poznanie rzeczywistego celu tego posunięcia portalu przyjdzie nam jeszcze poczekać.

W odpowiedzi na potrzebę zachowania anonimowości niektórych użytkowników Internetu będących obywatelami państw rządzonych przez dyktaturę, np. Korei Północnej czy Chin, stworzono wspomnianą wyżej anonimową sieć TOR, tak aby umożliwić ludności tych państw niczym nieograniczony dostęp do niektórych zakazanych w ich krajach stron internetowych. Jednakże tego, co stało się później, nikt nie mógł nawet częściowo przewidzieć, gdyż obecnie sieć TOR stała się rajem dla przestępców, w tym głównie pedofilów, złodziei i hakerów.

Odpowiednie organy podejmują działania celem zahamowania nieprzewidzianego rozwoju tej sieci, a jednak ciągle jest to bardzo trudne. Zdarzają się działania organów ścigania podejmowane na szeroką skalę, ale po każdym z takich głośnych sukcesów pojawiają się nowi przestępcy, którzy zapełniają powstałą lukę.

Podstawowe pojęcia

Sieć TOR nazywana jest również ciemniejszą stroną Internetu, darknetem, *dark web* czy też *shadow* Internetu. Skrót TOR pochodzi od słów *The Onion Router*[1]. Sieć TOR została stworzona przez amerykańską Marynarkę Wojenną 20 września 2002 roku, a od 2005 roku rozwijana jest przez organizację non-profit Tor Project. Znakiem rozpoznawczym, a zarazem logo sieci jest cebula, a domenę stanowi .onion.

Jest to bezpłatny serwis, który prowadzi działalność równolegle do uniwersalnego Internetu, a jedyna różnica polega na tym, że aby z niej korzystać, należy posłużyć się specjalnym programem, który dostępny jest w Internecie.

Z założenia sieć TOR ma służyć zapewnieniu anonimowości użytkownikom, tak aby niemożliwe było namierzenie adresu IP danego użytkownika. W tym celu adres IP użytkownika przechodzi przez kilka serwerów.

Sieć TOR słynie z funkcjonujących na niej forów internetowych, które zawierają rady i wskazówki przydatne w działalności przestępczej i innej zabronionej. Przykładowo polskie fora zawierają działy dotyczące: kradzieży, przejmowania kont, podrabiania dokumentów, zemsty, szantażu czy też stalkingu. Ponadto prezentują ogromne ilości treści pornograficznych i pedofilskich. Te wpisy nie są jedynie poradami osób nieletnich, ale jak pokazują statystyki, z sieci TOR korzystają głównie osoby dorosłe, które zdają sobie sprawę z bezsilności policji, dlatego też często jawnie drwią z tej sytuacji. Popularne polskie fora w sieci to m.in. Polish Board & Market, Torowisko i ToRepublic.

Jak stwierdzają przedstawiciele policji różnych krajów, poza monitoringiem sieci TOR niewiele można obecnie zdziałać. Również taka instytucja jak EUROPOL jest bezradna w tej kwestii. W przeważającej mierze skuteczne działania policji bazują na błędach użytkowników sieci. Niektóre z większych operacji policyjnych, których efektem było zatrzymanie pedofilów, prowadziły właśnie do sieci TOR.

Za granicą zdarza się coraz częściej, że po kradzieży prywatnych zdjęć znanych osób przestępcy szantażują je lub nielegalnie wykorzystują. Nie jest problemem poruszanie się po sieci TOR, ale problem stanowi wejście do jej głębszych warstw, dokąd dostęp mają tylko nieliczni. Aby wejść na utworzone strony, należy uzyskać często bardzo skomplikowany ciąg znaków w domenie .onion, który składa się na adres sieci.

Wewnątrz sieci dokonano podziału na zaufanych i nowych użytkowników. Co więcej, ustalono, że będą przyznawane punkty zaufania, a za przeprowadzone transakcje udzielane będą rekomendacje. Dla użytkowników sieci TOR użytkownicy „clear netu" stanowią cel pogardliwych wypowiedzi.

W sieci TOR najczęściej dochodzi do handlu dokumentami, danymi oraz kontami z portali aukcyjnych, np. Allegro. Nawet jeśli założymy, że część ofert jest fikcyjna, to i tak wiele z nich rzeczywiście jest zawieranych. Zwykle transakcje opłacane są za pomocą kart prepaidowych albo bitcoinami. Każdy użytkownik sieci TOR może założyć swój portfel będący kontem, na które składa się ciąg liczb. Na to konto

[1] https://www.torproject.org/, stan na dzień: 14 kwietnia 2015 r.

przekazywane są kryptowaluty, a następnie za pośrednictwem kantoru *on line* są one wypłacane na rzeczywiste konto bankowe.

Utworzone w sieci TOR fora internetowe pozostają ciągle poza jakąkolwiek kontrolą policji. Jedynie jej administratorzy na bieżąco monitorują każdego użytkownika i niekiedy stosują blokady według tylko sobie znanych zasad postępowania.

W skład sieci TOR wchodzą węzły wyjściowe oraz węzły pośredniczące, które stanowią stanowiska komputerowe na całym świecie, w odpowiedni sposób skonfigurowane i uruchomione. Obecnie funkcjonuje około kilku tysięcy węzłów obu rodzajów i dziewięć głównych serwerów. Zaszyfrowana informacja (inaczej pakiet) z komputera jednego użytkownika przesyłana jest do innego użytkownika komputera, następnie ten użytkownik rozszyfrowuje ją według klucza, który jest znany tylko jemu, i szyfruje ją w inny sposób. Kolejno dochodzi do przesłania tej nowo zaszyfrowanej informacji następnemu użytkownikowi komputera i cały proces się powtarza. Stąd wzięło się porównanie sieci TOR do cebuli, ponieważ cały proces przesyłu podlega rozwarstwieniu. Najbardziej narażony na wykrycie tożsamości jest użytkownik wyjściowy (ostatni, zwany również Tor Exit Node) oraz ten, który go poprzedza. Ta okoliczność stanowi najsłabszy punkt sieci. Natomiast pierwszy i pośredni użytkownicy są praktycznie niewykrywalni. Co dziesięć minut dochodzi do wyboru nowej, przypadkowej drogi w sieci dla działających aktualnie 8000 serwerów. Według ostatnich statystyk 11% użytkowników TOR pochodzi z USA, 7% z Niemiec, a 3,5% z Polski[2].

Sam program potrzebny do podłączenia się do sieci TOR jest legalny, dostępny w internecie, bazuje na przeglądarce Firefox. Istnieje możliwość pobrania go na trzy najpowszechniejsze systemy komputerowe, tj. Windows, Linux i Mac. Program dostępny jest również jako aplikacja mobilna dla telefonów komórkowych i tabletów. Jedną z głównych wad sieci jest powolne działanie i ciągle jeszcze ograniczona dostępność niektórych popularnych stron, które nie udostępniają swoich adresów w sieci TOR.

Kod programu określany jest jako *open source*, co oznacza, że jest publiczny. Umożliwia dzięki temu wykrywanie słabych punktów oraz uniemożliwia działanie funkcji szpiegowskich.

W nawiązaniu do funkcjonującej sieci TOR utworzony został blog „Arma", który publikuje zapewnienia, że sieć jest w pełni bezpieczna; na bieżąco umieszczane są na nim wpisy informujące o możliwych atakach na sieć i jej użytkowników.

Zakup kontrolowany oraz przesyłka niejawnie nadzorowana

Zakup kontrolowany jako czynność operacyjno-rozpoznawcza możliwy jest dzięki art. 19 ust. 1 i 2 ustawy o Policji i właśnie ta czynność operacyjno-rozpoznawcza najczęściej jest stosowana w przypadku walki policji z przestępcami z sieci TOR. Zakup kontrolowany niesłusznie czasami nazywany bywa prowokacją policyjną[3]. Wspomniany przepis jest zwykle stosowany w celu sprawdzenia uzyskanych

[2] www.metrics.torproject.org/users.html, stan na dzień: 14 kwietnia 2015 r.

[3] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Oficyna Wydawnicza Łośgraf, Warszawa 2011, s. 69.

wcześniej wiarygodnych informacji o przestępstwie, a następnie ustalenia sprawców oraz zdobycia dowodów przestępstwa.

Wyróżnia się cztery metody przeprowadzenia zakupu kontrolowanego:

- dokonanie w sposób niejawny nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione;
- przyjęcie lub wręczenie korzyści majątkowej;
- złożenie propozycji nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione;
- złożenie propozycji przyjęcia lub wręczenia korzyści majątkowej.

W czasie przeprowadzanych czynności podejmuje się wszelkie dopuszczalne przez prawo środki konieczne do zapewnienia bezpieczeństwa osobistego policjantów i osób udzielających pomocy Policji[4].

Przewiduje się dwa mechanizmy przeprowadzania zakupu kontrolowanego. Jako pierwszy wskazuje się zatrzymanie osoby podejrzewanej przez funkcjonariusza w momencie przekazywania przedmiotów lub korzyści, które są przedmiotem transakcji, przy nieujawnianiu powodów dokonania transakcji oraz danych osób uczestniczących w czynnościach. Natomiast drugim z tych mechanizmów jest przeprowadzanie kilku zakupów kontrolowanych w celu ustalenia wszystkich powiązań pomiędzy osobami biorącymi udział w transakcji, tj. dostawcy, sprzedawcy oraz odbiorcy[5].

Sama procedura przeprowadzenia czynności wskazanych w art. 19a ustawy o Policji przebiega zwykle w podobny sposób. Zwykle prowadzone są wcześniej inne czynności operacyjno-rozpoznawcze, które dają przypuszczenie, że zaistniał zamiar lub dokonanie jednego z czynów zabronionych wskazanych w art. 19a ust. 1 ustawy o Policji. W wyniku podjęcia takiego przypuszczenia rozpoczyna się od przygotowania do przeprowadzenia zakupu kontrolowanego. W przypadku sieci TOR najczęściej wystarczy informacja, że źródłem przestępczego działania jest ta sieć, tj. strona internetowa w domenie .onion.

Przed rozpoczęciem faktycznych przygotowań kierownik jednostki Policji lub kierownik komórki organizacyjnej jednostki Policji właściwej do wykonywania czynności operacyjno-rozpoznawczych kieruje pisemny wniosek do Komendanta Głównego Policji lub komendanta wojewódzkiego Policji o wydanie stosownego zarządzenia. Tymczasem Komendant Główny Policji lub komendant wojewódzki Policji może na czas określony zarządzić czynności, wcześniej jednak musi uzyskać pisemną zgodę właściwego miejscowo prokuratora okręgowego, chyba że stało się

[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 maja 2002 r. w sprawie szczególnych zasad i trybu wydawania, posługiwania się, przechowywania i ewidencji dokumentów, które uniemożliwiają ustalenie danych identyfikujących policjanta lub osobę udzielającą pomocy Policji oraz środków, którymi posługują się przy wykonywaniu zadań służbowych (DzU Nr 74, poz. 684).

[5] R. Zakrzewski, A. Woźniak, *Nowe metody operacyjnego działania Policji*, „Kontrola Państwowa" 1996, nr 4, s. 131.

to już niecelowe lub nie ma takiej możliwości bądź prokurator zarządził zaniechanie tych czynności.

Prokurator przed wydaniem pisemnej zgody zapoznaje się z materiałem będącym uzasadnieniem do przeprowadzenia wnioskowanych czynności. Czas, na jaki zarządza się czynności podejmowane celem przeprowadzenia zakupu kontrolowanego, nie może być dłuższy niż trzy miesiące. Czas stosowania zarządzonych czynności można przedłużyć na okres nie dłuższy niż kolejne trzy miesiące, jeżeli jest to celowe przy zastosowaniu odpowiedniej procedury, tj. na mocy kolejnego zarządzenia Komendanta Głównego Policji lub komendanta wojewódzkiego Policji, po uzyskaniu pisemnej zgody prokuratora.

Co istotne, takie przedłużenie możliwe jest tylko jednorazowo i tylko w razie pojawienia się nowych istotnych okoliczności dla sprawdzenia uzyskanych wcześniej, wiarygodnych informacji o przestępstwie oraz po ustaleniu sprawców i uzyskaniu dowodów przestępstwa można zarządzić kontynuację tych czynności na dalszy czas oznaczony.

Prokurator właściwy miejscowo na bieżąco informowany jest o wynikach przeprowadzonych czynności i w każdej chwili może zarządzić, aby zaniechano ich kontynuowania. W razie zgromadzenia dowodów umożliwiających wszczęcie postępowania karnego lub takich, które mają znaczenie dla toczącego się postępowania karnego, uzyskane materiały wraz z wnioskiem o wszczęcie postępowania przekazywane są prokuratorowi okręgowemu; materiały te wykorzystywane są z zastosowaniem art. 393 § 1 zd. 1 Kodeksu postępowania karnego.

Na podstawie art. 15 ust. 1 pkt 5a ustawy o Policji czynności związane z zakupem kontrolowanym mogą być niejawnie rejestrowane za pomocą urządzeń rejestrujących obraz lub dźwięk. Zgodnie z treścią art. 19a ust. 6 ustawy o Policji, który stanowi *lex specialis* w stosunku do art. 19 tej ustawy, ten sam organ może podjąć decyzję o przeprowadzeniu zakupu kontrolowanego oraz o rejestracji składających się nań czynności.

Zakup kontrolowany określany bywa również jako „operacja pod przykryciem", a funkcjonariuszy uczestniczących w czynnościach nazywa się „policjantami pod przykryciem", natomiast tych, którzy wykonują działania zlecone – „tajnymi agentami"[6]. Całe przedsięwzięcie wymaga zwykle wielu przygotowań i pracy, gdyż należy przeniknąć do wnętrza środowiska przestępczego, dokonać obserwacji, nawiązać kontakty, zebrać potrzebne informacje i rozpracować wybrane osoby. Operacje z wykorzystaniem tajnych agentów mogą przynieść efekty w postaci zebrania materiału dowodowego, którego uzyskanie w inny sposób byłoby niemożliwe lub bardzo uciążliwe[7]. Celem czynności wykonanych przez wprowadzenie tajnego agenta do środowiska przestępczego jest:

[6] A. Szumski, *Wykorzystanie taktyki i techniki kryminalistycznej w ramach czynności operacyjno-rozpoznawczych*, Oficyna Wydawnicza Arboretum, Wrocław 2010, s. 178–188.
[7] J. Kudła, Z. Bielecki, *Przyjęcie lub wręczenie korzyści majątkowej i zakup kontrolowany. Raport z badań (część jawna). Cz. 1*, „Policja" 2007, s. 73.

- ustalenie zakresu podmiotowego i przedmiotowego działalności rozpracowywanych grup,
- uprzedzenie planowanych przedsięwzięć przestępczych,
- zwerbowanie informatora,
- zebranie informacji o konkretnych przestępstwach,
- ułatwienie czynności związanych z konfiskatą ukrywanego przez przestępców mienia,
- zatrzymanie sprawców przestępstwa[8].

Przeprowadzenie operacji tego rodzaju wymaga zwykle dużego zaangażowania finansowego i organizacyjnego ze strony organów ścigania, ich olbrzymiego doświadczenia w zwalczaniu struktur przestępczych, doskonałych informatorów, perfekcyjnej ochrony dla policjantów działających pod przykryciem[9]. Wzięcie udziału w takich czynnościach wiąże się również z wysiłkiem osób w nich uczestniczących. Należy ciągle mieć na uwadze to, że mogą z tego przedsięwzięcia wyniknąć nieprzewidziane skutki. Często są nimi stres spowodowany takim działaniem oraz załamanie nerwowe, popadanie w alkoholizm, narkotyzowanie się czy wręcz identyfikacja ze swoją przestępczą tożsamością, dlatego też niezwykle ważną rolę odgrywa specjalistyczne szkolenie tajnych agentów[10].

Omawiając zakup kontrolowany, należy poruszyć jeszcze trzy istotne zagadnienia. Po pierwsze, zwrócić uwagę na szczególną ochronę, jaką objęte są osoby biorące udział w czynnościach, ale niebędące funkcjonariuszami. Wszelkie dane ich dotyczące i mogące je zidentyfikować stanowią informację niejawną z nadaną klauzulą „ściśle tajne", a ich ujawnienie może nastąpić jedynie w trybie wskazanym w art. 9 ustawy. Udział takich osób w czynnościach jest dobrowolny. Opcjonalnie przyznaje się im wynagrodzenie i w razie utraty życia lub zdrowia przysługują stosowne świadczenia odszkodowawcze. Jednakże wydaje się, że trudno przyjąć, iż taką osobę współpracującą, na wzór innych porządków prawnych, można byłoby nazwać „tajnym agentem". Polskie regulacje nie są wystarczające dla przyjęcia takiego wniosku.

Po drugie, pozostało jeszcze zagadnienie, na które należy tylko zwrócić uwagę, tj. art. 144 ustawy o Policji, który pozwala przyjąć, że osoba uczestnicząca w opisywanych czynnościach nie popełnia przestępstwa, a więc mamy tutaj do czynienia z ustawowym kontratypem. Kontratyp ten odnosi się również do przesyłki niejawnie kontrolowanej, o której mowa będzie w dalszej części pracy.

Po trzecie, niezmiernie istotne jest odpowiednie dokumentowanie zarządzanych czynności, określonych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji, a szczególnie w sprawach, w których miejscem dokonania czynu zabronionego jest Internet. Każdą z przeprowadzanych czynności dokumentuje się w postaci

[8] J. Kudła, B. Kupis, *Nowe uregulowania prawne dotyczące polskich działań pod przykryciem*, „Przegląd Policyjny" 2002, nr 3–4, s. 166.

[9] P. Podsiedlik, T. Czyłok, *Zakup kontrolowany, przyjęcie lub wręczenie korzyści majątkowej*, Wydawnictwo Szkoły Policji w Katowicach, Katowice 2012, s. 13.

[10] S. Waltoś, *Tajny agent (na obrzeżach odpowiedzialności karnej)*, „Państwo i Prawo" 1993, nr 11–12, s. 27.

notatki służbowej, a w razie potrzeby oddaje się do badań określonemu specjaliście. Co istotne, rejestrując każdą z czynności, wykonuje się również kopię tych rejestracji. Wszelkie materiały zawierające dowody przekazuje się organowi prowadzącemu postępowanie, a te, które ich nie zawierają, przechowuje przez dwa miesiące od dnia zakończenia lub zaniechania czynności. Następnie wydawane jest zarządzenie o protokolarnym, komisyjnym zniszczeniu zgromadzonych materiałów.

Zapisy utrwalone na nośnikach usuwa się w sposób uniemożliwiający odtworzenie tych zapisów z chwilą zniszczenia materiałów[11]. W przypadku gdy usunięcie z nośników utrwalonych na nich zapisów nie jest możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie albo dokonuje się ich fizycznego zniszczenia, przy zastosowaniu przepisów o ochronie informacji niejawnych[12].

Natomiast przesyłka niejawnie kontrolowana (inaczej nazywana również dostawą niejawnie kontrolowaną)[13], pomimo że funkcjonuje w naszym systemie prawnym od 20 lat, nie cieszy się dużym zainteresowaniem. Została wprowadzona w myśl zaleceń zawartych w Konwencji Narodów Zjednoczonych o zwalczaniu obrotu środkami odurzającymi i substancjami psychotropowymi z 1988 roku. W Polsce została wprowadzona ustawą z 21 lipca 1995 roku zmieniającą ustawę o urzędzie Ministra Spraw Wewnętrznych, o Policji, o Urzędzie Ochrony Państwa, o Straży Granicznej oraz niektóre inne ustawy. Zaliczana jest do taktycznych czynności operacyjno-rozpoznawczych[14] oraz metod szczególnych „ofensywnych"[15].

Czynności dokonywane w celu niejawnego kontrolowania przesyłki polegają na niejawnym nadzorowaniu wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia dla życia lub zdrowia ludzkiego. W ustawie w art. 19b ust. 1 wskazano również cele tych czynności, wymieniając:

- udokumentowanie przestępstw,
- ustalenie tożsamości osób uczestniczących w tych przestępstwach,
- przejęcie przedmiotów przestępstwa[16].

Obserwowanie odbywa się przy użyciu urządzeń technicznych utrwalających dźwięk lub obraz, a także przy użyciu urządzenia wykorzystującego *Global Positioning System – Navigation Signal Timing and Ranging* (GPS). Przesyłka okresowo może zostać wyłączona z obrotu, może również zostać otwarta celem sprawdzenia, oznakowania lub usunięcia przedmiotów lub zastąpienia ich innymi, a wszystko po to, aby ujawnić i utrwalić ślady kryminalistyczne.

---

[11] P. Podsiedlik, T. Czyłok, *Zakup kontrolowany*…, op. cit., s. 13.

[12] Tamże.

[13] A. Taracha, *Czynności operacyjno-rozpoznawcze: aspekty kryminalistyczne i prawnodowodowe*, Wydawnictwo Uniwersytetu Marii Skłodowskiej-Curie, Lublin 2006, s. 65-67.

[14] S. Pikulski, *Działania operacyjne policji*, „Wojskowy Przegląd Prawniczy" 1996, nr 2, s. 54.

[15] J. Kudła, *Wykorzystanie wyników czynności operacyjno-rozpoznawczych określonych w art. 19, 19a, 19b ustawy o Policji w postępowaniu karnym*, w: S. Lelental, J. Kudrelek, I. Nowicka (red.), *Czynności dochodzeniowo-śledcze i działania operacyjne policji a rola sądu w postępowaniu przygotowawczym*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2008, s. 246.

[16] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Zakamycze, Kraków 2006, s. 142–143.

Wyróżnia się kilka rodzajów przesyłek niejawnie nadzorowanych:
- „czyste", w których przedmiot przestępstwa w całości lub w części został w sposób tajny podmieniony na identyczny albo usunięty;
- „brudne", w których nadzoruje się przesyłkę w stanie nienaruszonym;
- dostawy wewnątrzkrajowe – nadzorowanie dotyczy terytorium tylko jednego państwa;
- dostawy międzynarodowe, transgraniczne;
- międzynarodowe „wewnętrzne", w tym przypadku informacje np. o przemycie uzyskały organy ścigania kraju docelowego, który jednocześnie podejmuje czynności koordynujące operację od kraju nadania (wysyłającego) przez kraje tranzytowe;
- międzynarodowe „zewnętrzne", gdy wiadomość o nielegalnej dostawie powzięły władze innych państw, nie docelowego, i wówczas one uzgadniają warunki bezpiecznego przebiegu dostawy kontrolowanej do kraju docelowego[17].

Zarządzenie o wdrożeniu niejawnego nadzorowania, wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa wydaje Komendant Główny Policji lub komendant wojewódzki Policji. Po wydaniu tego zarządzenia zobowiązany jest poinformować prokuratora okręgowego właściwego według siedziby zarządzającego organu Policji. Również tutaj prokurator w każdym czasie może nakazać zaniechanie czynności i musi być informowany na bieżąco o wynikach czynności. Inaczej niż przy zakupie kontrolowanym ustawodawca nie wskazał czasu, na jaki można zarządzić tę czynność, zapewne z powodu braku możliwości przewidzenia, jak długo będzie to konieczne. Odmienność stanowi również zastrzeżenie, że nie przeprowadza się tych czynności, jeśli istnieje zagrożenie dla życia i zdrowia ludzkiego. Tego zastrzeżenia należy przestrzegać również wtedy, gdy istnieje potencjalne zagrożenie.

Dla niektórych przedstawicieli doktryny przesyłka niejawnie kontrolowana stanowi odmianę zakupu kontrolowanego[18]. W tym przypadku dochodzi również najczęściej do nawiązania współpracy z innymi organami zarówno publicznymi, jak i prywatnymi (np. firmą kurierską) celem osiągnięcia zamierzonego celu. To jednak generuje dodatkowe zagrożenie dla powodzenia przedsięwzięcia. W wyniku przedsięwziętych czynności można doprowadzić do:
- zatrzymania sprawcy lub sprawców na gorącym uczynku, np. przemytu,
- przejęcia przedmiotów przestępstwa, np. alkoholu, broni,
- niedopuszczenia przedmiotów przestępstwa do dalszego obrotu,
- pełnego ustalenia odbiorców przedmiotów przestępstwa, np. paserów;
- likwidacji szlaków przemytniczych;
- ustalenia składu osobowego grup i związków przestępczych;

[17] D. Potakowski, *Nowe uprawnienia Policji w walce z przestępczością zorganizowaną*, „Przegląd Policyjny" 1996, nr 1–6, s. 90.
[18] A. Woźniak, R. Zakrzewski, *Nowelizacja ustawy o Policji – rozszerzenie uprawnień operacyjno-rozpoznawczych*, „Monitor Prawniczy" 1996, nr 1, s. 6.

– zebrania bardzo mocnego i należycie udokumentowanego materiału dowodowego jeszcze przed wydaniem postanowienia o wszczęciu postępowania przygotowawczego.

Przesyłka (dostawa) niejawnie kontrolowana jest działaniem podejmowanym w celu stwierdzenia tożsamości uczestników przestępstwa w sytuacji, gdy określone przedmioty są nielegalnie przemieszczane, przechowywane lub dochodzi do obrotu nimi. Zamiast zająć je natychmiast po stwierdzeniu, że pochodzą z przestępstwa, służba policyjna nadzoruje ich „ruch", by w rezultacie sporządzić dokumentację, mającą walor dowodowy w przyszłym procesie karnym. Przyjmuje się, iż w wielu przypadkach w celu potwierdzenia zasadności podjęcia niejawnej kontroli przesyłki niezbędne jest przeprowadzenie tajnego przeszukania[19].

Przykłady walki organów ścigania w Polsce i na świecie z siecią TOR

Tylko pozornie wydaje się, że nie jest możliwe dotarcie do użytkowników sieci TOR. Doskonałym przykładem możliwości przełamania anonimowości w tej sieci jest operacja przeprowadzona przez amerykańskie FBI, które po kilku miesiącach intensywnej pracy zatrzymało kilkadziesiąt osób zaangażowanych w działalność pedofilską w jej ramach.

W październiku 2013 roku amerykańskie służby federalne zamknęły pierwszy internetowy bazar, czyli serwis pod nazwą Silk Road, a w wyniku tych działań zatrzymano domniemanego założyciela serwisu Williama Ulbrichta oraz, na wniosek władz amerykańskich, 28-letniego Erika Eoina Marquesa (w Irlandii)[20]. W tym samym czasie doszło do zastanawiającego zbiegu okoliczności i zamknięcia wielu ukrytych serwisów, m.in. poczty Tormail i systemu płatności bitcoinowych Onionbank. Jak się okazało, FBI ustaliło IP osób odwiedzających witryny na serwerze Freedom Hosting, wykorzystując błąd w podstawowym oprogramowaniu (exploit 0-day Firefox 17).

Po roku te same służby odniosły kolejny sukces i ramach zakrojonej na szeroką skalę operacji doszło do zlikwidowania serwisów, w tym serwisu Silk Road 2.0, a tym samym zatrzymano domniemanego założyciela tego serwisu Blake'a Benthala, który powszechnie znany jest pod pseudonimem „Defcon". Został on oskarżony o utworzenie serwisu, który umożliwił ponad stu tysiącom osób prowadzenie transakcji kupna-sprzedaży narkotyków i innych nielegalnych towarów, np. sfałszowanych dokumentów. „Defcon" może zostać skazany nawet na karę dożywotniego pozbawienia wolności. Zgodnie z oficjalnym oświadczeniem nowojorskiego Prokuratora Generalnego obroty Silk Road 2.0 sięgały 8 mln dolarów miesięcznie.

Mowa tutaj o operacji „Onymous" przeprowadzonej w listopadzie 2014 roku, podczas której FBI zlokalizowało i zamknęło 410 serwisów w sieci TOR. Działalność tych serwisów związana była ze sprzedażą narkotyków, broni, fałszywych banknotów oraz kart kredytowych. Operacja została przeprowadzona w 16 krajach. Wzięły w niej udział następujące jednostki: European Cybercrime Centre (EC3) Europol, FBI,

[19] J. Widacki, *Kryminalistyka*, Wydawnictwo C.H. Beck, Warszawa 2012, s. 138.

[20] http://www.dobreprogramy.pl/FBI-triumfuje-najwiekszy-hosting-sieci-Tor-przejety-tysiace-uzytkownikow-zdemaskowanych,News,45424.html, stan na dzień: 14 kwietnia 2015 r.

Służby Imigracyjne i Celne USA (ICE) oraz Departament Bezpieczeństwa USA. Jak się przypuszcza, w tej sprawie wiele zawdzięczać można eksperymentowi wykonanemu przez ekspertów z CERT University Carnegie Mellon, którzy wykorzystali w tym celu 115 bardzo szybkich serwerów. Ich eksperyment polegał na oznaczeniu w sieci pewnych elementów i identyfikacji ich drogi od nadawcy do odbiorcy. Eksperyment trwał od stycznia do lipca 2014 roku. W lipcu serwery te zostały wyłączone. Stanowi to doskonały przykład zastosowania niejawnego nadzorowania przesyłki. Wspomniani eksperci wystąpili na konferencji Black Hat w 2014 roku, opisując mechanizm tego doświadczenia. W swoim wystąpieniu poinformowali: „In our analysis, we've discovered that a persistent adversary with a handful of powerful Server and a coupe gigabit links can deanonymize hundreds of thousands TOR clients and thousands of hidden services within a couple of months. The total investment cost? Just under $3,000"[21]. Tłumacząc ich wypowiedź, należy stwierdzić: „odkryliśmy, że zdeterminowany atakujący, dysponujący kilkoma serwerami dużej mocy i kilkoma połączeniami o przepuszczalności kilku gigabitów, może w ciągu paru miesięcy odkryć tożsamość setek tysięcy klientów sieci TOR oraz tysięcy ukrytych serwerów. Całkowity koszt inwestycji? Niecałe 3000 dolarów". Zaskakuje zarówno prostota podejścia do problemu, jak i skala skuteczności.

Po ujawnieniu informacji o przeprowadzonej operacji magazyn „The Economist" stwierdził, że zlikwidowane serwisy wraz z serwisem Silk Road 2.0 obsługiwały 30% rynku, gdyż od czasu Silk Road 1.0 pojawiły się nowe. Wbrew temu, co utrzymuje FBI, nie zlikwidowano głównego ośrodka internetowego handlu niedozwolonymi towarami. Prawdą jest jednak, że doszło do zlikwidowania jednego ze znaczących centrów. Natomiast w dzienniku „The Washington Post" opublikowano krytyczny artykuł o działaniach FBI, w którym stwierdzono, że operacja uwieńczona sukcesem spowoduje wzrost zagrożenia przestępczością narkotykową na ulicach miast, gdyż dzięki przeniesieniu się nielegalnego handlu z ulicy do sieci te zagrożenia w rzeczywistym świecie się zmniejszyły.

FBI ujawniło przykłady zamkniętych w wyniku operacji serwisów, tj.:

- „Pandora" (pandora3uym4z42b.onion), „Blue Sky" (blueskyplzv4zv4fsti.onion) będące sklepami z narkotykami,
- „Executive Outcomes" (http://iczyaan7hzkyjown.onion) będący sklepem z bronią,
- „Fake Real Plastic" (http://igvmwp3544wpnd6u.onion) będący sklepem z kartami kredytowymi,
- „Fast Cash!" (http://5oulvdsnka55buw6.onion) handlujący fałszywymi banknotami.

Zamknięte serwery znajdowały się w Bułgarii, Czechach, Finlandii, Francji, Niemczech, na Węgrzech, w Irlandii, na Łotwie, Litwie, w Luksemburgu, Holandii, Rumunii, Hiszpanii, Szwecji, Szwajcarii i w Wielkiej Brytanii. Dziwi fakt, że lista ta nie uwzględnia np. Rosji.

Aby zniwelować ryzyko objęcia pozycji „stanowiska wyjściowego", czyli najbardziej narażonego na ujawnienie IP, specjaliści polecają takie skonfigurowanie

[21] http://www.belowgotham.com/Tor-trust.pdf, stan na dzień: 14 kwietnia 2015 r.

ruchów stacji roboczej, aby możliwy był jedynie ruch wyjściowy przez Proxy do sieci TOR. W tym celu istnieje możliwość skorzystania z gotowej konfiguracji dystrybucji Tails. Szczególnie narażeni na różne niebezpieczeństwa, jakie wiążą się z siecią TOR, są użytkownicy urządzeń mobilnych, tj. telefonów i tabletów, gdyż w ich przypadku łatwiejsze pozostaje ustalenie tożsamości. Taka możliwość zwiększa się zwłaszcza w razie umieszczenia w kodzie strony obiektu wideo lub audio w standardzie HTML5 z opcją autoodtwarzania. Ta czynność powoduje, że program uruchomi bez wcześniejszego zapytania wewnętrzny odtwarzacz, który łączy się z siecią, ignorując ustawienia Proxy i przekierowując ruch do sieci TOR[22]; w ten sposób umożliwia ujawnienie prawdziwego adresu IP użytkownika urządzenia mobilnego.

Na początku 2014 roku Kaspersky Lab poinformował, że odkryto ponad 900 usług rozsyłających *malware* z sieci TOR.

W 2014 roku również w Polsce doszło do rozesłania z sieci TOR wiadomości mailowych zawierających fałszywe alarmy bombowe. Jednak specjaliści zakładają, że policji nie udałoby się ustalić tożsamości ich nadawcy, gdyż pomimo iż doszło do zatrzymania osoby podejrzanej o nadanie tych alarmów dzięki połączeniu ze sobą wszystkich istotnych okoliczności dotyczących poszczególnych zdarzeń, dopiero po kilku dniach do tych czynów przyznała się inna osoba, która sama określała się mianem „CyberBrevika"[23]. W związku z tym zatrzymano kolejnego podejrzanego. Przypuszcza się, że ten pierwszy podejrzany został zatrzymany na podstawie wyciągnięcia przez policję zbyt pochopnych wniosków.

Bardzo często przedmiotem transakcji w sieci TOR stają się konta na Allegro posiadające dużą liczbę pozytywnych komentarzy czy też konta bankowe ze zgromadzonymi środkami finansowymi.

Innym obrazowym przykładem problemu z siecią TOR jest zdarzenie z lutego 2014 roku, kiedy to umieszczono w niej materiały o jednym z kapitanów ABW, który był w przeszłości ekspertem wydziału bezpieczeństwa teleinformatycznego. W sieci tej dostępne były jego pełne dane osobowe, łącznie ze zdjęciem, numerem PESEL oraz informacjami o jego rodzinie. Dowodzi to, że wiele ze skradzionych danych gromadzonych jest właśnie w sieci TOR i tam są one wykorzystywane do przestępczych celów.

Podsumowanie

Pomimo złej reputacji, jaką obecnie cieszy się sieć TOR, pozostaje ona nadal w oczach wielu symbolem wolności i wzorcem w dążeniu do ochrony prywatności w ramach komunikacji internetowej.

Przykładami pozytywnych skutków jej funkcjonowania są przykładowo dostęp do Internetu użytkowników będących dziennikarzami w krajach, gdzie sieć poddawana jest cenzurze, dostęp do Internetu osób przebywających na urlopie w krajach,

[22] http://zaufanatrzeciastrona.pl/post/korzystasz-z-sieci-tor-na-telefonie-lepiej-uwazaj/, stan na dzień: 14 kwietnia 2015 r.

[23] http://wyborcza.pl/1,75478,16404430,CyberBrevik__To_ja_wyslalem_maile_o_bombach__W_areszcie.html, stan na dzień: 14 kwietnia 2015 r.

w których istnieją ograniczenia ze względu na ich położenie geograficzne czy też ochronę przed poniesieniem odpowiedzialności za działalność w Internecie klientów różnych instytucji, np. hoteli.

Liczyć należy na to, że w przyszłości wzrośnie skala działań podejmowanych na rzecz przeciwdziałania problemom pojawiającym się w związku z funkcjonowaniem sieci TOR i dzięki temu uda się uniknąć wielu niebezpiecznych zdarzeń, do których aktualnie dochodzi za pośrednictwem tej sieci. Pocieszające wydaje się to, że szybki postęp technologiczny sprzyja nie tylko przestępcom, lecz także organom ścigania, i wszyscy spodziewamy się, że w przyszłości eksperci znajdą sposób na zniwelowanie zagrożeń płynących z tej sieci. Już teraz bowiem docierają do nas niepotwierdzone jeszcze informacje o tym, że FBI posiada *malware* pozwalający namierzyć użytkowników sieci TOR, czyli przypuszczać można, że jesteśmy coraz bliżej kresu bezkarności jej użytkowników.

Streszczenie

W związku z pojawieniem się nowego zagrożenia, jakim jest anonimowa sieć TOR, występuje coraz więcej problemów wynikających z przekształcenia jej w narzędzie wyrafinowanych przestępców. W założeniu celem twórców tej sieci było ułatwienie dostępu do informacji zawartych w sieci komputerowej tym, którzy mieszkają w państwach, gdzie Internet jest cenzurowany, np. dla dziennikarzy w Korei. Stało się jednak inaczej i aktualnie siecią tą posługują się głównie złodzieje, hakerzy, handlarze narkotyków i pedofile. Organy ścigania zdają sobie sprawę z płynącego stąd zagrożenia i podejmują działania w celu wykrywania sprawców przestępstw, których źródło pochodzi z sieci TOR, np. poprzez zakup kontrolowany. Choć jest to niezmiernie trudne, to zagraniczne służby odnoszą sukcesy. Pocieszające wydaje się to, że szybki postęp technologiczny sprzyja nie tylko przestępcom, lecz także organom ścigania, i wszyscy spodziewamy się, że w przyszłości eksperci znajdą sposób na zniwelowanie zagrożeń płynących z tej sieci.

Słowa kluczowe: sieć TOR, anonimowa sieć, zakup kontrolowany, przesyłka niejawnie nadzorowana

Summary

With the new threat which is anonymity network TOR appeared a huge number of problems which are connected with a transformation of this new network as a tool for sophisticated offenders. The creator of this specific network wanted to make easier to have an access to Internet by people in same countries which decided to censor e.g. for journalists from North Korea. But we have now different reality and the TOR is currently using by thieves, hackers, drug dealers and paedophiles who are dealing with this network. The law enforcement agencies realized that it is a very dangerous threat and they are making an effort to descry a real offenders of these crimes which source comes from the TOR e.g. through a sting operation. It is extremely difficult, however the overseas services are getting off the ground. It is comforting that a quick technological development encourage offender but the law enforcement agencies as well, and we expected that in future the experts will find a way to level this threat which is deriving from the TOR.

Keywords: TOR network, anonymity network, sting operation, controlled delivery

Diana Kazimierska

METODY WERYFIKACJI SPORNYCH OSIĄGNIĘĆ ALPINISTYCZNYCH

Methods of verification of disputed achievements in mountaineering

W artykule zostanie przedstawiony temat ustalania spornych osiągnięć w sporcie, który jeszcze w ubiegłym wieku uznawano za elitarny. Fundamentem uprawiania alpinizmu był jego etos[1] i zasady etyki, które nakazywały ufać oświadczeniom alpinistów – weryfikacja tych oświadczeń nie stanowiła bezwzględnie obowiązującej reguły. Jest to jedna z przyczyn tego, że do dzisiaj nie istnieją jasne procedury i zasady uznawania osiągnięć sportowych w alpinizmie[2]. Drugą z przyczyn jest specyfika środowiska naturalnego, w jakim uprawiany jest ten sport.

Na wstępie należy zaznaczyć, że rozważania poniższe ograniczone będą do alpinizmu wysokościowego, tj. zdobywania szczytów w górach wysokich oraz przeprowadzania i pokonywania dróg wspinaczkowych w naturalnym terenie. Poniższe uwagi nie dotyczą natomiast wspinaczki sportowej, szczególnie tej uprawianej na sztucznie zbudowanych formacjach i w ramach zawodów. Ograniczenie to jest uzasadnione tym, iż akurat ten obszar działalności sportowej, wywodzący się z tradycyjnie rozumianego alpinizmu, dopracował się precyzyjnych norm i uregulowań[3].

---

[1] Alpinizm (taternictwo, himalaizm) można rozumieć jako sposób życia. Podejmowanie wyzwań i dokonywanie kolejnych wyczynów może być utożsamiane z pokonywaniem własnych słabości. Oszustwo, przypisywanie sobie osiągnięć, których się nie dokonało, jest więc równoznaczne z „oszukiwaniem samego siebie".

[2] Wartość sportową danych osiągnięć można powiązać z historyczną ewolucją alpinizmu. W pierwszym etapie wartość miało wejście na szczyt – najprostszą, najbardziej dogodną i oczywistą drogą. Znaczące były takie wyczyny, jak zdobycie np. najwyższego wierzchołka w danym masywie górskim, na danym kontynencie. Następnie wartościowe stało się zdobywanie szczytów trudniejszymi drogami oraz pokonywanie tych trudności w konkretnych warunkach bądź w określonym stylu (np. pierwsze zimowe wejście na dany szczyt, wejście bez sztucznych ułatwień, bez użycia tlenu z butli, zdobycie ośmiotysięcznika w stylu „alpejskim"). Rozwój alpinizmu, a także związane z osiągnięciami alpinistycznymi zainteresowanie mediów, doprowadziło do powstania specyficznych „konkurencji", polegających np. na zdobywaniu „Korony Himalajów", tj. wejściu na wszystkie ośmiotysięczniki przez jedną osobę.

[3] Zgodnie z treścią pkt 6 Statutu Polskiego Związku Alpinizmu, alpinizmem są „wszelkie sporty wymagające umiejętności wspinaczkowych" (Statut PZA opublikowany jest na stronie www.pza.org.pl).

Weryfikacja spornych oświadczeń i w związku z tym ustalanie faktów, mających znaczenie (nie tylko dla ograniczonej społeczności), to zagadnienia, w których można dostrzec problem kryminalistyczny. Rezultatem przeprowadzonego postępowania „weryfikującego" powinno być potwierdzenie jednej z wersji – czy deklaracja alpinisty, odnosząca się do danego wyczynu sportowego, odpowiada prawdzie, czy też alpinista niesłusznie przypisuje sobie dane osiągnięcie.

Wykorzystanie wiedzy wypracowanej w ramach kryminalistyki może być pomocne dla tej weryfikacji.

Znajomość zagadnień związanych z psychologią zeznań i wyjaśnień (dotyczących m.in. uzyskiwania i zachowywania w pamięci odtwarzanych spostrzeżeń) oraz taktyki przesłuchań (wraz z etapem przygotowywania się do odbioru depozycji osób przesłuchiwanych) może zostać wykorzystana w celu kontroli oświadczenia alpinisty. Należy wskazać, iż odbierający deklarację alpinisty powinien przygotować się do tej rozmowy, podobnie jak osoba, która przygotowuje się do przesłuchania – „weryfikator" powinien m.in. zapoznać się ze szczegółami topografii miejsca (drogi), której przejście alpinista deklaruje, jak również dysponować innymi informacjami, które pozwolą mu ocenić, czy deklaracje alpinisty są szczere.

Zdjęcia i filmy, które przedstawiane są przez alpinistów na dowód tego, iż byli w zadeklarowanym miejscu (np. na wierzchołku góry), są poddawane analizie, przypominającej znane z praktyki kryminalistycznej badania porównawcze. Do badań tych wykorzystywany jest materiał „dowodowy" – tj. fotografia wykonana przez alpinistę (np. tzw. zdjęcie szczytowe) – oraz materiał „porównawczy", w postaci fotografii i filmów wykonanych (niespornie) w miejscu, które zostało zadeklarowane przez alpinistę jako miejsce wykonania fotografii.

Czynności wykonywane przez weryfikatorów mogą również przypominać oględziny bądź wizję lokalną (przeprowadzaną na miejscu spornego osiągnięcia). Dla prawidłowego przygotowania i przeprowadzenia tych czynności wiedza z zakresu kryminalistyki wydaje się niezbędna.

Poniżej przedstawione zostaną sposoby weryfikacji spornych oświadczeń alpinistów, wraz z ilustrującymi je przykładami autentycznych historii.

Analiza oświadczenia alpinisty

Pierwszym dającym się wyodrębnić sposobem wykazania danego dokonania alpinistycznego była (i pozostaje nadal) deklaracja samego alpinisty. Weryfikacja jej nabiera wyjątkowego znaczenia w sytuacjach, gdy osiągnięcie nie zostało udokumentowane w żaden inny sposób (szczególnie wtedy, gdy wyczyn realizowany był samotnie). Weryfikacja opiera się na założeniu, że przejście danej drogi jest doświadczeniem, które każdy alpinista powinien umieć opisać. W tej relacji nie powinno zabraknąć szczegółów, dzięki którym możliwa byłaby identyfikacja konkretnych, mających znaczenie miejsc (np. wierzchołka zdobytej góry, jego bezpośredniego otoczenia), i to nie tylko topografii, ale również śladów pozostawionych ewentualnie przez innych alpinistów. Znajomość tych szczegółów może świadczyć, że dana osoba znajdowała się w opisywanym przez siebie miejscu, natomiast opis niezgodny

z rzeczywistością może stać się jednym z argumentów, które będą przemawiały za nieuczciwym przypisywaniem sobie osiągnięcia.

Wydaje się, że pretendująca do miana „pierwszej kobiety, która zdobyła wszystkie czternaście ośmiotysięczników" Koreanka Oh Eun-Sun nie przeszła pozytywnie tej weryfikacji. W 2009 r. pani Oh miała zdobyć Kanczendzongę. Alpiniści, którzy w tym czasie zdobyli szczyt, widzieli tam puste butle tlenowe (niektórzy je sfotografowali). Koreanka, relacjonując swoje wejście, powiedziała, że nie widziała ich, jednak po pewnym czasie oświadczyła, że „nie wie, czy je widziała, bo tego nie pamięta". Zarzucono jej zatem, że nie weszła na sam wierzchołek, czego dowodzić miało również przedstawione przez nią zdjęcie „szczytowe", które wykonano znacznie poniżej wierzchołka. Wyczyn Koreanki zakwestionowała m.in. Elizabeth Hawley[4] – autorytet w sprawach wejść na szczyty w Himalajach. Ostatecznie oficjalnie[5] uznano, iż pierwszą kobietą, która zdobyła Koronę Himalajów, jest Baskijka Edurne Pasaban[6]. Nie wszyscy jednak uznają ten werdykt za sprawiedliwy[7].

Istotnymi okolicznościami, które mogą być pomocne w ocenie wiarygodności deklaracji alpinisty, są np. jego postępowanie po powrocie z wyprawy oraz analiza jego wcześniejszych dokonań.

Tomo Cesen urażony tym, że zwątpiono, iż pokonał samotnie północną ścianę Lhotse (w 1990 r.), przekazał do publikacji w czasopiśmie zdjęcia, które miały dokumentować to osiągnięcie. Fotografie (slajdy) zostały jednak rozpoznane przez innego alpinistę jako zrobione przez niego na zachodniej ścianie Lhotse[8]. Cesen nie potrafił w przekonujący sposób wytłumaczyć tej sytuacji – należy podkreślić, że przed zakwestionowaniem tego, iż jest autorem zdjęć, nie wspomniał, że nie są jego autorstwa. Przeciwko Cesenowi przedstawiano również takie zarzuty, jak: wcześniejsze wątpliwości dotyczące przejścia zadeklarowanych dróg, niesłychanie (niewiarygodnie) szybka aklimatyzacja w związku ze zdobyciem Lhotse oraz to, że wyczyn, którego miał dokonać, został przeprowadzony wyjątkowo szybko i sprawnie (co również miało świadczyć przeciwko jego wiarygodności). Relacja Cesena ze szczytu korespondowała natomiast z relacjami innych alpinistów, którzy w tym czasie zdobyli wierzchołek Lhotse – Cesen opisał znajdujące się tam w tym czasie butle tlenowe. W tej sprawie wypowiedział się m.in. R. Messner, uznając, że sam opis szczytu nie jest dostatecznym argumentem przemawiającym na korzyść alpinisty – Cesen

[4] Sama E. Hawley mówi o sobie: „nie jestem arbitrem sportowym ani sędzią, a jedynie archiwistką zbierającą sprawozdania alpinistów" (R. Messner, *Na szczycie – kobiety na górze*, Wydawnictwo Stapis, Katowice 2012, s. 17).

[5] „Śledztwo" w tej sprawie prowadziły portal Explorersweb i południowokoreańskie Ministerstwo Sportu.

[6] J. Kurczab, *Oh Eun-Sun traci pierwszeństwo, Edurne Pasaban na tronie* (artykuł opublikowany na portalu wspinanie.pl, 14 grudnia 2010 r.).

[7] Wypowiedział się w tej sprawie R. Messner; uznał on, że kwestionowanie wyczynu Koreanki jest spowodowane brakiem akceptacji stylu, w którym się wspinała, oraz chęcią, aby w konkurencji zwyciężyła Europejka (Edurne Pasaban). Messner orzekł, że „rzetelność Miss Oh jest poza dyskusją" (R. Messner, op. cit., s. 32, 224–251).

[8] Wiadomo, jak Cesen wszedł w ich posiadanie – pożyczył je od żony autora zdjęć.

mógł się od kogoś dowiedzieć, co znajduje się na wierzchołku czwartej góry świata. Zwolennicy Cesena uważają, że argumenty przeciwko niemu są nieprzekonujące, a ci, którzy kwestionują jego osiągnięcia, z góry zakładają, że nie mógł on dokonać czynów spektakularnych, przerastających wyobrażenia innych[9].

Tego typu weryfikacje nie są typowe wyłącznie dla współcześnie rozgrywających się wydarzeń – gdy zaczęto wątpić w wiarogodność Fredericka A. Cooka, który w 1906 r. ogłosił[10], iż jest pierwszym zdobywcą Mount McKinley, podjęto analizę jego pisemnych relacji z wyprawy. Zauważono m.in., iż opis drogi, którą miał pokonać, jest dokładny, precyzyjny i zgodny z późniejszymi doświadczeniami innych alpinistów, lecz wyłącznie do pewnego miejsca – ujścia Ruth Gorge. Dalej trasa, którą opisuje Cook, nie odpowiada ani opisom, ani zdjęciom wykonanym przez późniejszych zdobywców tej góry (dowodem, który jednak ostatecznie pogrążył Cooka, była analiza przedstawionych przez niego fotografii z wyprawy, o czym będzie mowa w dalszej części artykułu)[11].

„Fanty" na szczycie

Zwyczaj zostawiania przedmiotów (bądź znoszenia ich ze szczytu przez kolejnych zdobywców) jest jednym z pierwszych klasycznych sposobów udowadniania wejść alpinistycznych.

W 1981 r. nepalskie Ministerstwo Turystyki nie uznało samotnego (i bez użycia tlenu z butli) wejścia Jerzego Kukuczki na Makalu, uznając, iż wyczyn ten jest niewiarygodny. Alpinista musiał poczekać na uznanie swojego osiągnięcia. Rok później koreańska wyprawa, która zdobyła Makalu, odnalazła tam „czerwonego żółwia w kropki" (maskotkę – biedronkę, którą zostawił Kukuczka na szczycie). W ten sposób wejście na Makalu polskiego alpinisty zostało potwierdzone[12].

Pozostawienie śladów aktywności wspinaczkowej

Pozostawienie (w sposób niezamierzony) śladów działalności alpinistycznej może być wartościowym dowodem przejścia danej drogi (szczególnie w dotąd nieeksplorowanym terenie), natomiast brak jakichkolwiek śladów – świadczyć o mistyfikacji.

Do 2005 r. nikt w sposób stanowczy i otwarty nie zakwestionował (wątpliwego jednak wcześniej) zdobycia w 1959 r. patagońskiej iglicy Cerro Torre przez włoskiego wspinacza Cesare Maestriego. W 2005 r. wyprawa, która miała ambicje powtórzyć jego wyczyn, odnalazła ślady wspinaczki Maestriego (i jego towarzysza Toniego Eggera, który według relacji Maestriego zginął po zdobyciu

[9] J. Radziejowski, *Najbardziej znane kontrowersje w historii alpinizmu*, „Góry" 2010, nr 4; W. Słowakiewicz, P. Turkot, *Tomo Cesen – zdobywca czy mistyfikator*, „Góry" 1994, nr 11.

[10] Cook opisał swoje osiągnięcie w czasopiśmie „Harper's Monthly Magazine" oraz wydał książkę, w której zamieścił relację z wyprawy.

[11] J. Radziejowski, op. cit., s. 26.

[12] Historia ta została opisana m.in. w książce: J. Kukuczka, *Mój pionowy świat*, Mac System, Katowice 2008.

iglicy), ale do pewnego miejsca – trójkątnego pola śnieżnego w dolnej części ściany. Powyżej tego miejsca nie odnaleziono niczego, co świadczyłoby o tym, że szczyt został wcześniej zdobyty – nie było śladów po boltach, śrubach lodowych i hakach, które powinny pozostać po niezbędnej na tej drodze asekuracji i po zjazdach. Wątpliwości w sprawie Cerro Torre wzmacniał fakt, iż Maestri, pomimo że na wspinaczkę zabrał aparat fotograficzny, nie posiadał zdjęcia szczytowego. Alpinista tłumaczył, że aparat zaginął wraz z jego towarzyszem. Gdy jednak odnaleziono ciało Toniego Eggera, nie było przy nim aparatu. Kolejnym argumentem przemawiającym za mistyfikacją jest to, że opis drogi przedstawiony przez Maestriego nie zgadza się z doświadczeniami wszystkich innych zespołów, które próbowały zdobyć iglicę[13].

Dokumentacja zdjęciowa (filmowa) i jej weryfikacja

Zdjęcie wykonane przez alpinistę w zadeklarowanym przez niego miejscu, np. na wierzchołku zdobytej góry, powinno przedstawiać topografię terenu, która jest z niego widoczna. Wydawać by się mogło, że taka fotografia to najbardziej wiarygodny dowód, jaki można przedstawić na potwierdzenie swoich dokonań[14]. Zdobycie Annapurny w 1991 r. przez Wandę Rutkiewicz zostało udokumentowane w ten właśnie sposób. Alpinistce udało się wywołać zdjęcie (wykonane o zmierzchu, w bardzo złych warunkach atmosferycznych) zrobione na wierzchołku tego ośmiotysięcznika. Fotografia, po przeprowadzeniu stosownej analizy, stała się dowodem jej wiarygodności. Rutkiewicz podjęła walkę o swoje dobre imię po tym, jak zarzucono jej, iż – wbrew swojej deklaracji – nie weszła na wierzchołek. Po przeprowadzonym przez Polski Związek Alpinizmu (na jej wniosek) postępowaniu uznano, iż szczyt zdobyła. Wybitna himalaistka musiała jednak przedstawić na to dowód (np. zdjęcie), ponieważ samo jej oświadczenie okazało się niewystarczające[15].

Analiza zdjęcia mająca zweryfikować jego autentyczność[16] polega najczęściej na przeprowadzeniu typowych badań porównawczych. Porównywane są zdjęcia wykonane przez alpinistę z fotografiami wykonanymi z tego samego miejsca co zadeklarowane przez alpinistę, których autentyczność nie jest kwestionowana. W badaniach istotna jest zbieżność charakterystycznych szczegółów topografii terenu oraz brak

[13] Bardziej wyczerpującą relację tej historii można odnaleźć w: M. Wilanowski, *Ważne postacie alpinizmu. Cesare Maestri – Pająk Dolomitów* (artykuł zamieszczony na portalu wspinanie.pl, 16 sierpnia 2011 r.); *Puzzle na Cerro Torre ułożone? Nowe odkrycie w sprawie sprzed 50 lat* (artykuł zamieszczony na portalu wspinanie.pl, 2 lutego 2015 r.). Natomiast obszerne relacje z wyprawy (autorstwa C. Maestriego) zostały zamieszczone w miesięczniku „Góry" 1996, nr 3, s. 16–19.

[14] Jednak nie może to być aż tak oczywiste, chociażby z tego powodu, iż zostały już opisane przypadki posłużenia się zdjęciem wykonanym przez inną osobę jako ilustrującym własne dokonania.

[15] B. Rusowicz, *Wszystko o Wandzie Rutkiewicz*: *wywiad [rzeka] Barbary Rusowicz*, Comer – Ekolog, Toruń–Piła 1992, s. 165.

[16] Rozumianą tutaj jako wykonanie zdjęcia z określonego, zadeklarowanego miejsca.

różnic, chyba że te różnice można wytłumaczyć np. inaczej kształtującą się pokrywą śnieżną związaną ze zmianą warunków atmosferycznych bądź faktem, iż zdjęcie dowodowe i weryfikujące (porównawcze) zostało wykonane z nieco innego miejsca bądź pod innym kątem. Badania mogą również zmierzać do wykazania, że zdjęcie zrobiono z innego miejsca niż deklarowane – zdjęcie dowodowe porównywane jest z wykonanym w miejscu wytypowanym jako to, w którym faktycznie zostało ono zrobione (np. poniżej szczytu).

Tego typu weryfikacje przeprowadzono m.in. w sprawie Oh Eun-Sun (Kanczendzonga), Christiana Stangla (K2) oraz F.A. Cooka (McKinley).

Koreanka Oh Eun-Sun nie od razu przyznała, że przedstawione przez nią zdjęcie dokumentujące zdobycie Kanczendzongi wykonano poniżej szczytu. Najpierw zostało przeprowadzone śledztwo i analiza porównawcza przedstawionej przez nią fotografii. Na zdjęciu pani Oh widoczne są skały (podczas gdy wierzchołek góry pokryty jest całkowicie śniegiem). Dzięki analizie charakterystycznych cech widocznej na zdjęciu skały udało się zidentyfikować miejsce, w którym wykonano fotografię. Ekspertem był Tom Holzel[17], a jako materiał porównawczy wykorzystano m.in. (udoskonalone cyfrowo) zdjęcia autorstwa Krzysztofa Wielickiego oraz film Kingi Baranowskiej ze szczytu. Badacz stwierdził, że zdjęcie najprawdopodobniej zrobiono na wysokości 8300 m n.p.m. (na pewno nie bliżej niż 50 metrów od szczytu). Oh Eun-Sun tłumaczyła później, iż rzeczywiście zostało ono wykonane niżej, ze względu na złą pogodę panującą na szczycie. Przeciwko Koreance świadczyć miały jednak również: nieścisłości w słowach towarzyszących jej Szerpów, wątpliwości dotyczące flagi, którą miała zatknąć na szczycie (nie odnaleziono jej tam), oraz wspomniane już zastrzeżenia dotyczące jej relacji z wierzchołka[18].

Po przeprowadzeniu analizy zdjęć szczytowych Stangla, który deklarował zdobycie K2, uznano, iż zostały one wykonane na wysokości 7500 m n.p.m., tj. ponad tysiąc metrów poniżej wierzchołka[19]. Po przedstawieniu opinii dotyczącej autentyczności zdjęcia szczytowego Stangl zachował się nietypowo – przyznał się do winy. Interesujące było podane przez niego uzasadnienie postępowania: obawa przed niepowodzeniem „w środowisku zorientowanym na sukces" oraz chęć przełamania złej passy po wielu nieudanych sezonach i porażkach (siedmiu) związanych z próbami zdobycia tej góry. Można przypuszczać, że nie bez znaczenia było również to, iż alpinista ten był w środowisku postacią rozpoznawalną i korzystającą ze wsparcia sponsorów[20].

---

[17] Badacz historii zaginięcia Ivine'a i Mallory'ego.

[18] J. Kurczab, op. cit.; *Koreańska Federacja Alpinistów kwestionuje wejście Oh Eun-Sun na Kanczendzongę w 2009 roku!* (artykuł zamieszczony na portalu drytooling.com.pl, 31 sierpnia 2010 r.).

[19] Jako materiał porównawczy posłużyły zdjęcia wykonane przez Jima Haberla, opublikowane w książce poświęconej K2. Zdjęcia porównawcze zostały zrobione z obozu III, który znajdował się na wysokości ok. 7500 m n.p.m.

[20] J. Radziejowski, op. cit.; *Kłamiesz, nie było cię tam!* (artykuł zamieszczony na portalu onet.sport.pl, 19 grudnia 2011 r.).

W przypadku analizy zdjęć wykonanych przez F.A. Cooka ustalono, że fotografie, które zgodnie z jego oświadczeniem przedstawiać miały wierzchołek najwyższego szczytu Ameryki Północnej, pokazują zupełnie inne miejsce, inny wierzchołek, inną górę, która nawet została ochrzczona przez weryfikatorów jako Fake Peak (Fałszywy Szczyt). Szczyt ten leży w dużej odległości od Mount McKinley (1600 metrów w linii prostej), w związku z tym przedstawienie zdjęcia z Fake Peak jako tego, które miało dokumentować powodzenie wyprawy, uznano za argument przemawiający za mistyfikacją.

Wyprawy weryfikacyjne i ich zadania

W przypadku braku dostatecznych danych, które umożliwiłyby weryfikację deklaracji alpinisty, konieczne może być zebranie dowodów w miejscu spornego osiągnięcia. Dokonanie takiej wizji lokalnej ma bogatą tradycję oraz nazwę – wyprawa weryfikacyjna. Takie wyprawy były organizowane np. w sprawie zdobycia szczytu McKinley przez F.A. Cooka[21].

Jednym z podstawowych zadań uczestników wypraw weryfikacyjnych jest zebranie materiału porównawczego, niezbędnego do analizy zdjęć, które zostały przedstawione jako dowód mający potwierdzić alpinistyczne osiągnięcie.

Bardzo interesującym przykładem wyprawy weryfikacyjnej jest przeprowadzona z inicjatywy Polskiego Związku Alpinizmu wyprawa na Grenlandię w 2012 r. Potrzeba zorganizowania ekspedycji powstała z powodu narastających kontrowersji wokół wyczynu pary polskich alpinistów (Elizy i Dawida) na Grenlandii w 2007 r.

Relację z wyprawy Eliza i Dawid zamieścili w miesięczniku „Góry"[22] oraz w sprawozdaniu przygotowanym dla PZA. Z opisu alpinistów wynika, iż wyprawa obfitowała w niezwykłe trudności związane z działaniem w nieeksplorowanym dotychczas terenie, uwieńczone wytyczeniem drogi wspinaczkowej o imponujących (zadeklarowanych w sprawozdaniach) trudnościach. Elizie i Dawidowi wręczono „Jedynkę" – nagrodę za wybitne osiągnięcia sportowe, przyznawaną przez środowisko alpinistów. Wspomnieć również należy, że wyprawa była częściowo finansowana przez Polski Związek Alpinizmu. Źródłem wątpliwości dotyczącej wartości dokonań alpinistów początkowo stała się książka, w której w krytycznym tonie zdano relację z wyprawy. Autorka książki pojechała na Grenlandię po to, aby pomóc Elizie i Dawidowi w realizacji filmu (m.in. z przejścia ściany), jednak ostatecznie postanowiła stanowczo ich skrytykować. W książce pt. *Sekretne życie motyli* zostały sformułowane wobec wspinaczy takie zarzuty, jak: przeszacowanie wartości eksploracyjnej wyprawy oraz zawyżenie trudności przeprowadzonej drogi wspinaczkowej (nazwanej Golden Lunacy)[23].

[21] Wyprawy weryfikacyjne były organizowane zarówno zaraz po ogłoszeniu sukcesu przez F.A. Cooka, jak i współcześnie – w 1994, 2005 i 2006 r. Podejmowali je przeciwnicy i zwolennicy podróżnika w celu zebrania argumentów potwierdzających zdobycie przezeń Mount McKinley.

[22] „Góry" 2009, nr 10.

[23] Między autorką książki a alpinistami aktualnie toczy się proces. Opisani alpiniści pozwali autorkę, zarzucając jej naruszenie dóbr osobistych, na czas procesu obowiązuje zakaz

Po burzliwej dyskusji (toczonej również na forach internetowych) alpiniści pod wpływem opinii środowiska dobrowolnie oddali nagrodę, a Polski Związek Alpinizmu postanowił wyjaśnić sprawę. Powołana przez PZA komisja uznała, że materiały konieczne do ustalenia rzeczywistej wartości dokonań alpinistów powinny zostać zebrane w trakcie wyprawy weryfikacyjnej. Zadania zespołu weryfikacyjnego określono bardzo szczegółowo i polegały one m.in. na:

- sporządzeniu materiału fotograficznego i filmowego ściany, na której została poprowadzona droga Golden Lunacy;
- dokonaniu pomiarów altymetrem i GPS w określonych przez komisję punktach;
- powtórzeniu drogi Golden Lunacy oraz zmierzeniu czasu pokonywania poszczególnych odcinków drogi;
- oszacowaniu rzeczywistej wartości drogi (tj. nie tylko ocenie trudności drogi, ale również określeniu jej niedostępności);
- udokumentowaniu śladów, które pozostały po działalności wspinaczkowej autorów drogi Golden Lunacy[24].

Wyprawa, zdaniem zarządu PZA, pozwoliła przygotować „usystematyzowane kompendium o drodze" oraz zgromadzić „bogaty materiał multimedialny". Z raportu[25] opublikowanego przez zespół PZA ds. Golden Lunacy, który został opracowany po przeprowadzeniu analizy dostarczonych przez wyprawę materiałów, wynika, iż: „wiele zarzutów stawianych autorom drogi jest nieuprawnionych", natomiast wartość (trudność) drogi „jest na ogół 1,5 stopnia niższa, niż zadeklarowali jej autorzy". W sprawie oceny dokonań alpinistów i klasy drogi „w ujęciu sportowym i eksploracyjnym" nie byli zgodni powołani przez zarząd PZA eksperci – opublikowane zostało zdanie odrębne. Potwierdziły się wcześniej formułowane wobec wspinaczy zarzuty, że ich relacje z wyprawy są niedostatecznie precyzyjne, nierzetelne, „momentami wprowadzają czytającego w błąd".

Warto jednak przede wszystkim przytoczyć konkluzję autorów raportu, wynikającą z doświadczeń związanych ze „sprawą Golden Lunacy". Uznano, iż: „sprawa pokazała, że środowisko wspinaczkowe nie posiada wypracowanych standardów postępowania w tego typu kontrowersyjnych sytuacjach". Pojawił się zatem postulat, aby „podczas dokumentacji eksploracji odlegle położonych ścian, gór czy jaskiń obowiązywał standard bliższy naukowych publikacji niż tekstów reklamowych". Absolutnym minimum powinno być opublikowanie schematu drogi i jej wrysowanie na zdjęcie o możliwie wysokiej rozdzielczości. Pożądane byłoby wykonanie dokumentacji fotograficznej i filmowej, jeżeli tylko jest to możliwe. W raporcie zawarte zostały również zalecenia co do sposobu i stylu, w jakim powinien być przedstawiony opis wytyczonych dróg i kalendarz wyprawy.

publikacji książki.

[24] Pełna lista zadań zespołu weryfikacyjnego jest dostępna m.in. na portalu wspinanie.pl.

[25] Raport zespołu PZA ds. drogi Golden Lunacy jest dostępny na stronie pza.org.pl.

Wykorzystanie możliwości technicznych (lokalizatorów)

Wydaje się, że urządzenie GPS, wyposażone w funkcję zapisywania przebytej trasy (wraz ze współrzędnymi geograficznymi i wysokością), to idealne narzędzie weryfikacji zdolne udokumentować, czy alpinista osiągnął zadeklarowany cel.

W czasopismach i na portalach internetowych poświęconych wspinaczce wysokogórskiej można odnaleźć informacje dotyczące wykorzystywania Globalnego Systemu Pozycjonowania, jednak tylko jako narzędzia, które ma pomóc alpiniście np. w określeniu aktualnego położenia, przy planowaniu trasy itp.

Przy rozważaniu, czy lokalizatory byłyby przydatne do weryfikacji spornych osiągnięć (np. wejść na szczyty), należy zauważyć, iż urządzenie GPS jest zawodne. Działa na baterie, które mają ograniczoną żywotność. Dla prawidłowego ustalenia położenia wraz z wysokością konieczne jest przeanalizowanie sygnału z co najmniej czterech satelitów, co oznacza, że odbiornik musi być zdolny je namierzyć. W górach, z uwagi na występowanie naturalnych przeszkód (skalnych ścian), nie zawsze będzie to możliwe. Ponadto właściciel satelitów lokalizacyjnych (Departament Obrony USA), który udostępnia sygnał cywilnym użytkownikom urządzeń odbiorczych, sygnał ten częściowo zakłóca – wpływa to na dokładność podawanych danych. W związku z tym posiadanie lokalizatora przez zdobywającego szczyt alpinistę nie zawsze pozwoliłoby dać precyzyjną odpowiedź, która weryfikowałaby jego deklaracje.

Cięzu

Jedno z zasadniczych pytań, związanych z tematem artykułu, brzmi: czy to na alpiniście spoczywa obowiązek udowodnienia swojego osiągnięcia? Do podstawowych zasad etyki alpinistycznej należy przecież wzajemne zaufanie, którym mają darzyć się alpiniści. Wielu wybitnych przedstawicieli tego środowiska deklaruje, iż ta zasada nie ma dla nich jedynie wartości historycznej. Dlatego warto się zastanowić, czy obowiązek wykazania, że deklaracje są zgodne z prawdą, powstaje dopiero z chwilą, gdy pojawią się wątpliwości i zarzuty, że dokonanie jest mistyfikacją. A może to ci, którzy formułują zarzuty, powinni udowodnić, że alpinista bezpodstawnie przypisuje sobie osiągnięcie?

Istotne jest, że współcześnie osiągnięcie danego wyczynu sportowego wiąże się z konkretnymi gratyfikacjami, które może dzięki swoim dokonaniom uzyskać alpinista[26]. Przypisanie sobie danego osiągnięcia przestało być więc prywatną sprawą – często z tym osiągnięciem związane są wymierne profity oraz potencjalna strata innych osób,

[26] Zainteresowanie mediów osiągnięciami alpinistycznymi spowodowało, iż alpiniści (i ich wyczyny) stali się atrakcyjnym sposobem promowania produktów (firmy) – wykazywanie osiągnięć w tej dziedzinie jest więc związane z pozyskiwaniem sponsorów. Przed epoką „prywatnych sponsorów" wyprawy były (i zdarza się, że są do tej pory) finansowane przez państwo. Wykazanie konkretnych, wyróżniających daną osobę osiągnięć sportowych jest podstawą do zakwalifikowania się do opłaconej (chociaż w części) wyprawy. Rozgłos i sława sprzyjają również takiej komercyjnej działalności jak prowadzenie wykładów czy wydawanie książek.

które mogły zostać ich pozbawione przez nieuczciwego konkurenta. Należy dostrzec również drugą stronę problemu – powstało ryzyko, że zarzucanie innym osobom nieuczciwości może stać się sposobem na pozbycie się niewygodnych rywali. Osoba pomówiona zostaje postawiona przed dylematem, czy podjąć walkę o swoje dobre imię (jak uczyniła to np. Wanda Rutkiewicz), czy postąpić tak jak Tomo Cesen, który ostatecznie stwierdził, że „wspina się dla samego siebie i nie będzie niczego udowadniać".

Pomocną wskazówką, czy i na kim spoczywa ciężar dowodu, może być cel, jaki chce osiągnąć alpinista. Jeżeli realizuje swój projekt wyłącznie dla własnej satysfakcji, to nie ma obowiązku, aby go udowadniać, szczególnie gdy nie dba o to, aby osiągnięcie zyskało rozgłos. W przypadku wyczynów, które zaczynają mieć znaczenie dla szerszego grona osób, warto, by oprócz deklaracji alpinista posiadał też inne argumenty, które dokumentowałyby jego osiągnięcie. Byłoby to uczciwe wobec innych – przede wszystkim wobec tych, którzy próbują zrealizować taki sam wyczyn.

Odrębną kwestią jest wykazanie osiągnięcia wobec sponsora bądź klubu sportowego, który zorganizował lub finansował wyprawę. Obowiązek udokumentowania wcześniej uzgodnionego projektu powinien wynikać z zawartej umowy.

Po przeprowadzeniu postępowania w „sprawie Golden Lunacy" Polski Związek Alpinizmu dostrzegł, iż brak jasnych zasad dotyczących dokumentacji z wypraw powoduje kontrowersje i problemy. Zostały sformułowane zalecenia dotyczące dokumentacji osiągnięć alpinistycznych. Świadczy to o tym, iż związek uznał, że deklaracja alpinisty (w sytuacji, gdy jest publikowana) może być przedmiotem weryfikacji – powinna więc być zilustrowana dowodami, które powinny spełniać określone w zaleceniach kryteria. Jest to jeden z argumentów przemawiających za tym, iż zasada zaufania ustępuje zasadzie ograniczonego zaufania, a ciężar dowodu, zdaniem związku, do pewnego stopnia obciąża osobę, która deklaruje osiągnięcie alpinistyczne.

W sytuacji, gdy zostaje wszczęte postępowanie dyscyplinarne (które może być wszczęte z urzędu bądź na wniosek zainteresowanego podmiotu)[27], kwestia rozkładu ciężaru dowodu wynika wprost z przepisów. Wszczęcie postępowania może być spowodowane m.in. podejrzeniem naruszenia zasad etyki taternickiej[28] (tak więc np. nieuczciwym przypisaniem sobie osiągnięcia sportowego). Zgodnie z par. 57 pkt 2 Regulaminu Dyscyplinarnego PZA, obwiniony „nie ma obowiązku dowodzenia swojej niewinności i może bez podania powodów odmówić składania wyjaśnień lub odpowiedzi na poszczególne pytania". W postępowaniu dyscyplinarnym obowiązuje, znana z postępowania karnego, zasada domniemania niewinności (pkt 1 par. 57 Regulaminu) oraz reguła *in dubio pro reo* (pkt 3 par. 57 Regulaminu). Obwinionemu przysługuje prawo do „przedstawiania dowodów na swoją obronę oraz składania wniosków dowodowych" (pkt 4 par. 55 Regulaminu), może on jednak skorzystać z prawa do milczenia i to na organach dyscyplinarnych spoczywa obowiązek udowodnienia mu winy.

[27] Par. 53 Regulaminu Dyscyplinarnego Polskiego Związku Alpinizmu (stanowiącego załącznik do uchwały Walnego Zgromadzenia Delegatów PZA z dn. 24 maja 2014 r.).

[28] Zgodnie z postanowieniami Regulaminu Dyscyplinarnego PZA odpowiedzialność dyscyplinarna „ponoszona jest za naruszenie zasad etyki taternickiej lub zasad dobrej praktyki taternickiej" (pkt 2 par. 2 Regulaminu).

Zasada swobodnej oceny dowodów

Fakt, że alpinista nie dysponuje zdjęciem wykonanym na samym wierzchołku góry, nie musi świadczyć o tym, iż go tam nie było – aparat fotograficzny mógł zawieść, warunki atmosferyczne mogły uniemożliwić wykonanie fotografii, na której znalazłyby się elementy mogące posłużyć do identyfikacji. Posiadanie zdjęcia ze szczytu nie wyklucza natomiast mistyfikacji – zostały przecież opisane przykłady posłużenia się cudzym zdjęciem jako dowodem wejścia na szczyt. Każda z przedstawionych w artykule metod jest w zasadzie zawodna. Aby dokonać weryfikacji, należy przeprowadzić całościową ocenę wszystkich dostępnych w sprawie danych. Istotną kwestią jest to, kto ma się tego podjąć. Najmniej korzystne dla wyjaśnienia sprawy są prasowe spekulacje oraz dyskusje na forach internetowych. Tego typu media mogą spełnić jednak pewną funkcję – inicjować postępowanie przez podmioty bardziej predysponowane do przeprowadzenia postępowania dowodowego.

W skład organów dyscyplinarnych (funkcjonujących w ramach PZA), których rola w rozstrzyganiu tego typu sporów powinna być kluczowa, powoływane są osoby posiadające niezbędną wiedzę i doświadczenie alpinistyczne[29]. Kwalifikacje te są niezbędne do tego, aby orzec, czy obwiniony dopuścił się przewinienia dyscyplinarnego (np. przypisując sobie niesłuszne dokonanie sportowe). Warto wspomnieć, iż organy dyscyplinarne, wyjaśniając sporne kwestie, mogą korzystać (i często korzystają) z pomocy ekspertów. Zgodnie z par. 64 Regulaminu, „jeżeli rozstrzygnięcie postępowania dyscyplinarnego wymaga wiadomości specjalnych, organ dyscyplinarny może zasięgnąć pisemnej lub ustnej opinii specjalistów i ekspertów zewnętrznych". W przypadku badania dowodowych fotografii i orzekania o ich autentyczności często jako biegli powoływane są osoby będące znawcami topografii terenu, w którym fotografia miała być (zgodnie z deklaracją alpinisty) wykonana.

Regulamin nie wartościuje dowodów i nie dokonuje ich klasyfikacji – dowodem może być „każdy fakt mający znaczenie dla rozstrzygnięcia sprawy"[30]. Można więc uznać, iż w postępowaniu dyscyplinarnym, prowadzonym przez powołane do jego podjęcia organy PZA, obowiązuje „zasada swobodnej oceny dowodów".

Zasady etyki alpinistycznej

Zasady etyki alpinistycznej (taternickiej), które nie zostały zdefiniowane w żadnym oficjalnym dokumencie, dla wielu alpinistów pozostają podstawą działalności wspinaczkowej. Dyskusja na temat tych zasad odżyła po tragedii na Broad Peak w 2013 r. W listopadzie 2013 r. w Podlesicach odbyła się zorganizowana przez Polski Związek Alpinizmu debata na temat bezpieczeństwa i etyki na wyprawach w góry najwyższe. Jednym z tematów dyskusji był sposób relacjonowania wypraw i dokumentowania działalności wspinaczkowej przez alpinistów[31].

[29] Skład i tryb powoływania członków organów dyscyplinarnych został określony w rozdziale II Regulaminu.

[30] Zgodnie z par. 62 Regulaminu.

[31] B. Kowalski, *Szczyt Podlesicki – etyka i zasady we współczesnym alpinizmie*, „Góry" 2013, nr 11, s. 16–17 (Szczyt Podlesicki miał być nawiązaniem do słynnego Szczytu Gliwickiego

Należy zauważyć, że tematy związane z kontrowersjami wokół działalności alpinistycznej stają się medialne. Kontrowersyjne wydarzenia są przedstawiane w taki sposób, aby podsycać wrażenie skandalu – wówczas temat jest bardziej atrakcyjny i lepiej się sprzedaje. W interesie środowiska wspinaczkowego jest to, aby wyjaśnianie sporów i kontrowersji nie przebiegało w atmosferze awantur i spekulacji. Umiejętność rzetelnego wyjaśniania spornych spraw może przesądzić o przyszłym stanie tego sportu oraz rozstrzygnąć, czy etyka, która w alpinizmie zawsze była ważna, nie stanie się wartością przebrzmiałą.

Streszczenie

W artykule został poruszony temat ustalania spornych osiągnięć w alpinizmie – sporcie uprawianym w górach wysokich. Przedstawione zostały sposoby weryfikacji spornych oświadczeń alpinistów takie jak: analiza dokumentacji fotograficznej i filmowej z wyprawy, wnioskowanie z pozostałych w miejscu spornego osiągnięcia śladów, weryfikacja deklaracji alpinisty. Metody zostały zilustrowane przykładami autentycznych historii. W przeprowadzeniu weryfikacji spornego osiągnięcia sportowego zaakcentowana została potrzeba wykorzystania wiedzy wypracowanej w ramach kryminalistyki.

Słowa kluczowe: postępowanie dowodowe, dowody, sportowe postępowanie dyscyplinarne, alpinizm, taternictwo, himalaizm, weryfikacja wyczynów sportowych, Polski Związek Alpinizmu

Summary

This article discusses the issue of how to address disputed achievements in mountaineering – the sport which is performed in the high mountains. It covers the presentation of methods of the verification of disputed declarations of mountaineers, which include among others: examination of photographic and film documentation of the expedition, drawing conclusions based on traces left in the disputed performance location, verification of the mountaineer's declaration. Said methods are illustrated by examples taken from real-life. Emphasis is put to the need to exploit the expertise in the field of forensics for the purpose of verification of disputed sporting performances

Keywords: taking of evidence, evidence, disciplinary proceedings in sport, mountaineering in the Alps, mountaineering in the Tatras, mountaineering in the Himalayas, verification of sporting performance, the Polish Mountaineering Association

z 1987 r., który zapoczątkował dyskusje na temat etyki we współczesnym alpinizmie. Relację ze Szczytu Gliwickiego można odnaleźć m.in. na portalu brytan.pl).

Maciej Kędzierski

PENALIZACJA FINANSOWANIA TERRORYZMU W ART. 165A KODEKSU KARNEGO

Criminalization of terrorist financing in Art. 165a of the Criminal Code

Budując każdy system, należy upatrywać w nim skuteczności, a przede wszystkim sprawnego i optymalnego mechanizmu realizowania celu, w jakim został opracowany. To ogólne, dość uniwersalne założenie dotyczy także kwestii aktualnego wzorca przeciwdziałania i zwalczania finansowania terroryzmu w Polsce. Jednym z głównych elementów wzorca systemu przeciwdziałania i zwalczania finansowania terroryzmu jest spenalizowanie przestępczego zachowania w art. 165a k.k. określanego jako finansowanie przestępstwa o charakterze terrorystycznym. O ile w ustawodawstwie polskim już w latach 90. zauważono potrzebę przeciwdziałania zjawisku prania pieniędzy (zarządzenie Prezesa NBP), o tyle na wprowadzenie szczególnych regulacji do polskiego obrotu prawnego w zakresie przeciwdziałania finansowaniu terroryzmu trzeba było poczekać kolejne prawie 10 lat.

W grudniu 1999 r. Zgromadzenie Ogólne ONZ przyjęło Międzynarodową konwencję o zwalczaniu finansowania terroryzmu[1]. W Preambule Konwencji powołano się na rezolucję Zgromadzenia Ogólnego 51/210 z dnia 17 grudnia 1996 r., w której Zgromadzenie wezwało wszystkie państwa do podjęcia działań: „celem zapobiegania i przeciwdziałania finansowaniu terrorystów i organizacji terrorystycznych poprzez stosowne działania wewnętrzne, niezależnie od tego, czy takie finansowanie odbywa się bezpośrednio czy pośrednio przez organizacje mające między innymi cele charytatywne, społeczne lub kulturalne, czy też utrzymujące, że mają takie cele, albo prowadzące również nielegalną działalność, taką jak nielegalny handel bronią, handel narkotykami i wymuszenia, w tym wykorzystywanie ludzi celem finansowania działań terrorystycznych". W szczególności zaś wezwano do rozważenia możliwości przyjęcia środków prawnych mających zapobiegać i przeciwdziałać przepływom funduszy, co do których podejrzewa się, że są przeznaczone

[1] Kwestie przeciwdziałania praniu pieniędzy zostały po raz pierwszy uregulowane 11 lat wcześniej, zawarto je w Konwencji Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi, sporządzonej we Wiedniu dnia 20 grudnia 1988 r. (Dz. U. z 1995 r., Nr 15, poz. 69). Konwencja weszła w życie w 1990 r.

na działalność terrorystyczną, tak jednak, by w żaden sposób nie ograniczać wolności legalnego przepływu kapitału[2].

Konwencja ONZ z 1999 r. zdefiniowała pojęcie przestępstwa *finansowania terroryzmu*. W rozumieniu niniejszej konwencji przestępstwo finansowania terroryzmu popełnia ten, kto jakimikolwiek środkami, bezpośrednio lub pośrednio, bezprawnie i umyślnie, udostępnia lub gromadzi fundusze z zamiarem ich wykorzystania, lub też mając świadomość, że zostaną one wykorzystane, w całości lub w części, do dokonania: czynu stanowiącego przestępstwo określone definicją zawartą w jednym z traktatów wymienionych w aneksie[3]; a także czynu mającego spowodować śmierć lub ciężki uszczerbek na zdrowiu osoby cywilnej, lub innej osoby nieuczestniczącej aktywnie w działaniach wojennych w sytuacji konfliktu zbrojnego, jeśli celem takiego czynu, wynikającym bądź z jego charakteru, bądź z kontekstu, w jakim jest popełniony, jest zastraszenie ludności albo skłonienie rządu lub organizacji międzynarodowej do dokonania lub do zaniechania określonej czynności.

Warto wspomnieć, że kolejna ewolucja ustawodawstwa i zaleceń instytucji międzynarodowych odpowiedzialnych za kreowanie modelu przeciwdziałania wskazywała na to, że na podstawie Konwencji o finansowaniu terroryzmu każdy kraj powinien penalizować finansowanie terroryzmu, przy czym kryminalizacji powinno podlegać finansowanie nie tylko aktów terrorystycznych, ale również organizacji terrorystycznych i indywidualnych terrorystów, nawet jeśli nie mają oni związku z określonym aktem bądź aktami terrorystycznymi (zalecenia FATF). Stąd też współczesne ujęcie prawnego sankcjonowania finansowania działalności terrorystycznej kumuluje w sobie dwa główne podejścia. Jedno odnosi się do sankcjonowania finansowania

[2] Zob. T. Aleksandrowicz, *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 61.

[3] 1) Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, sporządzona w Hadze dnia 16 grudnia 1970 r. 2) Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, sporządzona w Montrealu dnia 23 września 1971 r. 3) Konwencja o zapobieganiu przestępstwom i karaniu sprawców przestępstw przeciwko osobom korzystającym z ochrony międzynarodowej, w tym przeciwko dyplomatom, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 14 grudnia 1973 r. 4) Międzynarodowa Konwencja przeciwko braniu zakładników, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 17 grudnia 1979 r. 5) Konwencja o ochronie fizycznej materiałów jądrowych, przyjęta w Wiedniu dnia 3 marca 1980 r. 6) Protokół w sprawie zwalczania bezprawnych aktów przemocy w portach lotniczych służących międzynarodowemu lotnictwu cywilnemu, uzupełniający Konwencję o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, sporządzony w Montrealu dnia 24 lutego 1988 r. 7) Konwencja o zwalczaniu bezprawnych czynów przeciwko bezpieczeństwu żeglugi morskiej, sporządzona w Rzymie dnia 10 marca 1988 r. 8) Protokół o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu stałych platform umieszczonych w szelfie kontynentalnym, sporządzony w Rzymie dnia 10 marca 1988 r. 9) Międzynarodowa konwencja w sprawie zwalczania terrorystycznych ataków bombowych, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 grudnia 1997 r.

poszczególnych aktów terrorystycznych, drugie – do sankcjonowania organizacyjnych form funkcjonowania ugrupowań terrorystycznych, niezależnie od przygotowywanych ataków. Wydaje się, że takie kompleksowe podejście do przeciwdziałania finansowaniu terroryzmu powinno znaleźć swoje odzwierciedlenie także w polskim ustawodawstwie jako najbardziej adekwatne do przeciwdziałania zagrożeniu terrorystycznemu. Należy zauważyć, że poprzez finanse budowany jest potencjał organizacji terrorystycznej, którego uwolnienie realizowane jest w postaci dokonywanych zamachów, a ostatnio także budowania quasi-państwowych struktur terrorystycznych (tzw. Państwo Islamskie). Dopiero tak całościowe podejście pozwala na rzeczywiste realizowanie prewencyjnej roli przepisów prawa i racjonalne uniemożliwienie wystąpienia powszechnego zagrożenia wywołanego zamachem terrorystycznym.

Jeżeli chodzi o uregulowania zapobiegające finansowaniu terroryzmu w polskim ustawodawstwie, to wiele lat tkwiono w przekonaniu, że właściwym instrumentem prawnym do jego zwalczania jest art. 258 k.k. (penalizuje on zakładanie związku lub grupy mającej na celu popełnianie przestępstw o charakterze terrorystycznym, a także kierowanie takim związkiem czy grupą i udział w nim) oraz artykuł Kodeksu karnego dotyczący instytucji podżegania i pomocnictwa (art. 18 par. 2 i par. 3 k.k.). Art. 18 k.k. określa pomocnictwo i podżeganie jako ułatwienie popełnienia czynu zabronionego, a zachowania te obejmują w szczególności „dostarczanie narzędzi (...), udzielanie rady lub informacji”[4]. Podżeganie polega na nakłanianiu innej osoby do popełnienia czynu zabronionego, podżegacz musi chcieć nakłonić daną osobę do czynu zabronionego. Stąd też działa umyślnie w postaci zamiaru bezpośredniego[5]. Niemniej trzeba zauważyć, że nie jest podżeganiem nakłanianie osoby, która ma już zamiar popełnienia przestępstwa. Stąd też wykluczyć należy sytuację, w której podżegacz będzie namawiał do dokonania zamachu członków organizacji terrorystycznej, którzy już powołali taki twór organizacyjny z zamiarem realizowania zamachów terrorystycznych, a jedynie poszukują poza organizacją środków finansowych na jego zorganizowanie. Ponadto nie można podżegać samego siebie do dokonania zamachu terrorystycznego, co wyklucza zastosowanie tego przepisu w przypadku gromadzenia środków przez samego sprawcę zamachu terrorystycznego. Dlatego też zachowanie określane jako podżeganie nie w pełni odzwierciedla możliwe zachowania sprawców finansowania terroryzmu.

Pomocnictwo polega na ułatwieniu innej osobie popełnienia czynu zabronionego przez dostarczenie jej narzędzi, środka przewozu, udzielenie rady lub informacji. Jest to jedynie przykładowe wyliczenie; zachowanie pomocnika może także polegać na dostarczeniu środków finansowych, udostępnieniu nieruchomości. Trudno będzie przy takim podejściu także rozróżnić, czy mamy do czynienia z pomocnictwem, czy już ze współsprawstwem. Chodzi przede wszystkim o „istotny” wkład w popełnienie przestępstwa[6]. „Istotność” takiego zachowania powinno się oceniać pod tym

[4] Zob. *Szczegółowe sprawozdanie z 3. rundy oceny w sprawie 1 przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu w Polsce*. Memorandum sporządzone przez Sekretariat Dyrekcji Generalnej ds. Praw Człowieka i Kwestii Prawnych, teza 144.

[5] L. Gardocki, *Prawo karne*, wyd. 18, Wydawnictwo C.H. Beck, Warszawa 2013, s. 101.

[6] Tamże, s. 104.

względem, czy dostarczone środki finansowe stały się warunkiem koniecznym do dokonania określonego zamachu terrorystycznego, czy też środki te jedynie stanowią uzupełnienie już istniejących, wykorzystywanych również w celu zapewnienia organizacyjnej formy grupy terrorystycznej.

Powoływanie się jedynie na zachowania określone jako podżeganie i pomocnictwo do dokonania zamachu terrorystycznego należy ocenić zdecydowanie negatywnie. Takie zachowanie ustawodawcy należy rozumieć jako „kamuflowanie" problemu lub też uważanie, że on nie istnieje jako finansowanie działalności terrorystycznej. Jednocześnie warto wskazać, że bazowanie wyłącznie na zachowaniu podżegacza czy pomocnika (jako finansujących terroryzm) byłoby całkowicie nieczytelne dla pracowników instytucji obowiązanych, które mają obowiązek monitorowania transakcji związanych z finansowaniem działalności terrorystycznej. Nieczytelność ta związana byłaby prawdopodobnie z całkowitym ograniczeniem się do śledzenia symptomów finansowania działalności terrorystycznej, co i tak jest bardzo trudne przy aktualnym zapisie art. 165a k.k. Odbiór takich zachowań dla pracowników podmiotów obowiązanych byłby całkowicie nieczytelny. Ponadto pozostawienie takiej regulacji nie byłoby kompatybilne z regulacjami występującymi w innych krajach, które z finansowania terroryzmu ustanowiły odrębny rodzaj przestępstwa.

W konsekwencji przyjętych rozwiązań, głównie na tle zaleceń FATF, dopiero w 2009 roku odrębnie spenalizowano w Polsce zachowanie polegające na realizowaniu określonych działań mających na celu *sfinansowanie przestępstwa o charakterze terrorystycznym*. Uprzednio w 2002 r. dokonano zmiany przepisów podstawowych z punktu widzenia przeciwdziałania zawartych w Ustawie o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł, w tym między innymi w 2002 r. zmieniono jej tytuł, uwzględniając również tematykę przeciwdziałania finansowaniu terroryzmu[7]. Stąd też tytuł ustawy został ostatecznie ustalony następująco: Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. W ustawie tej nie zdefiniowano jednak, co należy rozumieć przez pojęcie finansowania terroryzmu, określono jedynie, kiedy jest mowa o akcie terrorystycznym[8]. Jak słusznie zauważyła A. Golonka, „sformułowania zawarte w ustawie z 2002 r. odnośnie aktu terrorystycznego – obarczone były nieścisłościami, w tym wynikającymi z wewnętrznej sprzeczności, w jakiej

[7] Ponadto ustanowiono urząd Generalnego Inspektora Informacji Finansowej jako dodatkowy organ w sprawach przeciwdziałania finansowaniu terroryzmu, nadając mu jednocześnie uprawnienia kontrolne w tym zakresie wobec instytucji obowiązanych. Instytucje obowiązane w wewnętrznych procedurach miały uwzględnić tematykę przeciwdziałania finansowania terroryzmu. Informacje związane z finansowaniem terroryzmu mogły być udostępniane przez Generalnego Inspektora zagranicznym instytucjom na zasadzie wzajemności. Dokonano również szeregu zmian w poszczególnych ustawach kompetencyjnych regulujących działalność instytucji obowiązanych (Druk sejmowy, nr 881 z dn. 11.09.2002).

[8] Przez to pojęcie rozumiano przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne, przestępstwa przeciwko bezpieczeństwu powszechnemu oraz przestępstwa określone w art. 134 i 136 k.k.

dyspozycja normy prawnej zawartej w tym przepisie pozostawała względem pewnych unormowań Kodeksu karnego. W tym miejscu wypada wskazać chociażby na niepoprawność związaną ze zwrotem nawiązującym do kategorii czynów wymienionych jako *„»akt terrorystyczny«”*[9]. W konsekwencji więc trudno było wskazać, czemu należy przeciwdziałać, niekoniecznie uznając, czym jest „finansowanie terroryzmu" czy też finansowanie „aktu terrorystycznego". Interpretując ówczesny stan prawny, można stwierdzić, że ideą stało się raczej umiejscowienie określonej „atrapy prawnej" niż racjonalne uregulowanie kwestii przeciwdziałania finansowaniu terroryzmu. Nadal zgodnie z regułą *nullum crime sine lege* trudne do określenia było udzielenie odpowiedzi na pytanie, co należałoby ścigać, gdy brak było jasno sprecyzowanego ustawowo przestępstwa finansowania terroryzmu. Taki sposób postępowania ustawodawcy mógł jedynie implikować dwie sytuacje. Jedną – wprowadzającą chaos decyzyjny i obawę przed odpowiedzialnością za niewłaściwe postępowanie tych podmiotów, które obarczono obowiązkiem przeciwdziałania. Drugą – wprowadzającą całkowitą obojętność i niewykonywanie obowiązku wobec braku skonkretyzowania celu i zakresu negatywnego zachowania potencjalnego sprawcy.

Następnie Polska przyjęła i ratyfikowała Międzynarodową konwencję o zwalczaniu finansowania terroryzmu. Dokument ten stał się wiążący dla Polski od 13 grudnia 2004 r. W następnych latach wywarł on istotny wpływ na kształtowanie się modelu przeciwdziałania finansowaniu terroryzmu w Polsce.

Na przestrzeni szeregu lat polskie ustawodawstwo było dostosowywane do rozwiązań międzynarodowych w zakresie przeciwdziałania finansowaniu terroryzmu. Przyjęcie tych rozwiązań miało także na celu implementację do krajowego porządku prawnego dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady Europy z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu, a także dostosowanie przepisów ustawy w celu zapewnienia stosowania aktów prawa międzynarodowego w zakresie przeciwdziałania finansowaniu terroryzmu oraz dyrektywy Komisji 2006/70/WE ustanawiającej środki wykonawcze do dyrektywy 2005/60/WE w odniesieniu do definicji osoby zajmującej eksponowane stanowisko polityczne, jak również w odniesieniu do technicznych kryteriów stosowania uproszczonych zasad należytej staranności wobec klienta, ponadto wprowadzono wyłączenia z uwagi na prowadzoną działalność finansową w sposób sporadyczny lub w bardzo ograniczonym zakresie[10]. W rzeczywistości powstała sytuacja utrzymująca się do 2009 r., w której powołano szeroki aparat „przeciwdziałania" czemuś, czego nie definiowano na poziomie przestępstwa kryminalnego. Jeszcze w 2006 r. misja ewaluacyjna MONEYVAL zauważyła,

[9] Zob. A. Golonka, *Polskie rozwiązania prawne w zakresie przeciwdziałania finansowaniu terroryzmu*, „Prokuratura i Prawo" 2013, nr 3, s. 97.

[10] *Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw* (Druk sejmowy nr 1660).

że obecnie polski system prawny nie rozróżnia samodzielnego przestępstwa „finansowania terroryzmu", w związku z czym w przypadku takiego działania można jedynie wnieść oskarżenie o pomocnictwo i nakłanianie do popełnienia „przestępstwa o charakterze terrorystycznym". Dostrzeżono także, że do tej pory nie wniesiono jednak żadnych oskarżeń o finansowanie terroryzmu, a w świetle obowiązujących przepisów trudno wyobrazić sobie, w jaki sposób mogłoby przebiegać ściganie finansowania organizacji terrorystycznej. Jako przyczynę tego stanu rzeczy wskazano to, że Polska nie rozpoczęła procedury legislacyjnej mającej na celu wprowadzenie do Kodeksu karnego odrębnego przestępstwa finansowania terroryzmu[11]. Komisja Europejska wielokrotnie zwracała Polsce uwagę na fakt braku transpozycji ww. aktów wspólnotowych do rodzimego porządku prawnego. Opieszałość naszego kraju sprawiła, że na początku 2009 r. Komisja Europejska podjęła bardziej zdecydowane kroki, w które wyposaża ją Traktat. W dniu 29 stycznia 2009 r. w trybie art. 226 TWE2 skierowała ona do Europejskiego Trybunału Sprawiedliwości sprawę przeciwko Polsce, zarzucając brak implementacji postanowień Trzeciej Dyrektywy[12]. Dostosowanie prawa krajowego do wymogów UE trwało dwa lata, na co zwrócił uwagę NIK w trakcie kontroli wypełniania przez GIIF obowiązków ustawowych[13]. Przyjęta w 2009 r. zmiana ustawy o przeciwdziałaniu wprowadziła nie tylko mechanizmy funkcjonowania wymienionych w niej podmiotów, ale także ustanowiła w Kodeksie karnym penalizację zachowań określonych jako finansowanie terroryzmu[14].

Przed nowelizacją Kodeksu karnego w 2009 r., która wprowadziła nowy typ przestępstwa w art. 165a k.k., możliwe było objęcie zachowania polegającego na finansowaniu działalności terrorystycznej następującymi kwalifikacjami prawnymi: wspomnianym pomocnictwem w zw. z art. 258 par. 2 k.k., przygotowaniem do własnego czynu o charakterze terrorystycznym, braniem udziału w grupie lub związku mającym na celu popełnienie przestępstwa o charakterze terrorystycznym (art. 258 par. 2 k.k.)[15]. Finansowanie terroryzmu powinno obejmować każdą osobę, która umyślnie zapewnia lub gromadzi środki, bezpośrednio lub pośrednio w niezgodnym z prawem zamiarze wykorzystania ich w całości lub w części do popełnienia nadużycia lub przy wiedzy o takim wykorzystaniu do

[11] Europejski Komitet ds. Problemów z Przestępczością (CDPC), Komitet Ekspertów ds. Oceny Środków Zapobiegania Praniu Pieniędzy (MONEYVAL), *Szczegółowe sprawozdanie z 3. rundy oceny w sprawie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu w Polsce*, memorandum sporządzone przez Sekretariat Dyrekcji Generalnej ds. Praw Człowieka i Kwestii Prawnych, teza 14.

[12] J. Skłodowska, *Nowe obowiązki adwokata jako instytucji obowiązanej*, „Palestra" 2009, nr 3–4 (wydanie internetowe).

[13] Informacja NIK o wynikach kontroli realizacji przez Generalnego Inspektora Informacji Finansowej obowiązków w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, Zielona Góra, sierpień 2011, www.nik.gov.pl.

[14] W ustawie z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.) wprowadzono zmiany poprzez dodanie art. 165a.

[15] E.M. Guzik-Makaruk, W. Filipkowski, *Kryminalizacja finansowania terroryzmu…*, s. 59.

przeprowadzenia aktu lub aktów terrorystycznych; przez organizację terrorystyczną lub przez terrorystę[16].

Tak więc na przestrzeni kilku lat kształtowania się ustawodawstwa karnego dotyczącego zwalczania finansowania terroryzmu w Polsce można wydzielić następujące etapy:

1. Brak przepisu penalizującego finansowanie terroryzmu z możliwością powołania się na przepisy art. 18 k.k. w związku z określonymi przepisami Kodeksu karnego do 1997 r.
2. Brak przepisu penalizującego finansowanie terroryzmu z możliwością powołania się na przepisy art. 258 par. 2 oraz 3–4 k.k. i art. 18 k.k. w związku z określonymi przepisami Kodeksu karnego od 1997 r. do 2004 r.
3. Brak przepisu penalizującego finansowanie terroryzmu z możliwością powołania się na przepisy art. 258 par. 2 oraz 3–4 k.k. i art. 18 k.k. w związku z określonymi przepisami Kodeksu karnego i jednoczesną implementacją przepisów Międzynarodowej konwencji o zwalczaniu finansowania terroryzmu od 2004 r. do 2009 r.
4. Spenalizowanie jako przestępstwa odrębnego zachowania określonego jako finansowanie terroryzmu w art. 165a k.k. od 2009 do 2010 r.
5. Spenalizowanie jako przestępstwa odrębnego zachowania określonego jako finansowanie terroryzmu w art. 165a k.k. przy jednoczesnym rozszerzeniu odpowiedzialności podmiotu zbiorowego za udział jego przedstawiciela w przestępstwie finansowania terroryzmu po 2010 r.
6. Stan aktualny (po 2010 r.) – penalizacja zachowania określonego jako finansowanie terroryzmu w art. 165a k.k. wraz z rozszerzeniem odpowiedzialności podmiotu zbiorowego za udział jego przedstawiciela w przestępstwie finansowania terroryzmu.
7. 2015 r. opracowanie przez Ministerstwo Sprawiedliwości projektu rządowego zmiany treści art. 165a przyjętego przez Rząd RP w dniu 07 lipca 2015 r. zawierającego szerszą penalizację zachowań sprawców finansowania przestępstwa o charakterze terrorystycznym, o finansowanie grup

[16] Zob. Europejski Komitet ds. Problemów z Przestępczością (CDPC), Komitet Ekspertów ds. Oceny Środków Zapobiegania Praniu Pieniędzy (MONEYVAL), *Szczegółowe sprawozdanie*..., op. cit., teza 145. Ewaluatorzy zauważyli także, że nie jest możliwe uwzględnienie w interpretacji art. 258 k.k. dostarczania lub gromadzenia funduszy z zamiarem wykorzystania ich w całości lub w części przez terrorystę (teza 148). Ponadto należy zwrócić uwagę, że finansowanie terroryzmu nie musi być realizowane przez zawiązanie się grupy lub związku przestępczego – w celu, którym, jak by się wydawało, byłoby finansowanie własnej działalności terrorystycznej, czy też działalności innego podmiotu. Ponadto dodatkowym elementem, który uniemożliwiałby skorzystanie niejako „zastępczo" z art. 258 k.k., jest to, że pozostaje on nieadekwatny do struktury organizacyjnej grupy/związku terrorystycznego. Zob. uwagi odnośnie do zorganizowanej grupy przestępczej w: Z. Rau, *Cechy polskiej zorganizowanej grupy przestępczej*, http://przestepczosczorganizowana.pl/index.php?go=15.

lub związków mających na celu popełnianie tego rodzaju przestępstw oraz wyeliminowanie działania wyłącznie w zamiarze bezpośrednim.

Kolejna propozycja zmiany przepisów w przedmiotowym zakresie pochodzi z 2010 r. i dotyczyła poszerzenia odpowiedzialności podmiotów zbiorowych za udział ich przedstawicieli w przestępstwie finansowania terroryzmu. Projekt[17] przewidywał konieczność transpozycji do porządku krajowego regulacji prawa unijnego w postaci decyzji ramowej Rady 2008/919/WSiSW z 28 listopada 2008 r. zmieniającej decyzję ramową 2002/475/WSiSW w sprawie zwalczania terroryzmu[18]. W konsekwencji wprowadzono przepis o odpowiedzialności podmiotów zbiorowych także za udział w przestępstwie finansowania terroryzmu[19].

Na przestrzeni kilku lat wykreowała się z jednej strony odpowiedzialność indywidualna za uczestnictwo w procederze finansowania terroryzmu, z drugiej ustanowiono także odpowiedzialność podmiotów zbiorowych za udział w finansowaniu działalności terrorystycznej. Są to, oprócz karalności zachowania związanego z nakłanianiem do popełnienia przestępstwa terrorystycznego, najnowsze uregulowania prawne w zakresie przestępstw okołoterrorystycznych[20].

W dniu 21 listopada 2008 r. Prezes Rady Ministrów skierował do Marszałka Sejmu projekt ustawy o zmianie ustawy Kodeks karny, Kodeks postępowania karnego, Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw[21]. W projekcie tym zaproponowano między innymi wprowadzenie penalizacji nowego przestępstwa – finansowania przestępstwa o charakterze terrorystycznym. W uzasadnieniu do projektu wskazano, że: „przewiduje się wprowadzenie nowego przepisu – oznaczonego jako art. 165a k.k. – kryminalizującego czyn polegający na gromadzeniu, przekazywaniu lub oferowaniu środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innego mienia ruchomego lub nieruchomego, w celu sfinansowania przestępstwa o charakterze terrorystycznym. Przepis ten jest wyrazem realizacji zobowiązań Rzeczypospolitej Polskiej wynikających z zaleceń Komitetu Antyterrorystycznego Rady Bezpieczeństwa ONZ, monitorującego przestrzeganie przez państwa członkowskie ONZ Rezolucji Rady Bezpieczeństwa 1373 (2001), jak również Konwencji ONZ z 1999 r. o zwalczaniu finansowania terroryzmu”[22]. Przepis został umieszczony w rozdzia-

[17] Projekt ustawy o zmianie ustawy – Kodeks karny i niektórych innych ustaw (Druk Sejmowy nr 4342 Sejmu VI kadencji).

[18] Dz. Urz. UE L 330 z 9.12.2008 r., s. 21–23.

[19] W art. 16 ust. 1 pkt 12 ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2002 r., Nr 197, poz. 1661 ze zm.).

[20] Wprowadzone przepisy można podzielić na te penalizujące przestępstwa o charakterze terrorystycznym oraz okołoterrorystyczne, w tym art. 165a k.k. oraz art. 255 k.k.

[21] Druk sejmowy nr 1394, Sejmu IX kadencji.

[22] Zob. A. Grzelak, *Opinia prawna dotycząca projektu nowelizacji art. 163–172b Kodeksu karnego (przestępstwa przeciwko bezpieczeństwu powszechnemu*), druk nr 1756, Warszawa, 20 czerwca 2007 r.

le XX – Przestępstwa przeciwko bezpieczeństwu powszechnemu. Tym samym oprócz przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, które można było realizować poprzez instrumenty administracyjne i inne wynikające z ustawy o przeciwdziałaniu, wzmocniono oddziaływanie dzięki ustanowieniu sankcji z zakresu prawa karnego umożliwiającej jego zwalczanie. Początkowo w trakcie prac ustawodawczych uznano przestępstwo finansowania terroryzmu za zbrodnię i było ono zagrożone karą pozbawienia wolności od lat 3 do lat 15[23].

Podstawową kwestią, która na gruncie projektowania zapisów art. 165a k.k. rodziła wątpliwości, była wysokość zaproponowanej sankcji za zachowania przybierające postać przygotowania do przestępstwa o charakterze terrorystycznym. Projektodawca nie wykazał, skąd wynika potrzeba tak wysokiej kary. Uznano, że nie można tracić z oczu także treści art. 115 par. 20 k.k. (górna granica wynosi co najmniej 5 lat) oraz konsekwencji dla sprawcy przestępstwa o charakterze terrorystycznym wynikającej z treści art. 65 par. 1 k.k.[24] W ostateczności stało się ono występkiem, sprawca podlega karze pozbawienia wolności od lat 2 do lat 12[25]. Ustawą z dnia 25 czerwca 2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw w *ustawie z dnia 6 czerwca 1997 r. – Kodeks karny*[26] zaproponowano wprowadzenie art. 165a w następującym brzmieniu: „Art. 165a. Kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie

[23] Zob. Druk sejmowy nr 1756 z dn. 18 maja 2007 r., *Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* wraz z projektem aktów wykonawczych oraz Druk Sejmowy nr 1958 z dnia 6 lipca 2007 r. Między innymi Ministerstwo Sprawiedliwości zaproponowało sankcję w postaci kary pozbawienia wolności od 2 lat do 12.

[24] Tamże, s. 19. Pogląd ten wydaje się niesłuszny wobec potrzeby niższego zagrożenia dla przestępstwa finansowania terroryzmu. Ograniczenie jedynie do występku zachowania określonego w art. 165a k.k. wskazuje na przywiązywanie niewielkiej wagi do zapobiegania organizacji samych zamachów terrorystycznych. Walcząc z finansowaniem terroryzmu, możemy zapobiec zamachowi w dość wstępnej fazie jego przygotowania czy skutecznie zakłócić ten proces. Dlatego też idea niskiego zagrożenia takiego zachowania jest niewłaściwa. W zakresie wymiaru kary, środków karnych oraz środków związanych z poddaniem sprawcy próbie wobec sprawcy, który z popełnienia przestępstwa uczynił sobie stałe źródło dochodu lub popełnia przestępstwo, działając w zorganizowanej grupie albo związku mającym na celu popełnienie przestępstwa, oraz wobec sprawcy przestępstwa o charakterze terrorystycznym stosuje się takie kryteria jak w przypadku powrotu do przestępstwa.

[25] Zgodnie z art. 258 Kodeksu karnego Ukrainy finansowanie terroryzmu jest traktowane bardziej rygorystycznie niż dokonywanie aktów terrorystycznych. Takie podejście ustawodawcy jest uzasadnione, ponieważ stopień niebezpieczeństwa publicznego działalności terrorystycznej jest wyższy w porównaniu z aktami terrorystycznymi. N.A. Lopashenko, Некоторые аспекты противодействия финансированию терроризма по законодательству Украины и России, „Satellite" 2005, s. 264–266, Saratow, Centrum Studiów nad Przestępczością Zorganizowaną i Korupcją.

[26] Dz. U. Nr 88, poz. 553, z późn. zm.

ruchome lub nieruchomości w celu sfinansowania przestępstwa o charakterze terrorystycznym, podlega karze pozbawienia wolności od lat 2 do 12".

Tym samym aktualnie na poziomie ustawowym przeciwdziałanie finansowaniu terroryzmu regulują następujące akty prawne: ustawa z dnia 6 czerwca 1997 r. – Kodeks karny[27] (ustawa ta zawiera definicję przestępstwa o charakterze terrorystycznym – art. 115 par. 20 k.k.[28] i przestępstwa finansowania przestępstwa o charakterze terrorystycznym – art. 165a); ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[29] wraz z przepisami wykonawczymi (określająca podmioty przeciwdziałania i mechanizmy realizacji tego działania, a w szczególności zakres podmiotowy i przedmiotowy obowiązków instytucji obowiązanych i podmiotów współpracujących); ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary[30] (art. 16 ust. 1 pkt 12) – określająca zasady odpowiedzialności podmiotu zbiorowego za zaangażowanie go w finansowanie działalności terrorystycznej.

W art. 165a k.k. zostało określone, na czym polega proceder finansowania terroryzmu. Sprawcą omawianego przestępstwa może być zatem każdy (podmiot przestępstwa powszechnego), na co wskazuje określenie (zaimek): „kto". W kontekście podmiotu przestępstwa z art. 165a k.k. należy wskazać na kwestię związaną z ustalonymi źródłami pozyskiwania środków finansowych na działalność terrorystyczną. Mimo znacznego zróżnicowania źródeł finansowania, w tym na wewnętrzne (samofinansowanie się organizacji terrorystycznej) czy też zewnętrzne (mocodawcy prywatni, korporacyjni, czy państwowi) za każdym razem sprawcą pozostaje określona osoba. To ona podejmuje działania zamierzające do zrealizowania wcześniejszego zamierzenia wykreowanego w jej psychice/umyśle. W aktualnym brzmieniu art. 165a k.k. nieważne jest, czy jest to osoba prywatna, właściciel przedsiębiorstwa, który przekazuje środki płatnicze na rzecz organizacji terrorystycznej, przedstawiciel organu państwowego, czy członek stowarzyszenia religijnego organizujący składki pieniężne na rzecz terrorystów oraz czy chciał on je w takim celu gromadzić, oferować, przekazać. Istotne jest to, aby sprawca miał świadomość celu, że środki te mają być przeznaczone na rzecz sfinansowania przestępstwa o charakterze terrorystycznym.

Penalizacji na podstawie art. 165a k.k. podlegają czynności przygotowawcze do finansowania akcji terrorystycznych, polegające na gromadzeniu, przekazywaniu lub oferowaniu wymienionych w przepisie środków płatniczych, instrumentów finansowych lub wartości majątkowych w celu sfinansowania przestępstwa

[27] Dz. U. 1997, Nr 88 poz. 553 ze zm.

[28] Przykładowo Kodeks karny do czynów terrorystycznych zalicza również: zamachy na bezpieczeństwo w komunikacji lotniczej lub morskiej (art. 166–167), zamachy na bezpieczeństwo powszechne – w tym zamachy bombowe (art. 163 par. l i art. 148 par. 2 pkt 4), wzięcie zakładnika (art. 252), zabójstwo w związku z wzięciem zakładnika (art. 148 par. 2 pkt 2).

[29] Dz. U. 2010, Nr 46, poz. 276 ze zm.

[30] Dz. U. z 2002 r., Nr 197, poz. 1661 ze zm.

o charakterze terrorystycznym. Jest to więc przestępstwo wymagające zamiaru bezpośredniego o charakterze kierunkowym (*dolus directus coloratus*). Ustanowienie karalności na przedpolu czynu zabronionego (przestępstwa terrorystycznego) uzasadnia rozmiar zagrożenia o charakterze powszechnym, związany z przestępczością terrorystyczną[31]. Przestępstwo owo może być popełnione wyłącznie umyślnie. Osoba realizująca czynności gromadzenia, przekazywania czy oferowania musi mieć świadomość – i w takim przekonaniu działać – że przekazuje je w celu sfinansowania przestępstwa o charakterze terrorystycznym. Przekazuje je w przekonaniu, że zostaną one wykorzystane celem popełnienia przestępstwa o charakterze terrorystycznym. Zdaje sobie sprawę z tego, że w ten sposób wspiera i popiera działania danego podmiotu kryminalnego celem dokonania zamachu. Ponadto może sama podejmować określone działania zmierzające do zapewnienia sobie środków na zrealizowanie zamachu terrorystycznego i w takim celu między innymi gromadzi środki finansowe. Przestępstwo z art. 165a k.k. jest więc przestępstwem powszechnym.

Wydaje się, że zapisy art. 165a k.k. bardziej odzwierciedlają charakter działań sprawcy indywidualnego lub też działającego w ramach organizacji terrorystycznej, w kontekście samofinansowania się, gdy podejmowane czynności zmierzają bezpośrednio wyłącznie do sfinansowania przygotowania do dokonania przestępstwa o charakterze terrorystycznym. Wniosek taki można wysnuć dlatego, że karalności podlega wyłącznie sfinansowanie przestępstwa o charakterze terrorystycznym, a więc spełniającego kryteria określone w art. 115 par. 20 k.k., co uznać trzeba za niewystarczające i nie spełniające warunku prewencyjnego (zapobiegawczego) kary. Takie rozwiązanie wydaje się też mało elastyczne, niepozwalające na pełne penalizowanie zachowań polegających na finansowaniu terroryzmu. Ewentualnie prewencyjne zachowanie można odnieść do zapobiegnięcia indywidualnemu zagrożeniu, nie zaś zapobieżeniu potencjałowi organizacji, która odpowiedzialna jest za przygotowanie i dokonanie zamachu. Niemniej tak sformułowany przepis pozostaje adekwatny wobec określenia finansowania terroryzmu w Konwencji ONZ z dnia 9 grudnia 1999 r. o zwalczaniu finansowania terroryzmu, zgodnie z którym przestępstwem jest podejmowanie opisanych działań także – „do dokonania czynu" (art. 2 ust. 1), oraz Konwencji RE z dnia 16 maja 2005 r. odwołującej się do konwencji ONZ. Z punktu widzenia wielu zachowań samej organizacji terrorystycznej oraz potrzeby jej trwania w czasie w związku z nabywaniem potencjału do zrealizowania zamachu należałoby przyjąć zdecydowanie szerszy cel finansowania działalności terrorystycznej, który nie zamyka się wyłącznie w sfinansowaniu przestępstwa o charakterze terrorystycznym.

[31] A. Marek, *Kodeks karny. Komentarz*, Wolters Kluwer & Lex, Warszawa 2010, wydanie V, komentarz do art. 165a k.k.

W art. 165a k.k. wymienia się następujące przedmioty czynności wykonawczej: środki płatnicze[32], instrumenty finansowe[33], papiery wartościowe[34], wartości dewizowe[35], prawa majątkowe[36] lub inne mienie ruchome[37] bądź nieruchomości[38].

Wskazane przedmioty czynności wykonawczej będą mogły być także przed „posłużeniem" się nimi w ramach realizacji przestępstwa z art. 165a k.k. przedmiotem innego przestępstwa (pierwotnego). Dla przykładu papiery wartościowe (przestępstwa z rozdziału 11 – Odpowiedzialność cywilna i karna – ustawy Prawo o publicznym obrocie papierami wartościowymi), wartości dewizowe (rozdział 8 – Przestępstwa skarbowe i wykroczenia skarbowe przeciwko obrotowi dewizowemu – ustawy Kodeks karny skarbowy), instrumenty finansowe (Dział X ustawy o obrocie instrumentami finansowymi), inne mienie ruchome (Rozdział XXXV – Przestępstwa przeciwko mieniu – Kodeksu karnego). Tym samym mogą one stanowić źródło zgromadzonych środków na cel terrorystyczny uzyskane w wyniku działalności przestępczej (kryminalne źródło finansowania działalności terrorystycznej). Jednocześnie mogą one stanowić przedmiot wcześniejszego legalnego nabycia, otrzymania, kupna itp., a następnie zgodnie z przyjętym sformalizowanym obrotem mogą być przekazane,

[32] Zgodnie z art. 31 i 32 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim środkami płatniczymi są znaki pieniężne emitowane przez NBP.

[33] Zgodnie z ustawą z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi instrumenty finansowe zostały określone w art. 2.

[34] W rozumieniu przepisów ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037, z późn. zm.), ustawy z dnia 21 sierpnia 1997 r. – Prawo o publicznym obrocie papierami wartościowymi (Dz. U. z 1997 r., Nr 118, poz. 754 ze zm.) oraz zgodnie z ustawą Prawo dewizowe (Dz. U. z dnia 5 września 2002 r.).

[35] Zgodnie z ustawą Prawo dewizowe (Dz. U. z dnia 5 września 2002 r.).

[36] Należą do nich własność, użytkowanie wieczyste, użytkowanie, służebności, zastaw, hipoteka, prawa spółdzielcze do lokali i do domu jednorodzinnego, prawa obligacyjne (wierzytelności i prawo związane z abonamentem telefonicznym), prawa majątkowe na dobrach niematerialnych, prawa rodzinne o charakterze niematerialnym, prawa spadkowe, prawa majątkowe o charakterze bezwzględnym, na dobrach niematerialnych niebędących rzeczami (kopaliny, woda energia). M. Bednarek, *Mienie: komentarz do art. 44–5523 Kodeksu cywilnego*, Zakamycze, Kraków 1997, s. 20 i n.

[37] Mieniem jest własność i inne prawa majątkowe (Kodeks cywilny). W piśmiennictwie prawa cywilnego zwracano uwagę, że wyraz „mienie" ma znaczenie niemal synonimiczne względem praw majątkowych, a bardziej precyzyjnie – mienie to pojęcie zbiorcze obejmujące ogół cywilnych praw podmiotowych, w: A. Doliwa, *Prawo cywilne – część ogólna*, Wydawnictwo C.H. Beck, Warszawa 2004, s. 107.

[38] Kodeks cywilny w art. 46 wyróżnia, że nieruchomościami są części powierzchni ziemskiej stanowiące odrębny przedmiot własności (grunty), jak również budynki trwale z gruntem związane lub części takich budynków, jeżeli na mocy przepisów szczególnych stanowią odrębny od gruntu przedmiot własności. Nieruchomościami rolnymi (gruntami rolnymi) są nieruchomości, które są lub mogą być wykorzystywane do prowadzenia działalności wytwórczej w rolnictwie w zakresie produkcji roślinnej i zwierzęcej, nie wyłączając produkcji ogrodniczej, sadowniczej i rybnej (art. 46 prim). Za części składowe nieruchomości uważa się także prawa związane z jej własnością.

zaoferowane w celu sfinansowania przestępstwa o charakterze terrorystycznym. Treść art. 165a k.k. jedynie w pewnym zakresie zapewnia penalizację zachowania określonego jako finansowanie terroryzmu. Zawęża on przedmiotowo i sprawczo podejście, jakie prezentuje np. Konwencja ONZ o zwalczaniu finansowania terroryzmu. Obie regulacje łączy zaś to, że czyn ten może popełnić każdy. Jednakże zawężenie przedmiotu przestępstwa do środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innych, mienia ruchomego oraz nieruchomości nie spełnia wymogów popełniania tego czynu przy wykorzystaniu jakichkolwiek środków (do rozstrzygnięcia pozostaje, czy dotyczy to tzw. kryptowaluty określanej jako *bitcoin* (BTC), która może być wykorzystana w cyberterroryzmie[39]).

Wydaje się jednak, że problem tkwi w tym jak będzie definiowany BTC. Czy jako środek płatniczy, czy jako mienie. W marcu 2014 r. IRS (Internal Revenue Service, amerykański urząd podatkowy) uznał wirtualne waluty za „własność" czy też „mienie" (ang. *property*). Według IRS nie stanowią one waluty, nawet jeśli w niektórych środowiskach i sytuacjach wirtualne waluty zachowują się jak zwykłe waluty. Zdaniem IRS istotne jest to, że wirtualne waluty nie są prawnym środkiem płatniczym w żadnym kraju[40]. Nieco innego zdania był Sąd Okręgowy dla Wschodniego Okręgu Teksasu (lipiec 2013 r.), przed którym stanął Trendon Shavers [Bitcoin Savings and Trust (BTCST)], twórca piramidy finansowej wykorzystującej walutę BTC. Tym samym uznał BTC za środek płatniczy – walutę i związku z tym mógł wszcząć postępowanie o oszustwo w postaci piramidy finansowej z udziałem waluty BTC[41].

MF w maju 2014 r. wskazało, że BTC nie jest określonym środkiem płatniczym, gdyż nie można go zakwalifikować jako krajowego środka płatniczego, zagranicznych środków płatniczych, nie spełnia także definicji pieniądza elektronicznego, a ponadto nie jest towarem giełdowym ani instrumentem finansowym w rozumieniu art. 2 ust. 1 ustawy o obrocie instrumentami finansowymi. BTC może być uznany za prawo majątkowe, ponieważ jest on przedmiotem obrotu oraz posiada określoną wartość majątkową[42]. Ministerstwo opowiedziało się za tym, iż BTC może stanowić aktywa jednostki gospodarczej lub prawa majątkowe należne takiej jednostce. Opcje

[39] Przez dłuższy czas *bitcoin* w Niemczech nie była traktowany jako środek płatniczy. Dopiero w sierpniu 2013 r. niemieckie Ministerstwo Finansów oficjalnie uznało tę wirtualną walutę za środek płatniczy, którym można się posługiwać w prywatnych transakcjach.

[40] Taka decyzja IRS ma duże znaczenie dla spraw podatkowych. Jeśli ktoś zapłaci komuś bitcoinami wartymi 2 tys. dolarów, a potem wartość bitcoinów skoczy do 5 tys. dolarów, osoba ta odnotowała zysk. Według IRS każdy, kto posiada bitcoiny powinien do celów podatkowych obliczać ich zmianę wartości od dnia, gdy wszedł ich w posiadanie [w] http://di.com.pl/bitcoin-to-nie-waluta-wedlug-wladz-usa-co-to-oznacza-49670 (dostęp 11 lipca 2015 r.).

[41] http://di.com.pl/bitcoin-to-waluta-uznal-amerykanski-sad-mozna-odpowiedziec-za-naduzycia-z-jej-udzialem-48640 (dostęp 11 lipca 2015 r.).

[42] O zaliczeniu danego prawa do kategorii prawa majątkowego rozstrzygają łącznie dwie przesłanki, po pierwsze – czy dane prawo może być przedmiotem obrotu, czy jest więc zbywalne, po drugie zaś – czy posiada ono dającą się określić wartość majątkową. [w] II FSK 839/05 – Wyrok NSA z dnia 20 czerwca 2006 r.

lub kontrakty terminowe oparte na BTC jako instrumencie bazowym uznać można za instrumenty pochodne, a tym samym za instrumenty finansowe w rozumieniu ustawy o obrocie instrumentami finansowymi[43]. Dlatego też BTC można zakwalifikować jako prawo majątkowe (a nie jako środek płatniczy) podlegające przedmiotowi czynności wykonawczej z art. 165a kk.

Należy dodać, że art. 165a k.k. wprowadzał na grunt Kodeksu karnego nowy termin „instrument finansowy", który w obrębie ustawy karnej nie posiada definicji legalnej. Wydaje się, że w takim zakresie będzie zachodziła potrzeba odwołania się do art. 2 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[44], jednak nie będzie to rzecz prosta[45].

Powstaje pytanie, kto może wykonywać takie czynności jak: gromadzenie, przekazywanie lub oferowanie. Jeżeli chodzi o czynność gromadzenia – to gromadzić środki może zarówno osoba niebędąca członkiem grupy terrorystycznej, jak i sam członek tej grupy/osoba indywidualna lub działający w mniej sformalizowanej strukturze przestępczej (samofinansowanie). Inaczej rzecz się ma w przypadku przekazywania. Tu raczej należy domniemywać, że chodzi o przekazywanie w celu sfinansowania aktu terrorystycznego – tak więc czynności tej mógłby dokonać wyłącznie podmiot zewnętrzny (mocodawca przestępstwa o charakterze terrorystycznym) wobec indywidualnego zamachowca lub zamachowców działających w ramach organizacji przestępczej. Podobnie w przypadku oferowania. Nie można wykluczyć takiej sytuacji, gdy dana osoba stanie się członkiem grupy terrorystycznej, wcześnie zgromadziwszy środki, i w chwili gdy jest członkiem tej grupy, przekaże je na rzecz tej organizacji (np. poleci wypłacenie czy przesłanie ich z uprzednio założonego konta bankowego). Przy czym karalność „gromadzenia" w przypadku bycia członkiem grupy terrorystycznej wydaje się możliwa także łącznie z karalnością za przynależność do takiej grupy na mocy art. 258 k.k. oraz dokonanie określonego przestępstwa kryminalnego, które stało się źródłem pozyskania środków na sfinansowanie działalności grupy, i przygotowanie zamachu terrorystycznego, a także za zgromadzenie środków celem przygotowania zamachu terrorystycznego[46]. Inaczej będzie w przypadku, gdy pozyskane w ten sposób środki zostaną przez sprawcę „przywłaszczone" na cele osobiste, tym samym uznać należałoby, iż występowałby tu pewnie element niesubordynacji i „nieuczciwości" wobec innych członków orga-

[43] Pismo (syg. FN3/0301/AQG/RWPD-40105/2014/RD-44024) podsekretarza stanu w MF, W. Kowalczyka do Marszałka Sejmu RP z dnia 13 maja 2014 r. jako odpowiedź na interpelacje Posła RP M. Pacholskiego.

[44] Dz. U. z 2005 r., Nr 183, poz. 1538 ze zm.

[45] A. Sakowicz, *Opinia o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw* (Druk nr 1394), 28 stycznia 2009 r., s. 18.

[46] Podobnie K. Wiak, który stwierdza, że procederem tym zajmować się może zarówno osoba zmierzająca popełnić przestępstwo o charakterze terrorystycznym, członek ugrupowania terrorystycznego, jak i „sympatyk" nienależący do takich struktur, w: K. Wiak, *Prawnokarne środki przeciwdziałania terroryzmowi*, Wydawnictwo KUL, Lublin 2009, s. 283.

nizacji. Takie zachowanie mieści się w działaniu z pobudek zysku finansowego, nie zaś przekonań, tym samym ideologicznych. Określony podmiotowo zakres sprawstwa („Kto gromadzi (...) w celu sfinansowania przestępstwa o charakterze terrorystycznym") wydaje się nie wykluczać zachowania polegającego na samofinansowaniu przestępstwa o charakterze terrorystycznym; w takim przypadku sprawca zdaje sobie sprawę z tego, że „nie ma jeszcze wszystkiego", co będzie mu pomocne do jego dokonania (np. brak odpowiedniej ilości komponentów do zbudowania domowym sposobem ładunku wybuchowego, co wymagać będzie zaangażowania środków finansowych). Samofinansowanie będzie więc nosiło elementy przygotowania do popełnienia innego przestępstwa.

R. Zgorzały stwierdza, że „cel terroryzmu może się różnić (i najczęściej się różni) od celu przestępstwa o charakterze terrorystycznym. Jest to zrozumiałe, jeśli się uwzględni, że każda aktywność terrorystyczna musi być oparta na zaangażowaniu się w nią poszczególnych osób. To spostrzeżenie implikuje pytanie o potrzebę rozważania motywu terroryzmu. W literaturze przedmiotu przeważa obecnie pogląd, że odwoływanie się do motywów nie jest konieczne dla wyjaśnienia fenomenu terroryzmu, nawet po uwzględnieniu, iż w praktyce trudno je oddzielić od motywów, jakimi kierują się terroryści. Zdecydowana większość autorów opowiada się obecnie za rozważaniem motywów tylko w związku z konkretnym sprawcą przestępstwa terrorystycznego. Motyw może być wówczas rozpatrywany jako element podmiotowej zawartości bezprawia czynu, choć motywacja nie występuje w roli znamienia typu czynu zabronionego wprost, a pośrednio w związku z zamiarem, współdecydując o zamiarze"[47]. Należy zauważyć, że cel realizowany w ramach art. 165a k.k. nie musi być zgodny z celem określonym w art. 115 par. 20 k.k. Oznacza to, że cel sfinansowania przestępstwa o charakterze terrorystycznym będzie zrealizowany niezależnie od tego, czy organizacja terrorystyczna zrealizuje cel przestępstwa o charakterze terrorystycznym (czy dokonana aktu terrorystycznego). Powstaje pytanie, co będzie w przypadku, gdy nie dojdzie, z różnych przyczyn, do dokonania przestępstwa o charakterze terrorystycznym, mimo że w tym celu zgromadzono, przekazano, zaoferowano środki na jego sfinansowanie. Nie jest wówczas ważne, czy dokonało się przestępstwo terrorystyczne, ważne jest przeświadczenie sprawcy, że środki, jakie oferował, przekazywał, gromadził, chciał przekazać innym osobom w związku z potrzebą finansowego wsparcia przygotowania do przestępstwa o charakterze terrorystycznym. Niezrealizowanie fizyczne przestępstwa o charakterze terrorystycznym przez określony podmiot nie usprawiedliwia tego, kto przekazał środki na jego sfinansowanie. Miał on przecież świadomość, że działa celem wsparcia dokonania jego realizacji. Motyw, jakim się kieruje sprawca z art. 165a k.k., może być dodatkowo rozpatrywany, w szczególności gdy jego poglądy będą pozostawały zbieżne z celem organizacji terrorystycznej przygotowującej zamach finansowany przez zewnętrznego mocodawcę. Ponadto można zauważyć, że przestępstwo z art. 165a k.k. jest na tyle przestępstwem „ukrytym" w świadomości sprawcy, że działając indywidualnie

[47] R. Zgorzały, *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, „Prokuratura i Prawo" 2007, nr 7–8, s. 64.

poprzez gromadzenie środków przeznaczonych na przygotowanie przestępstwa o charakterze terrorystycznym, a następnie od tego zamiaru odstępując – można w takiej sytuacji nigdy nie posiąść wiedzy o tym, że doszło do takiego przestępstwa. Dopiero podjęcie określonych czynności faktycznych (taktycznych i technicznych) może ujawnić zamiar działania sprawcy przestępstwa z art. 165a k.k.

Gromadzić oznacza: zbierać i składać w jednym miejscu jakieś rzeczy, odzyskiwać jakieś wartości lub dobra niematerialne, skupiać wokół siebie ludzi[48]. W omawianym przypadku mamy do czynienia z gromadzeniem „środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innego mienia ruchomego lub nieruchomości". Ponadto zachowanie polegające na gromadzeniu przez sprawcę z art. 165a k.k. powinno być realizowane nie w jakikolwiek sposób, lecz „w celu sfinansowania przestępstwa o charakterze terrorystycznym". Wydaje się, że z gromadzeniem mamy do czynienia nie tylko w wypadku zebrania większej liczby środków, lecz także w przypadku każdego ich pozyskiwania z przeznaczeniem do wykorzystania w przyszłości[49]. Na tle wymienionych przepisów zachowanie sprawcze polega na podjęciu czynności, w następstwie której sprawca uzyskuje określone przedmioty czy informacje lub wchodzi w ich posiadanie[50]. Jeżeli mówimy o gromadzeniu w rozumieniu art. 165a k.k., to można przez to zrozumieć zarówno: fizyczne pozyskiwanie i składowanie rzeczy w danym miejscu (miejscach) na przestrzeni określonego czasu, np. środków płatniczych, jak i rzeczy ruchomych, udokumentowanej formy własności do rzeczy, poprzez czynności prawne, np. nabywanie nieruchomości; deponowanie w skrytce pocztowej/bankowej, na rachunku bankowym, uzyskanie bezzwrotnej pożyczki, powierzanie innej osobie środków na przechowanie (w tym przypadku może to dotyczyć środków finansowych, papierów wartościowych, wartości dewizowych w oparciu o umowę z określonym podmiotem świadczącym w tym zakresie usługi, bądź też bez sporządzania umowy). Ważne jest przede wszystkim to, aby osoba taka, która gromadzi, miała świadomość przeznaczenia tych środków na sfinansowanie przestępstwa o charakterze terrorystycznym (przekazania zgromadzonych środków w bliżej nieokreślonym lub ustalonym okresie dalej, innej osobie lub też zgromadzenia celem własnego wykorzystania do sfinansowania przestępstwa o charakterze terrorystycznym) lub osobistego wykorzystania w tym celu. Niezależnie od takiego podziału można wskazać, że środki te mogą pochodzić ze źródeł zarówno legalnych, jak i nielegalnych. Taka świadomość wskazuje na to, że gromadzenie nie będzie dokonywane na potrzeby własne, na legalne własne działania (i dalsze legalne nimi rozporządzenie), ale w przekonaniu, że rzeczy, nieruchomości, środki finansowe przyczynią się do zrealizowania innego przestępstwa o charakterze terrorystycznym. Przy czym to gromadzenie może być dokonywane zarówno na osobiste potrzeby realizacji celu

[48] http://sjp.pwn.pl/szukaj/gromadzi.

[49] M. Mozgawa, *Kodeks karny. Praktyczny komentarz*, wyd. III, Wolters Kluwer Polska, Warszawa 2010, komentarz do art. 165a kk.

[50] K. Wiak, *Prawnokarne środki przeciwdziałania…*, op. cit., wraz z przywołaną literaturą, s. 283.

z art. 115 par. 20 k.k., jak i na rzecz osób trzecich. Inaczej będzie w przypadku oferowania i przekazania, jeśli czynność ta będzie związana wyłącznie z przekazaniem środków na rzecz osób trzecich. W tym przypadku sprawca z art. 165a k.k. będzie działał jak zleceniodawca (mocodawca) zrealizowania przestępstwa o charakterze terrorystycznym. Ponadto wydaje się, że sama konstrukcja przestępstwa o charakterze terrorystycznym nie ogranicza zachowania sprawcy przestępstwa z art. 165a k.k. Zastosowanie wykładni gramatycznej dla art. 115 par. 20 k.k. każe wnioskować, iż przestępstwo o charakterze terrorystycznym to każdy czyn przestępny spełniający kumulatywnie następujące warunki: zagrożenie karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełnienie go co najmniej w jednym z trzech wskazanych alternatywnie celów, jak również groźba popełnienia takiego czynu[51]. Jednocześnie można wskazać, że identyczny co do strony przedmiotowej czyn będzie lub nie przestępstwem o charakterze terrorystycznym w zależności wyłącznie od zawartości jego strony podmiotowej. To cel sprawcy wyznacza bowiem w takim przypadku terrorystyczny charakter czynu albo jego brak. Takie zaś ujęcie musi skutkować w praktyce powszechnie znanymi trudnościami dowodowymi znamiennymi dla przestępstw kierunkowych[52]. Powstaje też pytanie, co w przypadku, gdy środki te przekazane zostaną na rzecz organizacji terrorystycznej, ale nie na bezpośrednie ich zaangażowanie (np. celem zakupu materiałów wybuchowych czy prekursorów do ich wyprodukowania), lecz wyłącznie skonsumowane będą na cele szkoleniowe (organizacyjne). Art. 165a k.k. wskazuje, że środki mają być przeznaczone konkretnie na sfinansowanie przestępstwa o charakterze terrorystycznym – z art. 115 par. 20 k.k., czyli konkretnie zamachu, nie zaś na sfinansowanie przestępstwa spenalizowanego w art. 258 par. 2 k.k. (w części dotyczącej zakładania organizacji o charakterze terrorystycznym, kierowania nią i bycia jej członkiem). W rzeczywistości znaczna wielkość tych środków będzie konsumowana przez grupę na cele organizacyjne, a nie tylko sfinansowania samego przygotowania i dokonania zamachu. Wydaje się, że zachowania sprawców polegające wprost na finansowaniu przestępstwa terrorystycznego (odpowiedzialność z art. 165a k.k.) oraz na podtrzymywaniu zdolności organizacyjnej do popełnienia takiego zamachu (odpowiedzialność za pomocnictwo z art. 18 par. 3 k.k.) będą się wzajemnie uzupełniały. Tym samym trudne do rozróżnienia będzie ich wykorzystanie. Niemniej w celu określenia odpowiedzialności sprawcy z art. 165a k.k. nadal istotnym elementem pozostanie ocena, że za pomocą

[51] Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: 1) poważnego zastraszenia wielu osób, 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu.

[52] *Przestępczość zorganizowana*, 2200-1CWPK43, wykład specjalizacyjny III–V roku, koordynator projektu C. Sońta, http://informatorects.uw.edu.pl/pl/courses/view?prz_kod=2200-1CWPK43.

oferowanych czy też przekazywanych środków chciał on doprowadzić do zamachu. W jaki sposób środki te wykorzysta organizacja, jest rzeczą wtórną i nie będzie on wpływał na zakres odpowiedzialności sprawcy finansowania terroryzmu. W przypadku zaś samofinansowania się organizacji terrorystycznej sprawca – członek organizacji będzie odpowiadał z art. 258 par. 2 k.k. za działania z zamiarem popełnienia przestępstwa o charakterze terrorystycznym, a jego zachowanie, polegające np. na popełnieniu przestępstwa kryminalnego w celu sfinansowania dokonania przestępstwa o charakterze terrorystycznym, oprócz odpowiedzialności za to przestępstwo, będzie także objęte odpowiedzialnością za przygotowanie do dokonania przestępstwa o charakterze terrorystycznym.

Możliwe jest penalizowanie zachowania polegającego na tym, że prowadzący fundację bądź stowarzyszenie religijne, uzyskujący w sposób legalny kwoty środków płatniczych, członek tej fundacji, nie zdając sobie sprawy z tego, że inny upoważniony do pobierania tych kwot z konta podmiot, przeznaczy je nie na cel zgodny z działaniem fundacji czy stowarzyszenia, lecz pobierze je z celem przekazania członkowi organizacji terrorystycznej na sfinansowanie zamachu terrorystycznego. Będzie to możliwe wtedy, gdy dany podmiot będzie spełniał warunek bycia podmiotem zbiorowym, przy jednoczesnym wykazaniu winy w wyborze lub nadzorze. Zapis w celu sfinansowania przestępstwa o charakterze terrorystycznym wskazuje, że przede wszystkim finansuje się przygotowanie do takiego przestępstwa. Dotyczy to zdobycia środków na materiały do konstrukcji urządzenia wybuchowego, rozpoznanie terenu, niekiedy połączone np. z wynajmem pomieszczeń, zakup odpowiedniej broni, dlatego też trudno określić, że finansuje się przestępstwo tylko na poziomie dokonania. Środki finansowe będą traktowane inaczej, gdy zostaną przeznaczone na takie działania jak: zatarcie śladów, zorganizowanie drogi ucieczki, zapewnienie sobie egzystencji w kolejnych dniach czy miesiącach ukrywania się przed organami ścigania. Niekiedy także w dalszej kolejności na zapewnienie właściwej obsługi prawnej, gdy dojdzie do zatrzymania i procesu. Będą to środki z przeznaczeniem na działalność organizatorską. Samo sformułowanie – „w celu sfinansowania" – wskazuje na finansową potrzebę jego przygotowania aż do fazy realizacyjnej (zasilenie finansowe zmierza do osiągnięcia przez decydenta właściwego poziomu potencjału decyzyjnego). Pozyskanie czy otrzymanie środków jest etapem „przygotowania" niezbędnym do realizacji celu przestępstwa o charakterze terrorystycznym, a więc samego zamachu.

Przekazać oznacza: powierzyć komuś coś, powtórzyć komuś jakąś informację, czyjeś polecenie, słowa itp., wysłać jakiś bodziec, sygnał, impuls do jakiegoś urządzenia, narządu itp., wpłacić pieniądze do banku lub na pocztę, zlecając wypłacenie ich temu, na czyje nazwisko lub konto zostały wpłacone[53]. Przekazywanie polega na przenoszeniu władztwa nad środkami i przedmiotami na inną osobę. Wydaje się, że w grę wchodzi zarówno przekazanie fizyczne (dotyczy w pierwszym rzędzie rzeczy), jak i przekazanie czysto prawne (dotyczy przede wszystkim przekazania

[53] http://sjp.pwn.pl/szukaj/przekazuje.

praw majątkowych)[54], ale także dokonanie transakcji w postaci zlecenia przepływu elektronicznego środków. W przypadku przekazywania należałoby mieć na uwadze podmiot zewnętrzny spoza grupy terrorystycznej (przekazać komuś na czyjąś rzecz, czyli innej osobie niż podmiot gromadzący). Wówczas możemy mieć do czynienia z osobą fizyczną, która świadomie przekazuje wskazane w art. 165a k.k. środki (przedmiot przestępstwa) w celu sfinansowania przestępstwa o charakterze terrorystycznym, jak również z przedstawicielem osoby prawnej (zindywidualizowanie odpowiedzialności), kierującej środki na rzecz sfinansowania przestępstwa o charakterze terrorystycznym. W przypadku przekazania może się ono dokonać poprzez: przekazanie fizyczne (osobiste) rzeczy, środków płatniczych, wartości dewizowych; przekazanie uprawnień do dysponowania prawami majątkowymi, rzeczy ruchomych, nieruchomości w rozumieniu przede wszystkim sformalizowanej formy prawa do niej – aktu notarialnego, aktu darowizny (przekazanie prawne), przekazanie poprzez zadysponowanie przesłaniem środków na rzecz osoby, organizacji odpowiedzialnej za sfinansowanie przestępstwa o charakterze terrorystycznym, przesłanie za pomocą kuriera, firmy pośredniczącej, w przypadku podziemnej bankowości w szczególności przy zastosowaniu metody *havala*, podmiotów pośrednictwa obrotu instrumentami finansowymi[55]. Możliwe jest przekazanie poprzez wysłanie odpowiedniego sygnału (kodu) potrzeby wypłacenia danej osobie środków w przypadku zgłoszenia się i przedstawienia opracowanego hasła (przekazanie pośrednie). Możemy tu mieć także do czynienia z przypadkiem, gdy przedstawiciel przedsiębiorcy nie ma świadomości, że wykonując dyspozycję, przesyła środki celem sfinansowania przedmiotowego przestępstwa. Świadomość czynu będzie posiadał jedynie ten, kto polecił mu zadysponować (świadomość celu przeznaczenia środków). To właśnie taka osoba będzie mogła odpowiadać z art. 165a k.k. Przekazanie tych środków może odbywać się w różny sposób, poprzez przekazanie ich w gotówce, za pomocą instrumentów finansowych dostępnych w instytucjach finansowych, za pomocą systemu „podziemnej bankowości". Wydaje się, że sposobów postępowania może być tyle, ile przewidują przepisy prawa regulujące poszczególne stosunki własnościowe i finansowe oraz zwyczajowe postępowanie, np. w przypadku systemu *havala*[56]. Zachowana może być tu dowolność formy, przy czym osoba nie tylko dysponuje środkami, ale także posiada świadomość ich przeznaczenia w celu sfinansowania przestępstwa o charakterze terrorystycznym. Można przypuszczać, że sprawca, działając w warunkach dokonania przestępstwa z art. 165a k.k., będzie postępował w sposób dyskretny, starając się

[54] Zob. M. Mozgawa, *Kodeks karny. Praktyczny komentarz*..., op. cit., komentarz do art. 165a k.k.

[55] Np. domy maklerskie i banki prowadzące działalność maklerską, banki powiernicze, zagraniczne firmy inwestycyjne i zagraniczne osoby prawne prowadzące działalność maklerską na terytorium Rzeczypospolitej Polskiej w formie oddziału, jeżeli jednocześnie spełniają wymogi bycia instytucją obowiązaną.

[56] System *havala* nie we wszystkich krajach podlega formalnej rejestracji, tym samym stał się on systemem przepływu środków finansowych podlegających wypraniu, rozliczeń transakcji narkotykowych czy sposobem finansowania terroryzmu.

pozostawić jak najmniej śladów swojej działalności, lub też będzie postępował tak, aby stworzyć pozory legalności lub innej działalności (np. transakcji gospodarczej).

Kolejnym sposobem działania (czynności sprawczej) sprawcy przestępstwa z art. 165a k.k. jest oferowanie. Należy mieć tu na uwadze zachowanie polegające na złożeniu określonej propozycji – oferty. Oferowanie oznacza zaproponowanie kupna, usługi, pomocy itp.[57] Oferowanie w rozumieniu komentowanego przepisu polega na proponowaniu przekazania rzeczy lub praw innej osobie, zarówno odpłatnie, jak i nieodpłatnie, faktycznie lub pod jakimkolwiek tytułem prawnym[58]. Niezależnie od tego, kim jest oferent, czy to osoba fizyczna działająca w swoim imieniu, czy jako przedstawiciel osoby prawnej, ważne jest to, że chce przeznaczyć swoje środki finansowe na rzecz celu, jakim jest sfinansowanie przestępstwa o charakterze terrorystycznym. Przy czym inicjatywa działania nie musi leżeć po stronie oferenta. Niekiedy oferta może nadejść ze strony samej organizacji, która ogłaszając manifest, deklarację, program jako organizacja terrorystyczna, zwraca się również o środki finansowe na swoją działalność (powszechność oferty), czy też jest formułowana do określonej ściśle grupy bądź zindywidualizowanego podmiotu (niekiedy nie można przyjąć „oferty", gdy jest ona kierowana z zastrzeżeniem groźby)[59]. Taka sytuacja może mieć miejsce nie tylko na początku działalności, ale także w jej trakcie, w przypadku potrzeby zaangażowania dodatkowych środków bądź też ich braku z innych względów. W takim przypadku przekazanie środków będzie odpowiedzią na „ofertę" złożoną przez organizację terrorystyczną. Postulować należy, aby wykładni tego zachowania dokonywać w szczególności z uwzględnieniem znamion przestępstwa prania pieniędzy (art. 299 k.k.), po nowelizacji z dnia 25 czerwca 2009 r. zostało ono bowiem zrelacjonowane do takiego samego określonego katalogu wartości majątkowych jak w art. 165a k.k.[60] Ponadto należy zauważyć, że ustawodawca szerzej potraktował przedmiot przestępstwa w art. 165a k.k. niż w art. 299 k.k., dodając przedmioty stanowiące instrumenty finansowe niebędące papierami wartościowymi (art. 2 ust. 1 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi)[61].

Przedmiotem ochrony jest bezpieczeństwo państwa i obywateli, zagrożonych działalnością grup terrorystycznych i organizacją zamachów terrorystycznych (bezpieczeństwo powszechne) i mocodawców tych grup oraz działań przestępnych

[57] http://sjp.pwn.pl/szukaj/oferuje.

[58] M. Mozgawa, *Kodeks karny. Praktyczny komentarz*..., op. cit., komentarz do art. 165a k.k.

[59] Zgodnie z przepisem art. 87 Kodeksu cywilnego, kto złożył oświadczenie woli pod wpływem bezprawnej groźby drugiej strony lub osoby trzeciej, ten może uchylić się od skutków prawnych swego oświadczenia, jeżeli z okoliczności wynika, że mógł się obawiać, iż jemu samemu lub innej osobie grozi poważne niebezpieczeństwo osobiste lub majątkowe. Wydaje się jednak, że tego typu rozwiązanie nie wchodzi w grę, pozostając poza zwyczajowo przyjętym (zgodnym z chronionym prawem) obrotem cywilnoprawnym. W omawianym przypadku nie zawsze będziemy mieli do czynienia z zachowaniem sprawcy, który dla sfinansowania zamachu będzie korzystał z ustalonego ramami prawnymi sformalizowanego obrotu finansowego.

[60] T. Przesławski, *Cel w konstrukcji przestępstwa terrorystycznego*, „Prokuratura i Prawo" 2009, nr 5, s. 283.

[61] Dz. U. z 2005, Nr 183, poz. 1538 ze zm.

– a zatem możliwością zrealizowania czynu zabronionego zagrożonego karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, w jednym z celów określonych w art. 115 par. 20 k.k. Uzasadnieniem takiego rozwiązania wydaje się przekonanie, iż kryminalizowane zachowania przybliżają, ułatwiają lub stwarzają warunki do popełniania przestępstw o charakterze terrorystycznym. Tym samym wywołują stan niebezpieczeństwa dla dóbr prawnych w takim stopniu, który usprawiedliwia wprowadzenie zakazu pod groźbą kary[62]. Nie mniej ważne pozostaje również bezpieczeństwo obrotu finansowego (w tym instytucji finansowych)[63], w ramach którego przemieszczają się środki przeznaczane na rzecz sfinansowania przestępstwa o charakterze terrorystycznym.

Misja ewaluacyjna MONEYVAL w 2013 r. zwróciła uwagę na to, że przestępstwo z art. 165a k.k. nie obejmuje finansowania organizacji terrorystycznych lub indywidualnego terrorysty w dowolnym celu i wymaga dowodu zamiaru sfinansowania przestępstwa o charakterze terrorystycznym. Brak szerokiego zdefiniowania przestępstwa uznano za jeden z podstawowych mankamentów przeciwdziałania finansowaniu terroryzmu w Polsce[64]. W ramach 4. rundy ewaluacji wzajemnych MONEYVAL w raporcie z ewaluacji polskiego systemu walki z praniem pieniędzy i finansowaniem terroryzmu, przyjętym w kwietniu 2013 r., wskazano, że poszczególne krajowe instytucje powinny dokonać zmiany przepisów w celu ich dostosowania do artykułu 2 (1) (a) Konwencji o zwalczaniu finansowania terroryzmu, która nie wymaga żadnego konkretnego wspólnego celu dla ataków ustanawiających przestępstwa w traktatach załączonych do konwencji. Zachęca się polskie władze do pilnego zajęcia się brakiem w systemie przeciwdziałania finansowaniu terroryzmu, zwłaszcza w odniesieniu do kryminalizacji finansowania dowolnego celu działania organizacji terrorystycznej i poszczególnych terrorystów. Jako podmioty wykonawcze wskazano Ministerstwo Sprawiedliwości oraz Prokuraturę Generalną. Polska miała do marca 2015 r. czas na podjęcie i wdrożenie właściwych rozwiązań prawnych i organizacyjnych w celu usunięcia stwierdzonych nieprawidłowości oraz usprawnienie krajowego systemu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

W dniu 14 lutego 2014 r. Komisja Kodyfikacyjna Prawa Karnego przy Ministrze Sprawiedliwości wyraziła opinię, że wobec uwag zgłoszonych przez Komitet MONEYVAL zaproponowała „nowe ujęcie penalizacji zachowań polegających na finansowaniu terroryzmu. (...) Komisja Kodyfikacyjna uznała, że czynności polegające na finansowaniu terroryzmu spełniają cechy pomocnictwa do przestępstwa terrorystycznego

[62] K. Wiak, *Prawnokarne środki przeciwdziałania…*, op. cit., s. 282.

[63] Działania przestępców i ich wspólników podejmowane bądź w celu ukrycia pochodzenia korzyści z przestępstwa, bądź przekazania pieniędzy na cele terrorystyczne mogą stanowić poważne zagrożenie dla solidności, uczciwości i stabilności systemu przekazów pieniężnych oraz dla zaufania do całego systemu finansowego. Zob. Rozporządzenie (WE) nr 1781/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie informacji o zleceniodawcach, które towarzyszą przekazom pieniężnym (tekst mający znaczenie dla EOG).

[64] *Anti-Money Laundering and Combating the Financing of Terrorism*, Polska, 11 kwietnia 2013 r., s. 58 i n.

(co obejmuje także pomocnictwo do popełnienia przestępstwa polegającego na udziale w grupie lub związku mającym na celu popełnienie przestępstwa lub organizowaniu takiej grupy lub związku) i nie wymagają odrębnej typizacji". Ponadto, w art. 19 k.k., przewidziano zmianę polegającą na dodaniu par. 1b o następującej treści: „§ 1b. Za pomocnictwo do czynu zabronionego o charakterze terrorystycznym polegające w szczególności na gromadzeniu, oferowaniu lub przekazywaniu wartości majątkowych, szkoleniu terrorystycznym sąd wymierza karę w granicach ustawowego zagrożenia przewidzianego za sprawstwo tego czynu". Zgodnie z art. 18 par. 3 k.k. „Odpowiada za pomocnictwo, kto w zamiarze, aby inna osoba dokonała czynu zabronionego, swoim zachowaniem ułatwia jego popełnienie (...)". Umyślność pomocnika może przybrać postać zamiaru bezpośredniego albo ewentualnego. Tym samym, opierając odpowiedzialność karną z tytułu zachowań polegających na finansowaniu terroryzmu na konstrukcji pomocnictwa, eliminuje się problemy związane z kierunkowym charakterem przestępstwa z art. 165a k.k. Czynności pomocnika i towarzyszący im zamiar odnoszą się do konkretnego czynu zabronionego. Na tej podstawie można by wnioskować, że niesprecyzowane przekazywanie środków terroryście (organizacji terrorystycznej) pozostawałoby poza zakresem wyznaczonym treścią art. 18 par. 3 k.k. Z drugiej strony, na co trafnie zwrócono uwagę w uzasadnieniu projektu, art. 18 par. 3 k.k. „obejmuje także pomocnictwo do popełnienia przestępstwa polegającego na udziale w grupie lub związku mającym na celu popełnienie przestępstwa lub organizowaniu takiej grupy lub związku", które stanowią czyny zabronione *sui generis*. Tym samym przy zastosowaniu konstrukcji pomocnictwa zakresem kryminalizacji objęty będzie znaczny zakres przypadków umyślnego przekazania środków organizacji terrorystycznej. W związku z przedstawioną nową koncepcją Komisja Kodyfikacyjna zaproponowała uchylenie art. 165a k.k.[65]

Zaproponowane rozwiązanie odbiega od prezentowanych przez FATF i MONEYVAL zaleceń rekomendujących potrzebę usankcjonowania finansowania terroryzmu jako samoistnego przestępstwa. Ponadto takie rozwiązanie znacząco może wpłynąć na funkcjonowanie polskiego modelu przeciwdziałania finansowaniu terroryzmu opartego na działalności GIIF. Przedstawiona propozycja wskazuje na niezrozumienie istoty finansowania terroryzmu, która polega nie tylko na „pomocnictwie" finansowym w dokonaniu zamachu terrorystycznego, ale także na finansowaniu samej organizacji terrorystycznej. Dlatego też zaproponowane rozwiązanie nadal zbyt wąsko traktuje uznany już i rozpoznany obszar finansowego wspierania działalności terrorystycznej przez różnego rodzaju mocodawców. Jeszcze raz trzeba podkreślić, że stanowisko, jakie zostało zaprezentowane na posiedzeniu Komisji Kodyfikacyjnej, nie odzwierciedla współczesnych kierunków penalizacji zachowań okołoterrorystycznych związanych ze wspieraniem finansowym terroryzmu. Przyjęcie w zaproponowanej wersji niniejszego stanowiska pozostaje „ucieczką" od problemów związanych

[65] Opinia Komisji Kodyfikacyjnej Prawa Karnego przy Ministrze Sprawiedliwości (przyjęta po dyskusji plenarnej w dniu 18.02.2014 r.), http://bip.ms.gov.pl/pl/dzialalnosc/komisje-kodyfikacyjne/komisja-kodyfikacyjna-prawa-karnego/opinie-komisji-kodyfikacyjnej-prawa-karnego/.

z identyfikacją zachowań sprawców finansowania terroryzmu, wprowadzi chaos w działalności instytucji obowiązanych, nie mówiąc już o wywarciu istotnego negatywnego wpływu na kształt zapisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Sama istota art. 165a k.k. musi się zawierać w jej walorze prewencyjnym (niedopuszczenia do skutecznego zorganizowania zamachu) na wypadek wystąpienia określonego zachowania formułującego podstawy do dalszych działań. Nie można także zapomnieć o równoległych pracach analitycznych w zakresie typowania oceny realnego finansowego wsparcia na rzecz działań terrorystycznych. Stąd też zdecydowana rola działań analitycznych służb specjalnych pod kątem ekonomiki i realności zagrożenia.

Stąd też dla pełniejszego zapewnienia właściwego funkcjonowania systemu przeciwdziałania opartego także na przepisach kodeksu karnego proponuje się przyjęcie następujących rozwiązań: utrzymanie odrębnej penalizacji zachowania określonego jako finansowanie terroryzmu w art. 165a k.k., przy jednoczesnej jego modyfikacji w następującym zakresie:

a. objęcia zakresem kryminalizacji wszelkiej postaci dostarczania środków na rzecz organizacji terrorystycznej lub indywidualnego terrorysty poprzez dodanie zapisu „w szczególności";
b. wykreślenia znamion strony podmiotowej w postaci zamiaru kierunkowego – celu finansowania przestępstwa o charakterze terrorystycznym;
c. objęcia penalizacją zarówno finansowania skonkretyzowanego czynu kwalifikującego się jako przestępstwo o charakterze terrorystycznym, jak i finansowania form organizacyjnych (grupy, związku) działań terrorystycznych, w ramach której przygotowywane są i dokonywane przestępstwa o charakterze terrorystycznym;
d. zapewnienia objęcia karalnością zachowania osoby indywidualnej, która czyni finansowe przygotowania do zorganizowania i popełnienia przestępstwa o charakterze terrorystycznym.

Tym samym proponuje się następujące brzmienie art. 165a Kodeksu karnego:

„Kto, w szczególności, gromadzi, zarządza, oferuje, przekazuje, także poprzez działanie niezgodne z prawem, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe, inne środki będące w obrocie płatniczym, mienie ruchome lub nieruchomości, w taki sposób, że mogą one zostać użyte w całości lub w części do:

– popełnienia przestępstwa o charakterze terrorystycznym lub
– zapewnienia, w jakikolwiek sposób, funkcjonowania zorganizowanej grupy lub związku, o którym mowa w art. 258 par. 2 k.k., lub innego podmiotu, mającego na celu popełnienie przestępstwa o charakterze terrorystycznym, podlega karze ...".

Dalsze prace nad nowelizacją art. 165a kk podjęto w Ministerstwie Sprawiedliwości (MS) w 2015 r. W projekcie z 30 marca 2015 r. MS zaproponowało nowe brzmienie art. 165a kk., w następującej wersji: *Kto gromadzi, przekazuje lub oferuje środki płatnicze,*

instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w zamiarze sfinansowania przestępstwa o charakterze terrorystycznym albo udostępnienia ich zorganizowanej grupie lub związkowi mającym na celu popełnienie takiego przestępstwa lub osobie biorącej udział w takiej grupie lub związku, podlega karze pozbawienia wolności od lat 2 do 12. W dniu 7 lipca 2015 r. Rząd RP przyjął projekt zmiany Kodeksu karnego w zakresie między innymi art. 165a k.k. a 10 lipca 2015 r. projekt wpłynął do Sejmu RP. W uzasadnieniu do niniejszego projektu zaznaczono, że w obecnym stanie prawnym karze podlega osoba, która gromadzi, przekazuje lub oferuje pieniądze lub inne dobra w celu sfinansowania przestępstwa o charakterze terrorystycznym. Jest to więc przestępstwo wymagające wykazania sprawcy zamiaru bezpośredniego o charakterze kierunkowym (*dolus directus coloratus*). Omawiany przepis nie obejmuje zatem finansowania organizacji, o której wiadomo, że zajmuje się działalnością terrorystyczną, np. jeżeli osoba przekazująca środki zakłada, że przeznaczone one zostaną na inną działalność. Charakter takiej organizacji i brak przejrzystości finansowej umożliwiają jednak łatwe sprzeniewierzenie środków przeznaczonych na jej legalną działalność i wykorzystanie ich w innym celu niż zakładany przez darczyńcę. Podobne stanowisko zajął Trybunał Sprawiedliwości UE w wyroku z 29.06.2010 r. w sprawie C-550/09 przeciwko E. i F., wydanym na gruncie rozporządzenia Rady (WE) nr 2580/2001 z dnia 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu[66]. W orzeczeniu tym Trybunał stwierdził, że: „Fundusze udostępnione organizacji terrorystycznej same w sobie niosą ryzyko sprzeniewierzenia celem wspierania takiej działalności (...). Takie udostępnienie jest zatem objęte zakazem (…) i podlega sankcjom karnym przewidzianym przez właściwe prawo krajowe, niezależnie od dowodu, czy rzeczone fundusze zostały skutecznie wykorzystane przez omawianą organizację na działalność tego typu [terrorystyczną]" . Rekomendacja MONEYVAL opiera się na tym samym założeniu. Zgodnie z nią finansowanie terroryzmu to nie tylko przekazywanie środków w celu popełnienia przestępstwa o charakterze terrorystycznym, ale również przekazanie środków organizacji terrorystycznej lub terroryście w jakimkolwiek celu. Konieczność wykonania tej rekomendacji wynika także z *Planu działań Narodowy Program Antyterrorystyczny na lata 2015–2019* (priorytet 9)[67].

Należy jednak zauważyć, że postulat zmierzający do optymalnego i w miarę uniwersalnego zapewniania karalności zachowań sprawców polegających na finansowaniu terroryzmu nie będzie spełniony, gdy oprócz zaproponowanego rozwiązania nie zostaną zrealizowane również inne elementy przeciwdziałania. Należą do nich:

a. zwiększenie nadzoru nad pozabankowymi instytucjami oferującymi zbliżone usługi finansowe (*paralel-banki* czy tzw. *parabanki*);
b. poszukiwanie hybrydowych rozwiązań przesyłów środków finansowych wiążących dotychczasowe kontynentalne i islamskie instrumenty finansowe, co pozwoli wyeliminować tym samym niezgodne z prawem wykorzystywanie takich instrumentów jak *havala*;

[66] Dz. Urz. UE L 344 z 28.12.2001, s. 70, z późn. zm.

[67] http://orka.sejm.gov.pl/Druki7ka.nsf/Projekty/7-020-1406-2015/$file/7-020-1406-2015.pdf.

c. objęcie karalnością także zachowania polegającego na organizowaniu sieci terrorystycznej, kierowaniu (zarządzaniu) nią oraz pozostawaniu jej członkiem. Postulat ten związany jest z poszerzeniem zakresu art. 258 k.k. o inną organizacyjną formę popełniania przestępstw w postaci „sieci przestępczej" z możliwością wyodrębnienia karalności zakładania, kierowania i bycia członkiem grupy, związku lub sieci mającym na celu popełnianie przestępstw o charakterze terrorystycznym.
d. umieszczenie przestępstwa z art. 165a k.k. w katalogu przestępstw ściganych przez Agencję Bezpieczeństwa Wewnętrznego (art. 5)[68].

Streszczenie

Polski ustawodawca spenalizował finansowanie terroryzmu jako odrębne przestępstwo w 2009 roku. Umieszczone ono zostało w artykule 165a Kodeksu karnego. Istotna zmiana treści artykułu opracowana została przez Ministerstwo Sprawiedliwości. Projekt zmiany ustawy karnej w tym zakresie został przekazany przez rząd do Sejmu. W projekcie wskazano, że sprawcą będzie ten, kto nie tylko działa w zamiarze bezpośrednim, ale w jakimkolwiek. Karane będzie nie tylko, jak dotychczas, finansowanie pojedynczego sprawcy przestępstwa o charakterze terrorystycznym, ale również grup i związków, które dokonują takiego rodzaju przestępstw. Ważną rolę w przygotowaniu polskich rozwiązań w zakresie karania finansowania terroryzmu odegrały międzynarodowe organizacje FATF i Komitet MONEYVAL. Dotychczas w Polsce nie skazano żadnej osoby za finansowanie terroryzmu. Jedynie postawione zostały zarzuty obywatelom wyznania islamskiego za finansowanie Państwa Islamskiego poprzez gromadzenie funduszy na jego rzecz.

Słowa kluczowe: finansowanie terroryzmu, podżeganie, pomocnictwo, zamiar bezpośredni, gromadzenie, oferowanie, przekazywanie, środki pieniężne

Summary

Terrorist financing was criminalized in Polish legislation as a separate offense in 2009. It was placed in article 165a of the Penal Code. A significant change article content was developed by the Ministry of Justice. Draft amendment to the criminal law in this regard was submitted by the Government to the Parliament. The project indicated that the perpetrator is the one who not only works in the immediate intention but in any. It will not only be punished, so far, financing a single perpetrator of crimes of a terrorist nature, but also groups and associations which make this kind of crime. An important role in the preparation of Polish solutions to penalize the financing of terrorism have played international organizations FATF and MONEYVAL. So far, in Poland, not any person was convicted for the financing of terrorism. Only the allegations have been raised citizens of the Islamic religion as the Islamic State funding through fundraising on his behalf.

Keywords: financing of terrorism, inciting, aiding and abetting, the intention to direct, the collection, offering, transfer, financing funds

[68] Zob. inicjatywa ustawodawcza grupy senatorów, ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 967, Senatu RP VIII kadencji z dnia 25 czerwca 2015 r.).

Krzysztof Krassowski

WYBRANE ELEMENTY INFORMATYZACJI POLSKIEJ POLICJI

Selected elements of informatization of the Polish Police

Wprowadzenie

We współczesnym świecie informacji cyfrowej wykonywanie przez Policję oraz inne uprawnione organy państwa ich podstawowych, określonych ustawowo zadań związanych z najszerzej rozumianymi zapewnianiem bezpieczeństwa publicznego oraz ochroną interesów państwa, a także przeciwdziałaniem oraz zwalczaniem przestępczości, nie byłoby możliwe bez dysponowania przez przywołane instytucje stosowną infrastrukturą teleinformatyczną oraz odpowiednimi narzędziami z zakresu technologii informacyjnych. Umożliwiają one pozyskiwanie, przetwarzanie, przesyłanie oraz wykorzystywanie informacji związanych zarówno z realizacją wszelkich działań o charakterze policyjnym, jak również – co często bywa niesłusznie traktowane w sposób marginalny – z funkcjonowaniem wewnętrznym i zewnętrznym samych instytucji organów ścigania.

Sposób oraz tempo wdrażania technologii informacyjnych w praktykę funkcjonowania Policji jako instytucji – czy jeszcze bardziej ogólnie jej informatyzacja – ma zatem bezpośredni wpływ na realne możliwości tej formacji w zakresie ochrony życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami, ochronę bezpieczeństwa i porządku publicznego, inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń, wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców, gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych, prowadzenie zbiorów danych zawierających informacje o odciskach linii papilarnych osób oraz o wynikach analizy kwasu deoksyrybonukleinowego (DNA), a także współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi, w tym organami i instytucjami Unii Europejskiej – by wymienić tylko część z podstawowych zadań określonych w art. 1 ustawy o Policji[1].

Przenosząc dyskurs na poziom konkretu, należy uznać, że stopień aktualnej dostępności technologii informacyjnych wpływa zatem istotnie i bezpośrednio na sposób i efektywność prowadzenia wszelkich działań Policji o charakterze kryminalistycznym, realizowanych zarówno w toku klasycznych i rutynowych czynności, takich jak identyfikacja osób zatrzymywanych, oględziny miejsca zdarzenia czy

[1] Ustawa z dnia 6 kwietnia 1990 r. o Policji (j.t. Dz.U. 2015.0.355).

przesłuchanie świadka, jak również warunkuje możliwość oraz jakość wykonywania wszelkich rodzajów zadań opartych na urządzeniach i technologiach badań kryminalistycznych realizowanych przez policyjne laboratoria kryminalistyczne. Jest także wyznacznikiem nowoczesności i efektywności policyjnych baz danych – od KSIP poprzez AFIS i GENOM po System Informacji Operacyjnych. Dodatkowo informatyzacja ma zasadnicze znaczenie dla codziennego funkcjonowania i efektywności pracy całych jednostek i pojedynczych funkcjonariuszy Policji, a także wykorzystywania przez tę instytucję interaktywnych kanałów komunikacji oraz wymiany informacji ze światem zewnętrznym (społeczeństwem), co odgrywa niebagatelną rolę, zwłaszcza w prewencji aktualnych zagrożeń szczególnie poważnymi przestępstwami, w tym o charakterze globalnym – takimi jak terroryzm.

Informatyzacja Policji w kontekście informatyzacji administracji publicznej

Policja i jej informatyzacja nie mogą być postrzegane w oddzieleniu od szerszego kontekstu systemowej informatyzacji całej administracji, realizowanej w ramach określonej i planowej polityki państwa. Zgodnie z dyspozycją art. 5 ustawy o Policji jej Komendant Główny jest centralnym organem administracji rządowej, właściwym w sprawach ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego. Nie ulega zatem żadnej wątpliwości, że Policja jest organem administracji publicznej, która – wobec braku legalnej definicji tego pojęcia w polskim systemie prawnym[2] – może być określona jako działalność celowa, praktyczna, konkretna, planowa, bezpośrednia, władcza, regulująca, twórcza, kontrolowana, oparta na prawie, trwała, organizatorska, kierownicza i mająca na celu realizację zadań publicznych[3]. W świetle wielkości tej instytucji, w której zatrudnienie na 1 stycznia 2015 roku wynosiło niemal 100 000 osób, a jej budżet w bieżącym roku sięga kwoty 8,6 mld złotych[4], a także znaczenia zadań publicznych realizowanych przez Policję dla właściwego funkcjonowania państwa, wydaje się, że kwestia jej informatyzacji powinna racjonalnie stanowić stosowny element w ramach ogólnej i całościowej informatyzacji administracji publicznej, wyrażanej na gruncie odpowiednich regulacji prawnych, a także różnego rodzaju dokumentów strategicznych o charakterze politycznym.

Kwestia stosowania technologii informacyjnych w administracji państwowej stała się przedmiotem uwagi prawodawcy jeszcze w latach 90. XX wieku, ale traktowana była wówczas w sposób mało spójny, fragmentaryczny. Ocenia się, że

[2] L. Kaczmarski, *Ewolucja pojęcia administracji publicznej w polskiej doktrynie prawa administracyjnego po II wojnie światowej*, PWSZ IPiA „Studia Lubuskie" 2009, t. V (Prace Instytutu Prawa i Administracji Państwowej Wyższej Szkoły Zawodowej w Sulechowie), s. 229.

[3] P.A. Borowska, A. Brzostek, D. Kościuk, A. Modrzejewski, J. Radwanowicz-Wanczewska, P. Sitniewski, A. Suwałko-Karetko, P.J. Suwaj, R. Suwaj, M. Wenclik, M. Wincenciak (red. P.J. Suwaj), *Prawo administracyjne. Ćwiczenia*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2008, s. 19.

[4] Wykorzystano 98 775 etatów z nominalnych 102 309 – dane za: www.policja.pl, dostęp 20 czerwca 2015 r.

przedmiotowa materia stanowiła przykład tzw. resortowego tworzenia prawa, a zatem w poszczególnych aktach zakres regulacji był *de facto* ograniczony do konkretnie wyznaczonych obszarów zastosowania partykularnych technologii, same regulacje zaś były często nie do końca przemyślane[5]. Aktem prawnym o fundamentalnym znaczeniu dla przedmiotowego zagadnienia stała się ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, uchwalona 17 lutego 2015 roku[6], która dokonała kompleksowej regulacji problematyki informatyzacji administracji publicznej. Ustawa obejmuje swoim zakresem podmioty publiczne, wśród których znajdują się organy administracji rządowej (w tym Policja), organy kontroli państwowej i ochrony prawa, sądy, a także jednostki organizacyjne prokuratury. Istotnym elementem regulacji (art. 5 w brzmieniu z 2005 roku) było ustanowienie instytucji Planów Informatyzacji Państwa przyjmowanych w drodze rozporządzeń Rady Ministrów oraz Strategii Rozwoju Społeczeństwa Informacyjnego – w formie uchwały Rady Ministrów. Plany miały określać m.in. organizacyjne i technologiczne instrumenty rozwoju społeczeństwa informacyjnego oparte na przyjmowanej strategii, koordynować realizowane przez więcej niż jeden podmiot publiczny projekty informatyzacji, a także zasady modernizacji oraz łączenia systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Zawierały one przy tym określenie priorytetów rozwoju systemów teleinformatycznych używanych do realizacji zadań publicznych oraz systemów teleinformatycznych, których realizacja wypełniać miała cele określone w strategiach, wytyczających główne kierunki, cele i zadania na rzecz budowy społeczeństwa informacyjnego. Jak wykazała praktyka, ostatecznie opracowano trzy takie plany:

- rozporządzenie Rady Ministrów w sprawie Planu Informatyzacji Państwa na rok 2006[7];
- rozporządzenie Rady Ministrów w sprawie Planu Informatyzacji Państwa na lata 2007–2010[8];
- projekt rozporządzenia Rady Ministrów w sprawie Planu Informatyzacji Państwa na lata 2011–2015 – który poddany szerokiej krytyce[9] nie został ostatecznie uchwalony i nie wszedł w życie.

Plany Informatyzacji Państwa zostały zastąpione przyjmowanymi w drodze uchwały Rady Ministrów Zintegrowanymi Programami Informatyzacji Państwa, stanowiącymi programy rozwoju w rozumieniu art. 15 ust. 4 pkt 2 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju[10]. Pierwszy taki program

[5] G. Sibiga, *Informatyzacja administracji publicznej w Polsce*, „Edukacja Prawnicza" 2011, nr 3(123), s. 1 – www.edukacjaprawnicza.pl, dostęp on line 24 czerwca 2015 r.
[6] Dz.U. z 2005 r., Nr 64, poz. 565.
[7] Dz.U. z 2006 r., Nr 147, poz. 1064.
[8] Dz.U. z 2007 r., Nr 61, poz. 415.
[9] Szerzej: Opinia Polskiego Towarzystwa Informatycznego na temat projektu rozporządzenia Rady Ministrów w sprawie Planu Informatyzacji Państwa na lata 2011–2015, z dnia 26.08.2011, www.pti.org.pl, dostęp on line 26 czerwca 2015 r.
[10] Dz.U. z 2006 r., Nr 227, poz. 1658.

został opracowany i uchwalony na początku 2014 roku i objął swoim zasięgiem lata 2014–2020[11].

Analiza treści ww. planów wskazuje, że dotyczyły one rozwijania infrastruktury teleinformatycznej, z której w większym lub mniejszym stopniu korzystać miała również w różnych aspektach realizacji swoich zadań Policja – w tym przede wszystkim w ramach zintegrowanej sieci teleinformatycznej administracji publicznej STAP, elektronicznej platformy usług administracji publicznej e-PUAP oraz systemu centralnej ewidencji pojazdów i kierowców CEPIK – stanowiących priorytety Planu 2006. Dodatkowo oprócz kontynuacji wspomnianych priorytetów w planie na lata 2007–2010 przewidywał on nowe zadanie, tj. realizację centralnego węzła polskiego komponentu systemu SIS II oraz VIS. Projekt ten, mający zasadnicze znaczenie dla rozwoju zdolności informacyjnych Policji i innych organów państwa zaangażowanych w zapewnianie bezpieczeństwa publicznego, integrował istniejące już systemy teleinformatyczne, takie jak m.in. Krajowy System Informacyjny Policji, Odprawa SG, Pobyt, Centralna Ewidencja Wydanych i Unieważnionych Paszportów oraz CEPIK. Z kolei zintegrowany program na lata 2014–2020 przewiduje w ramach ustalonych priorytetów do wdrożenia na poziomie centralnym takie leżące w sferze zainteresowania Policji kwestie, jak m.in.:

- rozwijanie sieci bezpieczeństwa i powiadamiania ratunkowego w postaci systemów masowego powiadamiania o zagrożeniach, informowania obywateli w wiadomościach wysyłanych na urządzenia mobilne o konkretnych zagrożeniach i zdarzeniach, w tym o charakterze kryminalnym;
- dalszą rozbudowę sieci teleinformatycznej Policji oraz dziedzinowych systemów teleinformatycznych, ze szczególnym uwzględnieniem wymiany informacji i współdziałania służb bezpieczeństwa publicznego i ratownictwa;
- rozbudowę systemu powiadamiania ratunkowego; dzięki temu obywatel dodzwoni się do profesjonalnego operatora numeru alarmowego (112), który będzie w stanie obsłużyć zgłoszenie z każdej części kraju, korzystając z systemu teleinformatycznego wyposażonego w niezbędne nowoczesne narzędzia monitorowania i wymiany informacji;
- budowę ogólnopolskiego cyfrowego systemu łączności radiowej dla służb bezpieczeństwa publicznego (w oparciu o standard TETRA);
- system lokalizacji w terenie osób dokonujących zgłoszeń za pomocą urządzeń mobilnych[12].

Oprócz przedstawionych powyżej regulacji prawnych dotyczących informatyzacji całej administracji publicznej, w tym i organów ścigania, wypada wspomnieć o wydanych na przestrzeni ostatnich kilkunastu lat dokumentach o charakterze politycznym, będących wyrazem strategii państwa w zakresie budowy społeczeństwa informacyjnego. Za ich genezę można uznać uchwałę Sejmu RP w sprawie budowania

[11] Uchwała nr 1/2014 Rady Ministrów z dnia 8 stycznia 2014 r.

[12] *Zintegrowany Program Informatyzacji Państwa*, Ministerstwo Administracji i Cyfryzacji, listopad 2013, s. 38–39.

podstaw społeczeństwa informacyjnego z 2000 roku[13], skonkretyzowaną następnie dokumentami rządowymi, w tym przede wszystkim wzorowanym na unijnej inicjatywie eEuropa planie działania na lata 2001–2006 pod nazwą ePolska[14]. Dokument ten, wydany przez Ministerstwo Gospodarki, za absolutny priorytet uznawał budowę i rozwój infrastruktury teletransmisyjnej, dostrzegając również specyficzne potrzeby rozwijania teleinformatyki policyjnej. Wyrażało się to w sprecyzowanych planach dążenia do poprawy bezpieczeństwa państwa poprzez:

- organizowanie wsparcia z wykorzystaniem technologii informacyjnych i komunikacyjnych dla służb Policji,
- wzmocnienie mechanizmów współpracy z Unią Europejską w walce z przestępczością zorganizowaną,
- zwiększenie skuteczności działań operacyjno-rozpoznawczych i prewencyjnych przez wprowadzenie do policyjnej praktyki powszechnego i pełnego dostępu do potrzebnych informacji,
- zwiększenie skuteczności kierowania siłami policyjnymi odpowiedzialnymi za porządek publiczny i bezpieczeństwo obywateli w dużych aglomeracjach miejskich,
- stworzenie sieci oraz systemów umożliwiających współdziałanie służb i instytucji (pogotowia ratunkowego, służb ratownictwa technicznego)[15].

Kolejny dokument pod nazwą ePolska 2004, nadal uznając budowę sieci teleinformatycznej za główny priorytet, dostrzegał też kwestie związane z rozbudowywaniem policyjnego systemu KSIP, infrastruktury teleinformatycznej oraz Zintegrowanego Systemu Ewidencji Straży Granicznej, a także systemu CEPIK[16]. Opracowany w 2005 roku dokument strategiczny znany jako iPolska[17], zawierający strategię na lata 2005–2013, koncentrował się już raczej na kwestiach zapewnienia dostępności usług e-administracji, w tym możliwości dokonywania różnego rodzaju zgłoszeń na Policję w ramach rozwijanej platformy e-PUAP. Podobne treści, koncentrujące się w zasadzie całkowicie wokół e-usług, zawierał przedstawiony po zmianie rządu w 2007 roku nowy dokument strategii rozwoju społeczeństwa informacyjnego w Polsce do roku 2013[18]. Trend ten jest ugruntowany przez najnowszy dokument

[13] „Monitor Polski" 2000, nr 22, poz. 448.

[14] A. Ogonowska, *Polska polityka rozwoju społeczeństwa informacyjnego w latach 2000–2012*, „Studia Europejskie" 2013, nr 2, s. 96–97.

[15] *ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001–2006*, Ministerstwo Gospodarki, Warszawa 2001, s. 48–49, kbn.icm.edu.pl, dostęp 19 czerwca 2015 r.

[16] *Strategia Informatyzacji Rzeczypospolitej Polskiej – ePolska na lata 2004–2006*, Ministerstwo Nauki i Informatyzacji, Warszawa 2003, s. 44–45, www.epractice.eu, dostęp 19 czerwca 2015 r.

[17] *Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020*, Ministerstwo Nauki i Informatyzacji, Warszawa 2005, archiwum-ukie.polskawue.gov.pl, dostęp 19 czerwca 2015 r.

[18] *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2008, www.umwd.dolnyslask.pl, dostęp

strategiczny zawierający wizję cyfrowego rozwoju kraju (Polska Cyfrowa), w tym usług e-administracji na lata 2013–2030[19].

Warto także odnotować regulację o charakterze specyficznym, odnoszącą się wyłącznie do modernizacji służb odpowiedzialnych za bezpieczeństwo publiczne, a także ochronę życia i mienia, w której znaleźć można dyspozycje wpływające bezpośrednio na tempo informatyzacji m.in. polskiej Policji. Jest nią ustawowy program modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Biura Ochrony Rządu w latach 2007–2009[20], przedłużony w 2009 roku stosowną nowelizacją ustawy do roku 2011[21]. Program ten miał na celu stworzenie warunków do pełnej realizacji przez formacje ochrony bezpieczeństwa i porządku publicznego zadań ustawowych oraz istotną poprawę skuteczności działania tych formacji, warunkującą zapewnienie bezpieczeństwa państwa oraz obywateli. W jego ramach realizowane były przedsięwzięcia związane m.in. z zakupem, wymianą oraz modernizacją sprzętu oraz systemów teleinformatycznych Policji. Ustawa zapewniała przy tym środki z budżetu państwa na realizację priorytetowych zadań modernizacyjnych. W odniesieniu do sfery teleinformatyki w samej Policji alokowane środki sięgały kwoty 860 milionów złotych (w wersji programu na lata 2007–2011). Niestety ogólnoeuropejski kryzys gospodarczy z roku 2009 spowodował częściowe załamanie się planów wydatków budżetowych i realizacji zamierzeń modernizacyjnych. Mimo to w swojej informacji o wynikach kontroli realizacji programu modernizacji Policji Najwyższa Izba Kontroli pozytywnie oceniła realizację przedmiotowego programu, bez względu na stwierdzone w Komendzie Głównej Policji istotne nieprawidłowości, mające wpływ na kontrolowaną działalność[22]. Z powodu zmieniających się na niekorzyść warunków otoczenia gospodarczego, mimo podejmowanej inicjatywy w tym zakresie, program modernizacyjny nie był ostatecznie kontynuowany w postaci odrębnej regulacji ustawowej.

Wybrane programy informatyzacji polskiej Policji

Informatyzacja Policji to zagadnienie niezwykle kompleksowe, proces dokonujący się w ramach wielu składających się na całość działań oraz projektów fragmentarycznych, adresujących poszczególne potrzeby motywowane nierzadko bardziej celami doraźnymi niż długofalowymi planami czy strategiami. Wydaje się jednak, że na przestrzeni ostatnich kilkunastu lat w Policji realizowanych było kilka projektów w szeroko rozumianej sferze informatyzacji, które miały szczególne znaczenie

19 czerwca 2015 r.

[19] *Polska 2030. Trzecia fala nowoczesności. Długookresowa strategia rozwoju kraju*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, www,mac,gov.pl, dostęp 19 czerwca 2015 r.

[20] Dz.U. z 2007 r., Nr 35, poz. 213.

[21] Dz.U. z 2009 r., Nr 144, poz. 1174.

[22] *Informacja o wynikach kontroli realizacji Programu modernizacji Policji ustanowionego ustawą z dnia 12 stycznia 2007 r.*, Departament Obrony Krajowej i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli, dokument KOB-4101-03-00/2010, Warszawa 2011, nik.gov.pl, dostęp 24 czerwca 2015 r.

dla jej potencjału informacyjnego, efektywności wspierania procesu wykrywczego i prowadzenia czynności o charakterze kryminalistycznym, a także dla zewnętrznego postrzegania Policji oraz jakości jej – tak pożądanej – współpracy ze społeczeństwem. Należą do nich:

1. Sukces budowy i rozwoju infrastruktury teletransmisyjnej Policji (sieci POLWAN i OST 112)

Własna sieć teletransmisyjna, obejmująca terytorium całego kraju i łącząca ze sobą rozproszone jednostki Policji, jest newralgicznym elementem jej systemu informatycznego. W dużym uproszeniu stanowi ona podstawę bezpiecznej wymiany wszelkich informacji oraz dostępu do utrzymywanych centralnie zasobów informacyjnych (w tym baz danych takich jak AFIS czy GENOM) przez uprawnionych funkcjonariuszy. Jest ona zatem fundamentem umożliwiającym bezcenne wsparcie informacyjne w czasie rzeczywistym w zakresie procesu wykrywczego, a także wszelkich czynności o charakterze administracyjnym, realizowanych przez Policję.

Budowa sieci teletransmisyjnej stanowiła zatem priorytet u zarania informatyzacji Policji jeszcze w latach 90. XX wieku. Pierwszą siecią tego typu był budowany w latach 1997–2003 POLWAN, oparty na węzłach zlokalizowanych w komendach wojewódzkich Policji. Sieć ta zapewniała sprawną komunikację na poziomie stosowanych wówczas technologii i w kolejnych latach była rozbudowywana oraz doposażana, tak aby sprostać ewoluującym potrzebom informacyjnym Policji[23]. Warto przy tym podkreślić, że rozbudowa sieci POLWAN w latach 2004–2006 była realizowana w zasadzie ze środków Unii Europejskiej, w ramach programów Funduszu Schengen. Fundusz ten został przeznaczony dla nowych członków Unii, w tym Polski, w celu sfinansowania działań na nowych granicach zewnętrznych Unii Europejskiej. Przed przystąpieniem do układu Schengen infrastruktura teletransmisyjna niezbędna do przesyłania danych oraz policyjne systemy informatyczne musiały uzyskać odpowiednią wydajność, dostępność, a także spełnić warunki bezpieczeństwa zgodnie z wymogami Konwencji wykonawczej Schengen i zaleceniami Komisji Europejskiej. Spełnienie tych wymagań, w tym dostępności systemu SIS dla podstawowych jednostek Policji[24], stanowiło znakomite uzasadnienie dla wykorzystania funduszy europejskich do modernizacji starzejącej się sieci POLWAN.

Konieczność zasadniczej wymiany technologii sieci teletransmisyjnej Policji w połączeniu z europejskim wymogiem budowy systemu informatycznego do przyjmowania i obsługi numeru alarmowego 112 stały się podstawą koncepcji zintegrowanej sieci OST 112, zaspokajającej rosnące zapotrzebowanie transmisyjne Policji, jak też zapewniającej współdziałanie służb ratunkowych. Z inicjatywą w tej sprawie wystąpił Komendant Główny Policji, projekt zaś został umieszczony na liście 7 osi

[23] *Plany informatyzacji Komendy Głównej Policji*, „Computerworld" 2004, nr 1, www.computerworld.pl, dostęp 23 czerwca 2015 r.

[24] Fundusz Schengen, www.policja.pl, dostęp 23 czerwca 2015 r.

Programu Operacyjnego Innowacyjna Gospodarka[25] – z ostatecznym finansowaniem na poziomie 160 mln złotych, z czego aż 85% stanowiły środki Europejskiego Funduszu Rozwoju Regionalnego. Celem projektu OST 112 było poprawa bezpieczeństwa obywateli dzięki usprawnieniu komunikacji służb ratownictwa oraz porządku publicznego przez wdrożenie zintegrowanej platformy komunikacyjnej dla Systemu Informatycznego Powiadamiania Ratunkowego wykonanej w technologii IP/MPLS. Użytkownikiem działającej aktualnie sieci OST 112 są jednostki organizacyjne Policji, Państwowej Straży Pożarnej i jednostki administracji rządowej korzystające z sieci łączności głosowej resortu, zbudowanej w ramach projektu. Bezpośrednim użytkownikiem sieci są także operatorzy numeru alarmowego 112, dyspozytorzy i koordynatorzy służb porządku publicznego i ratownictwa umiejscowieni w centrach powiadamiania ratunkowego. Sieć umożliwia poprawę bezpieczeństwa obywateli i cudzoziemców przez zapewnienie szybkiego i skutecznego dostępu do służb ustawowo powołanych do niesienia pomocy, umocnienie wizerunku służb porządku publicznego i ratownictwa, jako nowoczesnej i sprawnie zarządzanej formacji wykorzystującej nowoczesne technologie teleinformatyczne, a także poprawę warunków pracy funkcjonariuszy i pracowników służb porządku publicznego i ratownictwa, dzięki zapewnieniu usług umożliwiających im szybki dostęp do informacji. Operatorem sieci OST 112, do której przeniesiono wszystkie usługi sieci POLWAN, odpowiedzialnym także za jej utrzymanie i dalszą rozbudowę, jest Policja[26]. Warto przy tym podkreślić, że budowa sieci teletransmisyjnej polskiej Policji, wieloletnie przedsięwzięcie o ogromnej organizacyjnej oraz finansowej, uznawana jest – również w odczuciu społecznym i medialnym – za przykład sukcesu w informatyzacji administracji publicznej, uzupełnionego dodatkowo inteligentnym i efektywnym podejściem do wykorzystywania dostępnych inwestycyjnych środków unijnych[27].

2. Udane wdrożenie Systemu Wspomagania Dowodzenia Policji (SWD)

Zgodnie z dyspozycją art. 20e ustawy o Policji System Wspomagania Dowodzenia Policji stanowi system teleinformatyczny wspierający wykonywanie zadań ustawowych przez jednostki organizacyjne Policji, jak również przyjmowanie zgłoszeń alarmowych z centrów powiadamiania ratunkowego; utrzymanie, rozbudowę oraz modyfikację SWD Policji zapewnia Komendant Główny Policji.

Historia Systemu Wspomagania Dowodzenia w polskiej Policji sięga 2000 roku, kiedy to w KMP w Szczecinie, Krakowie, Łodzi oraz w Komendzie Stołecznej Policji wdrożono pierwsze pilotażowe, budowane niezależnie od siebie instalacje tego typu. Z czasem opracowano założenia SWD dla całego kraju, co pozwoliło

[25] P. Fergiński, P. Hofman, K. Jarosławska, K. Kołodziński, M. Kozera, K. Pawłowski, D. Zakrzewski, *OST 112. Ogólnopolska sieć teleinformatyczna na potrzeby obsługi numeru alarmowego 112*, Centrum Projektów Informatycznych 2012, s. 10.

[26] *Projekt OST 112*, Centrum Projektów Informatycznych, www.cpi.gov.pl, dostęp 23 czerwca 2015 r.

[27] *OST 112: sieć dla całej administracji*, www.ratownik-med.pl, 25.05.2012, dostęp 23 czerwca 2015 r.

na uruchomienie w 2007 r. postępowania zakupowego na budowę nowego systemu informatycznego wspierającego pracę służb dyżurnych. W tym czasie Polska została zobowiązana do uruchomienia jednolitego Systemu Informatycznego powiadamiania Ratunkowego (SIPR), który miał obsługiwać zgłoszenia z numeru alarmowego 112. Aby zapewnić szybką i niezawodną wymianę danych, w ramach SIPR zbudowano sieć teleinformatyczną OST 112. Systemy informatyczne służb ratowniczych (w tym SWD Policji) mają się komunikować z SIPR za pomocą jednolitego interfejsu – w związku z czym podjęto decyzję o centralizacji SWD[28]. System ten został stworzony do ujednolicenia algorytmów postępowania, dokumentacji, analizy i raportowania działań podejmowanych we wszystkich jednostkach Policji w Polsce. SWD ma na celu kompletną, w znacznej części elektroniczną obsługę zdarzeń od momentu przyjęcia informacji o zdarzeniu, poprzez jego obsługę, do procesu analizowania danych, sporządzania opracowań statystycznych i raportowania. Głównym zadaniem systemu jest dostarczenie funkcjonariuszom jednolitej informacji, która zapewni standaryzację pracy i usprawni proces podejmowania decyzji związanych z obsługą zdarzeń[29]. Jego główne funkcjonalności to:

- przyjmowanie, rejestracja, obsługa zgłoszeń i zdarzeń,
- zarządzanie działaniami oraz personelem i zasobami interwencyjnymi Policji,
- zarządzanie informacją: sprawdzenia w Krajowym Systemie Informacyjnym Policji (KSIP) przez System Poszukiwawczy Policji (SPP), komunikaty,
- wizualizacja działań i wykorzystanie Uniwersalnego Modułu Mapowego (UMM) do obsługi realizowanych procesów,
- wykorzystanie Terminali Mobilnych (TM) do współpracy z SWD,
- system analityczny, raportowanie i statystyka,
- współpraca z systemem teleinformatycznym centrów powiadamiania ratunkowego i Państwową Strażą Pożarną (PSP)[30].

System Wspomagania Dowodzenia, finansowany w niewielkiej części z funduszy strukturalnych Unii Europejskiej, wdrażano w trzech etapach od 2011 do 2013 roku – początkowo pilotażowo w KGP i wybranych KWP oraz KMP, ostatecznie rozwijając go w pełni na terenie całego kraju od 1 stycznia 2013 roku – z jednoczesną obsługą około 3500 funkcjonariuszy służby dyżurnej. Po przeprowadzonej kontroli tego przedsięwzięcia Najwyższa Izba Kontroli oceniła pozytywnie, mimo stwierdzonych nieprawidłowości, planowanie i realizację projektu dotyczącego budowy Systemu Wspomagania Dowodzenia Policji. Wyniki kontroli wykazały, że od 1 stycznia 2013 roku system SWD został produkcyjnie wdrożony i jest wykorzystywany w praktyce w jednostkach organizacyjnych Policji na terenie całego kraju. Wskazane przez NIK

[28] T. Noszczyński, *System Wspomagania Dowodzenia. Element większej całości*, „Policja 997" 2013, nr 10(103), s. 28.
[29] K. Olejnik, M. Maciejewski, *Dyżurny jednostki organizacyjnej Policji*, Szkoła Policji w Słupsku, Słupsk 2015, s. 33.
[30] S. Makowski, *System Wspomagania Dowodzenia w Policji*, „Kwartalnik Policyjny" 2014, nr 1(27), s. 40.

nieprawidłowości dotyczyły m.in. braku należytego przygotowania KGP do realizacji przedsięwzięcia oraz wykorzystania dofinansowania ze środków UE przyznanego na rozbudowę SWD. W ocenie NIK nierzetelna i nieskuteczna była również współpraca w tym zakresie między KGP a CPI. NIK oceniła pozytywnie działania Komendanta Głównego Policji oraz komendantów terenowych jednostek organizacyjnych Policji w zakresie planowania i realizacji projektu SWD[31]. System ten należy zatem uznać za przykład udanej mimo wszystkich zastrzeżeń implementacji narzędzia informatycznego stanowiącego istotne wsparcie m.in. w ogólnej prewencji oraz w realizacji czynności kryminalistycznych przez funkcjonariuszy Policji bezpośrednio na miejscach zdarzeń.

3. Porażka projektu e-posterunek

Projekt e-posterunku został wymieniony (oprócz SWD) w Planie Przedsięwzięć Komendy Głównej Policji zawierającym priorytety Policji na lata 2010–2012. Oba projekty uznano za sztandarowe przedsięwzięcia Policji, realizowane w ramach jej informatyzacji i usprawnienia pracy funkcjonariuszy. E-posterunek miał przy tym wpłynąć na lepsze postrzeganie Policji przez opinię publiczną, promując jej nowoczesny elektroniczny wizerunek.

Projekt ten to w uproszczeniu aplikacja, która miała uprościć procedury związane z opisywaniem i dokumentowaniem czynności wykonywanych przez funkcjonariuszy służby dochodzeniowo-śledczej i ruchu drogowego prowadzących postępowania przygotowawcze oraz obsługujących zdarzenia drogowe. W jej ramach miały być generowane protokoły, zaświadczenia, postanowienia i inne druki, które dotychczas policjanci wypełniali oddzielnie, wpisując wielokrotnie te same informacje[32]. Aplikacja miała więc zmniejszyć istotnie biurokrację przez wyeliminowanie ręcznego wpisywania tych samych danych do różnych druków procesowych, co miało odciążyć funkcjonariuszy i przyspieszyć obsługę petentów na miejscach zaistniałych zdarzeń. W założeniach e-posterunku przewidziano jego współpracę z KSIP i innymi centralnymi bazami danych Policji. Przedsięwzięcie to było realizowane w latach 2007–2014 i wywodziło się z wypracowanej jeszcze w 2006 roku w Policji koncepcji Elektronicznego Modułu Procesowego, przejętego w 2008 roku do dalszej rozbudowy oraz realizacji przez Centrum Projektów Informatycznych pod zmienioną nazwą e-posterunek, z przewidywanym terminem uruchomienia w czerwcu 2011 roku. Ostatecznie e-posterunek, pomimo wydatkowania w ramach projektu kwoty ponad 19 milionów złotych, nigdy nie został wdrożony produkcyjnie w Policji, a z dniem 1 marca 2014 roku Komendant Główny Policji podjął ostateczną decyzję o zaprzestaniu jego realizacji[33]. W powszechnej opinii projekt ten stał się flagowym przykładem, jak nie

[31] Informacja o wynikach kontroli: Planowanie i realizacja wybranych projektów teleinformatycznych mających na celu usprawnienie funkcjonowania jednostek organizacyjnych Policji, Najwyższa Izba Kontroli 2012, Dokument: KPB-4101-05-00/2012, s. 9.

[32] *Rewolucja technologiczna w policji? Laptopy zamiast notesów*, www.tech.wp.pl, 23.07.2010, dostęp 23 czerwca 2015 r.

[33] *E-posterunek – korupcyjny thriller*, www.mediologia.pl, 29.04.2014, dostęp 22 czerwca 2015 r.

należy wdrażać przedsięwzięć informatycznych, będąc dodatkowo obciążonym jedną z najbardziej medialnych afer o charakterze korupcyjnym – dotyczącą postępowań przetargowych w ramach e-posterunku. Sformułowany w tej sprawie w 2012 roku akt oskarżenia, sporządzony po przeprowadzenia śledztwa zainicjowanego doniesieniem ministra SWiA z 2009 roku, objął m.in. funkcjonariusza publicznego – byłego dyrektora Biura Łączności i Informatyki KGP[34]. Realizacja e-posterunku była także przedmiotem kontroli NIK, która oceniła negatywnie planowanie i realizację projektu oraz stan wdrożenia tego narzędzia teleinformatycznego w jednostkach organizacyjnych Policji. Sformułowane zarzuty dotyczyły prowadzenia nierzetelnie i niezgodnie z prawem prac planistycznych mających na celu określenie wymagań dla tego narzędzia teleinformatycznego oraz warunków jego wdrożenia do praktyki policyjnej, niedotrzymania terminu uruchomienia produkcyjnego aplikacji w Policji, a także niegospodarności w postaci nieuruchomienia i nieudostępnienia znacznej części zakupionych funkcjonalności tej aplikacji zarówno policjantom, jak i obywatelom. NIK oceniła także negatywnie zabezpieczenie danych osobowych przetwarzanych w e-posterunku, wskazując, że eksploatacja tego systemu była prowadzona nielegalnie, tj. z naruszeniem przepisów ustawy o ochronie danych osobowych, co stworzyło zagrożenie dla integralności i poufności danych osobowych obywateli oraz funkcjonariuszy[35].

Opisany projekt jest niewątpliwie największą dotychczas porażką w ramach informatyzacji Policji, tym dotkliwszą, że oprócz praktyki prowadzenia czynności dowodowych dotyczącą również sfery bezpośredniego kontaktu Policji ze społeczeństwem. Jak się wydaje, bardzo sensowna w założeniach aplikacja, na skutek popełnienia wszelkich możliwych błędów w zarządzaniu projektem, a także działalności noszącej znamiona przestępstwa, stała się fatalnym przykładem niekompetencji oraz braku poszanowania prawa wewnątrz struktur samej Policji.

Podsumowanie – aktualne trendy rozwoju policyjnej infrastruktury informacyjnej

Technologie oraz narzędzia informacyjne są w nowoczesnym świecie elementem warunkującym skuteczne zwalczanie przestępczości oraz realizację innych ustawowych celów nałożonych na Policję. Dlatego też informatyzacja Policji powinna być postrzegana systemowo jako kluczowe zadanie, wpływające m.in. na możliwości i praktykę realizacji wielu czynności kryminalistycznych w ramach działań o charakterze operacyjnym oraz procesowym. Biorąc pod uwagę skalę instytucji takiej jak Policja – zarówno w wymiarze terenu działania, jak też zasobów ludzkich – należy zdawać sobie sprawę z kompleksowości i stopnia trudności wdrażania projektów jej informatyzacji, a także istnienia różnego rodzaju zagrożeń o charakterze zarówno organizacyjnym, jak i związanych z kwestiami nadzoru oraz realnego zagrożeniem zjawiskami niepożądanych zachowań, w tym korupcji.

[34] *Policja wycofuje się z programu e-posterunek*, „Rzeczpospolita", 1 marca 2014 r., www.rp.pl, dostęp 23 czerwca 2015 r.

[35] Informacja o wynikach kontroli: Planowanie i realizacja wybranych projektów..., op. cit., s. 8.

Spoglądając w przyszłość, warto przedstawić w podsumowaniu trendy związane z potrzebami organów ścigania w zakresie narzędzi oraz technologii informacyjnych w krajach Unii Europejskiej – wyznaczające w istocie aktualne kierunki informatyzacji instytucji takich jak polska Policja. Należą do nich:

- integracja systemów informacji wywiadowczych,
- wdrażanie systemów komunikacji mobilnej,
- wykorzystywanie systemów obserwacji wizyjnej,
- zastosowania cyfrowych systemów biometrycznych,
- wyzwania w zakresie wykorzystywania mediów społecznościowych[36].

Streszczenie

Artykuł przedstawia wybrane elementy procesu informatyzacji polskiej Policji, mającej fundamentalne znaczenie – w kontekście pozyskiwania, przetwarzania oraz wykorzystywania informacji – dla skuteczności procesu wykrywczego oraz przeciwdziałania przestępczości w ogóle, a także dla konkretnych prowadzonych przez Policję czynności o charakterze operacyjnym oraz procesowym. Wskazane są podstawy prawne oraz programy informatyzacji organów ścigania w powiązaniu z szerszym zagadnieniem informatyzacji administracji publicznej, a także ewolucja systemowego podejścia do informatyzacji kraju i wynikające stąd konsekwencje w sferze zainteresowania organów ścigania. Istotną częścią publikacji są analiza kluczowych dla aktualnych możliwości informacyjnych Policji programów informatyzacji przedstawiająca zarówno uzyskane sukcesy, jak i odniesione porażki, a także wskazanie aktualnych trendów rozwojowych w zakresie technologii i narzędzi informacyjnych w kontekście działania Policji w krajach Unii Europejskiej.

Słowa kluczowe: Policja, informatyzacja administracji, proces wykrywczy, narzędzia informatyczne, policyjne systemy IT

Summary

The paper presents selected elements of the informatization process of the Polish Police, having fundamental importance – in the context of data collection, evaluation and utilization – for effectiveness of investigative process and crime prevention in general, as well as for specific policing actions undertaken by the Police. An overview of legal basis and informatization programs of law enforcement institutions is presented in connection with even more general issue of informatization of public administration, together with considerations of evolution of general approach to informatization of the State and consequences arising and impacting law enfocement. An important part of the paper is analysis of the key informatization programmes constituting basis for information capabilities of the Police, presenting both successes and failures, and also consideration of the future trends of development of information tools and technologies in the context of Police activities in the EU Member States.

Keywords: Police, informatization of administration, investigative process, IT tools, police IT systems

[36] S. Denef (red.), *ICT Trends in European Policing COMPOSITE Draft of Deliverable D4.1*, 1.03.2011, www.composite-project.eu, dostęp 20 czerwca 2015 r.

Mateusz Kucharski

MODUS OPERANDI A WYWIAD PRZED WŁAMANIEM JAKO ELEMENT TAKTYCZNY DZIAŁANIA SPRAWCÓW PRZESTĘPSTW PRZECIWKO MIENIU

Modus operandi and the interview conducted before burglary as a tactical crime method against property

W strukturze przestępstw kryminalnych popełnianych w Polsce kradzież z włamaniem zajmuje dominującą pozycję i należy do kategorii przestępstw kwalifikowanych przez Policję jako szczególnie monitorowane. Mimo że na przestrzeni ostatniej dekady można zauważyć spadek liczby tych przestępstw, to tylko w ubiegłym roku odnotowano dziennie 317 takich zdarzeń na terenie całego kraju[1]. Niestety, poziom wykrywalności sprawców kradzieży z włamaniem jest niepokojąco niski. W roku 2014 wykryto sprawców jedynie 32,9% przestępstw przeciwko mieniu, co i tak stanowi jeden z najwyższych wyników wykrywalności w ostatnim dziesięcioleciu[2]. Z tego względu istotą rozważań w tym opracowaniu stało się ukazanie przydatności w wykorzystywaniu *modus operandi*[3] w kontekście jednego z najczęściej popełnianych w Polsce przestępstw kradzieży z włamaniem. Wiedza o sposobie działania włamywaczy może być wykorzystywana szczególnie w procesie wykrywczym przy użyciu potencjalnych nośników *modus operandi*, w każdym stadium realizacji czynu przestępczego. Elementem warunkującym skuteczność w zwalczaniu przestępczości przeciwko mieniu jest poznanie mechanizmów działania sprawców na poziomie wszystkich etapów aktywności przestępczej, zarówno przed popełnieniem czynu przestępczego, w jego trakcie, jak również na etapie zatarcia śladów[4]. Jednak szczególną uwagę należy zwrócić na elementy taktyczne działania włamywaczy w stadium

[1] Źródło: dane Komendy Głównej Policji, http://statystyka.policja.pl/st/ogolne-statystyki/47682,Postepowania-wszczete-przestepstwa-stwierdzone-i-wykrywalnosc-w-latach-1999-2014.html.

[2] Źródło: dane statystyczne, Biuletyn Informacji Publicznej Ministerstwa Sprawiedliwości, 2015 r.

[3] H. Grossw swoim poręczniku, *Handbuch für Untersuchungsrichter, Polizeibeamte, Gendarmen, u.s.w* wprowadza po raz pierwszy pojęcie *modus furandi* – pochodzącego od łacińskiego słowa *fur* – złodziej.

[4] J. Wnorowski, *Sposób działania jako środek identyfikacji sprawcy przestępstwa*, Wydawnictwo Prawnicze, Warszawa 1978, s. 7.

przygotowawczym przestępstwa, do których należy wywiad przed dokonaniem włamania. Wiedza o sposobie i metodach prowadzenia rozpoznania przez sprawców jeszcze przed realizacją zamierzenia przestępczego nie tylko warunkuje skuteczność postępowania przygotowawczego, lecz także ma istotny wpływ na prewencyjne działania organów ścigania.

Najogólniej pojęcie wywiadu możemy zdefiniować przez całokształt działań sprawcy mający na celu ustalenie niezbędnych informacji o obiekcie będącym przedmiotem zamachu przestępczego. Stosowanie wywiadu przez włamywacza, jako czynności poprzedzającej sprawstwo, odbywa się z reguły na drodze obserwacji obiektu oraz znajdujących się w nim osób. Kolejnym etapem jest uzyskanie niezbędnych informacji o przyszłym obiekcie włamania lub bezpośredniej weryfikacji sposobu zabezpieczeń. Dobrze przeprowadzony wywiad jednoznacznie warunkuje skuteczność planowanego przestępstwa, a sprawca nieposiadający danych o przedmiocie zamachu przestępczego lub stosowanych środkach zabezpieczeń w większym stopniu narażony jest na zatrzymanie. Włamywacze zwracają uwagę na wszystkie elementy mające wpływ na przebieg przestępstwa, gdyż charakterystyka położenia obiektu lub pora włamania mogą ułatwić lub ograniczyć swobodę działania. Doświadczeni włamywacze wiedzą, że w trakcie wywiadu poprzedzającego włamanie muszą zdobyć wszystkie konieczne dane o obiekcie oraz alternatywnych drogach zarówno swobodnego dojścia do celu, jak i umożliwiających wycofanie podczas ucieczki[5].

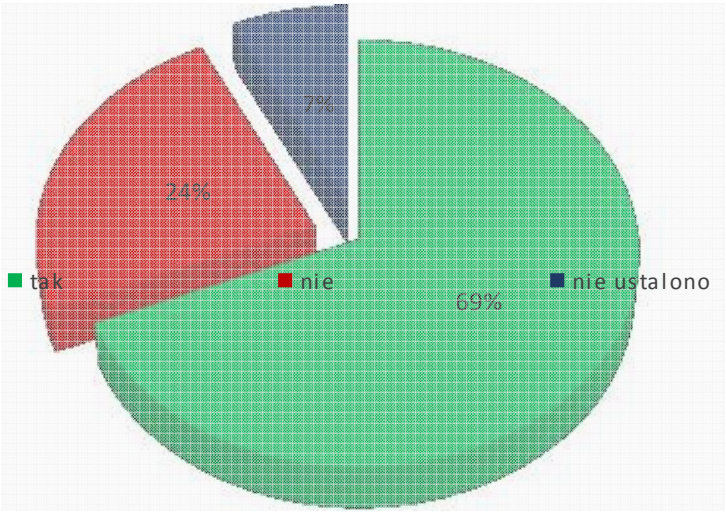
Zespół cech *modus operandi*, charakteryzujących stadium przygotowania do przestępstwa w pierwszym etapie realizacji czynu przestępczego, uwarunkowany jest w dużym stopniu typem obiektu, który jest celem ataku sprawcy[6]. Rodzaj obiektu na tym etapie bezpośrednio determinuje zakres występowania nośników *modus operandi* w zależności od stopnia zróżnicowania czynnika planowości lub też jego całkowitego braku, kiedy zamiar popełnienia przestępstwa pojawia się nagle i jest następstwem nadarzającej się okazji.W takich sytuacjach znaczącą rolę odgrywa element losowy zarówno w trakcie typizacji obiektu, jak i doboru odpowiednich narzędzi potrzebnych do dokonania przestępstwa[7]. Przypadek sprawia, iż sprawca decyduje się dokonać włamania pod wpływem nadarzającej się okazji, dlatego w takich sytuacjach ustalenie konkretnej formuły *modus operandi* bywa bardzo trudne lub nawet jest niemożliwe. Słusznie zauważył J. Wnorowski, że sposób działania sprawcy na etapie przygotowania przestępstwa zarówno determinuje jego rodzaj, jak i ściśle wpływa na wartość i układ indywidualizacji *modus operandi*. Wraz z rozwojem technologii i środków zabezpieczających przed włamaniami technika dokonywania przestępstw stała się bardziej złożona, co ma bezpośredni wpływ na realizację elementów taktycznych,

[5] Z. Bożyczko, *Przestępstwo i życie*, Zakład im. Ossolińskich, Wrocław 1972, s. 106–107.
[6] C. Bennell, N.J. Jones, *Between a ROC and a hard place: a method for linking serial burglaries by modus operandi*, „Journal of Investigative Psychology and Offender Profiling" 2005, t. 2 (1), s. 24–26.
[7] W.F.H. Nicolasien, *Burglars and Burglaries in Contemporary Legends*, Presidential Address Given To The Folklore Society, March 2002, s. 138.

a stadium przygotowawcze będzie odznaczało się znacznie „bogatszym asortymentem" charakterystycznych elementów *modus operandi*[8].

Czynniki decydujące o występowaniu wywiadu

Przeprowadzone badania aktowe wykazały, że 69% sprawców kradzieży z włamaniem przed dokonaniem przestępstwa prowadzi działania wywiadowcze (wykres 1). Wysoki współczynnik występowania wywiadu, jako czynności poprzedzającej włamanie, stał się asumptem do uzyskania odpowiedzi na pytanie, jakie czynniki decydują o stosowaniu przez włamywaczy takiej formy działań.



Wykres 1. Wywiad sprawcy włamania przed dokonaniem przestępstwa

Źródło: badania własne.

Autor obszernej monografii na temat sprawców włamań Z. Bożyczko przeprowadził klasyfikację mechanizmów warunkujących prowadzenie wywiadu przez włamywacza w latach sześćdziesiątych, przyjmując, że do elementów decydujących należy: stopień specjalizacji sprawcy, zabezpieczenie i położenie obiektu oraz sposób dokonania włamania[9]. Jednak taktyka i technika działania sprawców ulega ciągłym przemianom i przekształceniom wraz z postępem technicznym oraz cywilizacyjnym[10]. Zmiany te dotyczą nie tylko sposobu pokonywania zabezpieczeń, ale również elementów taktycznych działania sprawców. Dokonując rewizji postawionych przez

[8] J. Wnorowski, op. cit., s. 51.

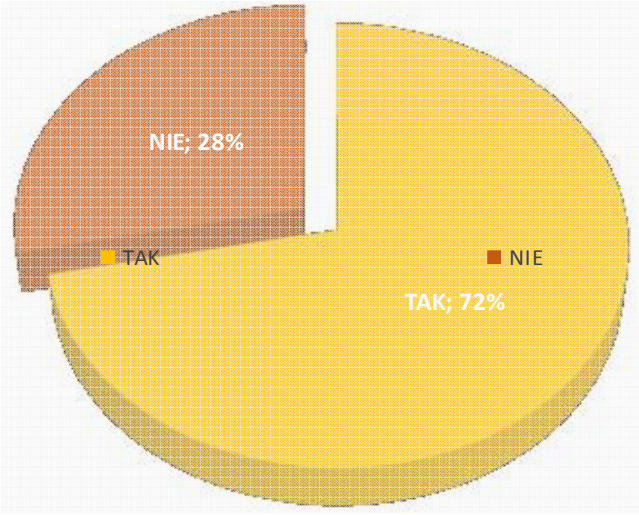
[9] Z. Bożyczko, *Kradzież z włamaniem i jej sprawca*, Wydawnictwo Prawnicze, Warszawa 1970, s. 52.

[10] T. Borzoł, S. Miszkiewicz, M. Tokarski, A. Winnicki, J. Bryk, *Kryminologiczne i kryminalistyczne aspekty przestępstwa kradzieży z włamaniem do mieszkań*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2005, s. 15.

autora korelacji w oparciu o prowadzone badania mechanizmów działań wywiadowczych współczesnych włamywaczy, należy przyjąć, że do czynników decydujących o stosowaniu rozpoznania jako czynności poprzedzającej włamanie zaliczymy:

1) wiek i stopień doświadczenia sprawcy,
2) rodzaj obiektu zamachu przestępczego oraz jego położenie,
3) rodzaj zabezpieczeń i sposób dokonania włamania.

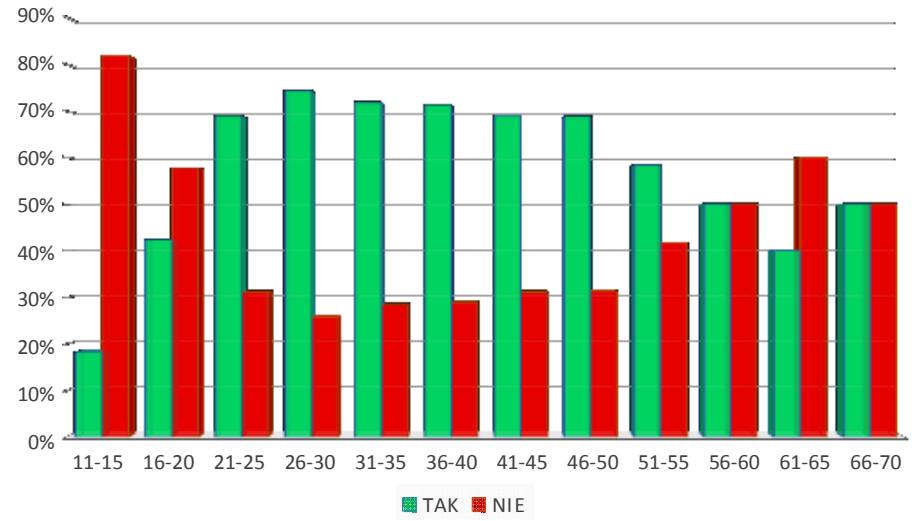
Wiek i stopień doświadczenia sprawcy to czynniki pozostające w ścisłym związku, gdyż sprawca z upływem lat zdobywa coraz więcej umiejętności w procederze przestępczym. Starsi i bardziej doświadczeni włamywacze z reguły byli już wcześniej karani, stąd zdają sobie sprawę, czym grozi zlekceważenie i pominięcie elementów wywiadowczych. Na podstawie przeprowadzonej analizy materiału badawczego stwierdzono zastosowanie elementów wywiadowczych częściej wśród sprawców karanych, odznaczających się większym doświadczeniem w procederze przestępczym, niż u przestępców niekaranych (wykres 2).



Wykres 2. Prowadzenie wywiadu przed włamaniem wśród sprawców wcześniej karanych

Źródło: badania własne.

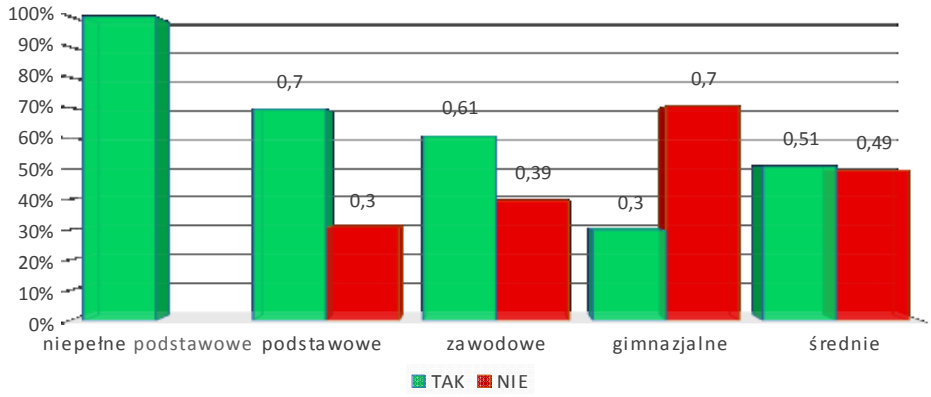
Sprawcy, których cechuje wysoki stopień specjalizacji, posiadają szeroką wiedzę taktyczną choćby w zakresie czasu i pory zmiany służby patroli funkcjonariuszy policji z określonej dzielnicy lub bezpośrednio prowadzą nasłuch policyjnych kanałów radiowych. Nabycie takich umiejętności na ogół przychodzi wraz z wiekiem i jest związane z empirycznym charakterem pozyskiwania kwalifikacji przestępczych. Uzasadnieniem przyjętego twierdzenia jest wynik korelacji przedstawiony na wykresie 3, który wskazuje, że sprawcy w przedziale wieku od 25 do 45 roku życia częściej stosują wywiad przed dokonaniem zaboru mienia niż ci w wieku od 11 do 25 lat.



Wykres 3. Wywiad przed włamaniem a wiek sprawcy

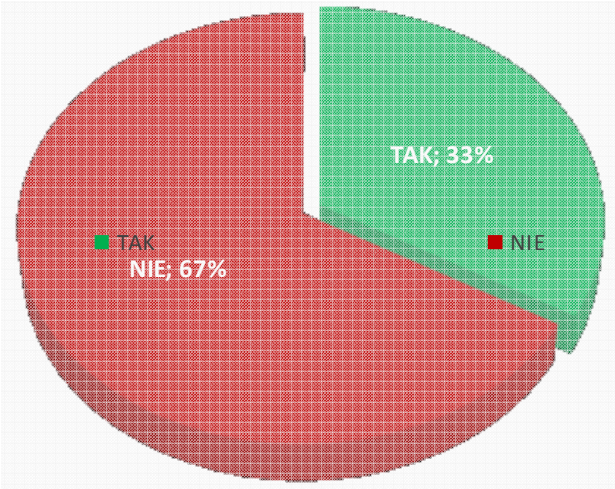
Źródło: badania własne.

Zauważono również występowanie zależności stosowania wywiadu w odniesieniu do wykształcenia sprawców. Włamywacze, którzy zakończyli swoją edukację na poziomie podstawowym i zawodowym, częściej stosują rozpoznanie niż gimnazjaliści (wykres 4). Wynika to przede wszystkim ze sposobu działania nieletnich i młodocianych sprawców o wykształceniu gimnazjalnym, który najczęściej ma charakter okazjonalny i rzadko odznacza się występowaniem elementów taktycznych. Analiza wyników badań jednoznacznie wykazała, że sprawcy będący pod wpływem alkoholu nie stosują wywiadu jako czynności poprzedzającej włamanie (wykres 5).



Wykres 4. Rodzaj wykształcenia sprawcy a wywiad przed włamaniem

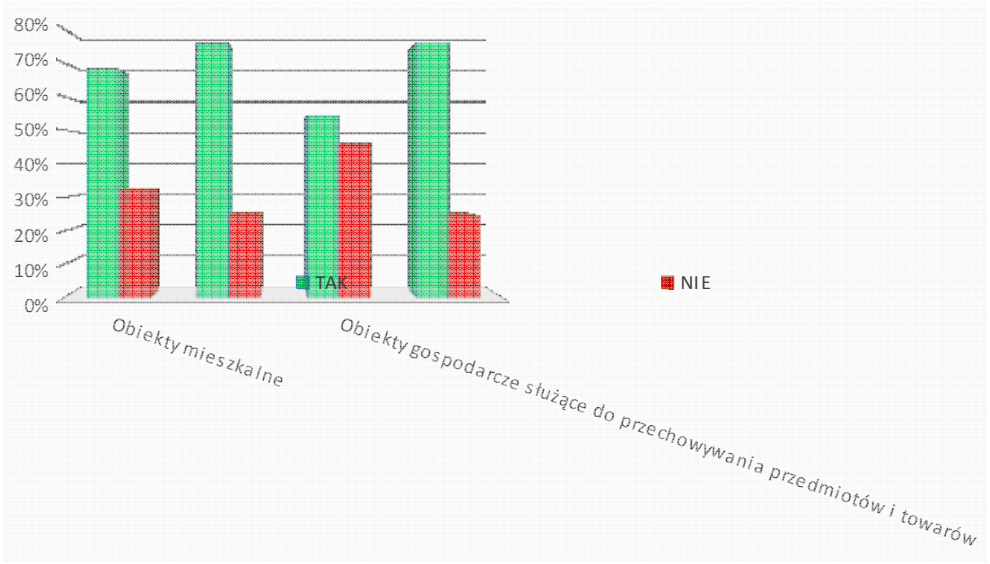
Źródło: badania własne.



Wykres 5. Sprawca pod wpływem alkoholu a wywiad przed włamaniem

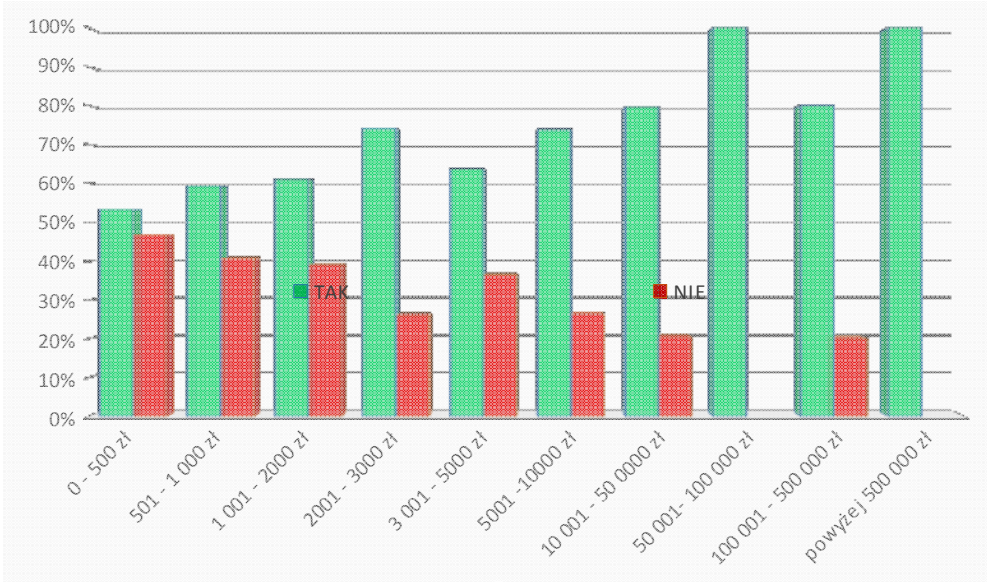
Źródło: badania własne.

Obiekt ataku włamywacza ma bezsprzecznie istotny wpływ na konieczność prowadzenia wywiadu przez sprawcę. Związane jest to przede wszystkim z wartością mienia, jakie może znajdować się w miejscu będącym celem zamachu przestępczego. W takich obiektach jak piwnice, altany ogrodowe czy garaże zazwyczaj przechowywane są przedmioty o niższej wartości. W związku z tym wśród włamywaczy istnieje powszechne przekonanie, że atak na takie cele nie wymaga uprzedniego rozpoznania. Uzasadnieniem tego stwierdzenia są dane przedstawione na wykresach 6 i 7 wskazujące, że sprawcy rzadziej poprzedzają włamanie wywiadem do obiektów gospodarczych służących przechowywaniu mienia, którego wartość nie przekracza 2 tys. zł, niż choćby do mieszkań lub sklepów, gdzie spodziewają się znaleźć przedmioty o większej wartości.



Wykres 6. Rodzaj obiektu a wywiad przed włamaniem

Źródło: badania własne.



Wykres 7. Wywiad przed włamaniem a wartość skradzionego mienia

Źródło: badania własne.

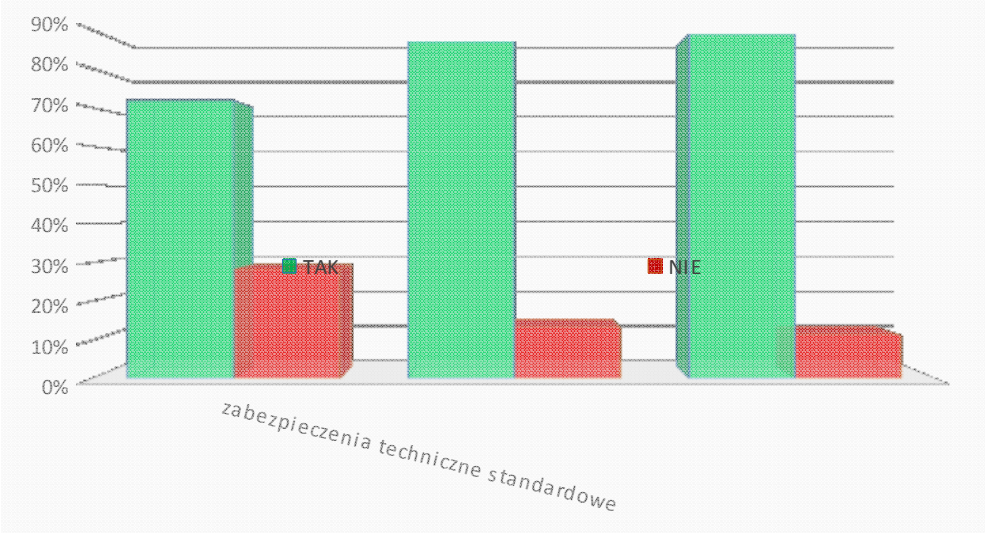
Jak wynika z badań, sprawcy najczęściej prowadzą wywiad przed popełnieniem przestępstwa włamania do obiektów handlowo-usługowych. Ma to związek z formą prowadzonego rozpoznania, gdyż dostęp do takich obiektów bez zwracania na siebie uwagi jest łatwiejszy niż choćby w przypadku obiektów mieszkalnych. Nie bez znaczenia pozostaje również położenie obiektu, który jest celem zamachu przestępczego, ponieważ włamania niepoprzedzone wywiadem występują częściej w centrum miasta niż na peryferiach (wykres 8). Na terenach położonych z dala od ścisłego centrum spotyka się głównie zabudowę w postaci domów jednorodzinnych. Włamania do domów przeważnie są poprzedzone wywiadem, w przeciwieństwie do piwnic w blokach osiedlowych czy altan działkowych, które znajdują się w centrum miasta i stanowią raczej cel okazjonalny.

Wykres 8. Położenie obiektu zamachu przestępczego a wywiad przed włamaniem

Źródło: badania własne.

Kolejnym czynnikiem pozostającym w ścisłej korelacji z wykorzystaniem elementów taktycznych w działaniach włamywaczy jest sposób zabezpieczenia obiektu. Obiekty, które wyposażono dodatkowo w zabezpieczenia elektroniczne lub które posiadają zabezpieczenia specjalne, są w większości wypadków poddawane przez włamywaczy uprzednim „oględzinom" (wykres 9). Pokonanie alarmu lub – w przypadku zabezpieczeń specjalnych – sejfu wymaga od sprawcy dodatkowych czynności rozpoznawczych mających na celu szczegółowe przygotowanie. Dokładne rozpoznanie terenu, drobiazgowe zaplanowanie alternatywnych dróg ucieczki, sposobu

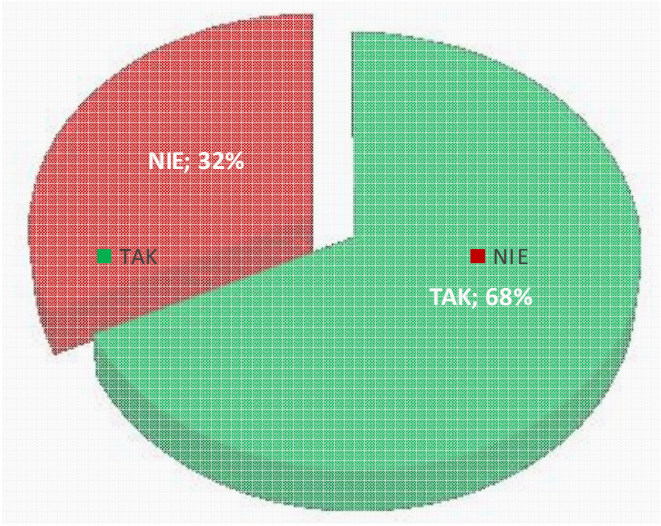
wyłączenia alarmu lub pokonania zabezpieczeń są „elementarzem" dla doświadczonego włamywacza.



Wykres 9. Wywiad przed włamaniem a rodzaje zabezpieczeń obiektu

Źródło: badania własne.

Sposób zachowania się sprawcy po dokonaniu przestępstwa i pozostawione na miejscu ślady nie zawsze prowadzą do jednoznacznego wniosku, czy działał on w sposób zorganizowany, czy jedynie kierowała nim natychmiastowa potrzeba zysku i prowadził włamanie „na ślepo", bez uprzedniego przygotowania. Nie bez znaczenia pozostaje również właściwy dobór odpowiednich narzędzi przez doświadczonych przestępców, co pozwala na wnikliwe i kompleksowe przygotowanie zamierzonego czynu. Sprawcy posługujący się narzędziami częściej poprzedzają swoje działania rozpoznaniem niż ci, którzy pokonywali zabezpieczenia przy użyciu siły fizycznej (wykres 10). Celem działań włamywaczy okazjonalnych są obiekty słabo zabezpieczone, do których pokonania wystarczy użycie siły fizycznej lub rozbicie szyby, stąd rzadziej posługują się oni narzędziami. Opracowanie sposobu pokonania przeszkody zabezpieczającej obiekt i przygotowanie odpowiednich narzędzi, które będą używane podczas włamania, pozostają w bezpośredniej zależności z elementami taktycznymi działania sprawcy na etapie przygotowań do zamierzenia przestępczego.



Wykres 10. Wywiad przed włamaniem sprawcy, który posługiwał się narzędziami

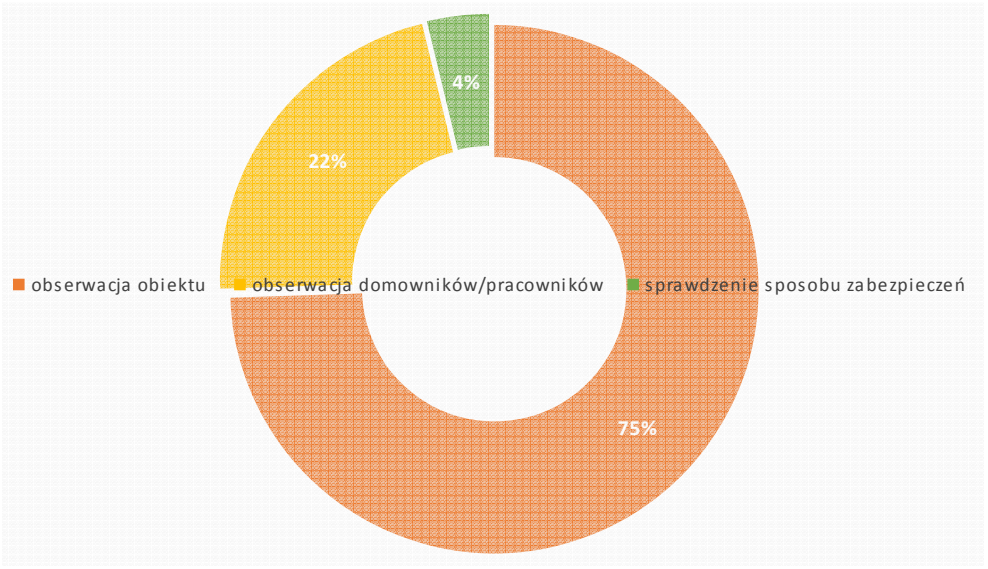
Źródło: badania własne.

Metody prowadzenia wywiadu

Wszechstronność metod wywiadowczych uwarunkowana jest rodzajem atakowanego obiektu, jak również stopniem doświadczenia sprawcy. Sposób prowadzenia wywiadu w dużej mierze uległ przekształceniom wraz z postępem, niemniej jednak pewne metody wypracowane przez całe pokolenia włamywaczy pozostały niezmienne.

W prowadzonych badaniach wytypowano trzy najczęściej występujące formy prowadzenia wywiadu, przez:

- obserwację obiektu,
- obserwację domowników lub pracowników,
- sprawdzenie sposobu zabezpieczeń.



Wykres 11. Formy wywiadu prowadzonego przez sprawców kradzieży z włamaniem

Źródło: badania własne.

Wyniki badań wskazują na występowanie zależności między rodzajem obiektu a sposobem prowadzenia wywiadu przez włamywacza (wykres 11). W obiektach mieszkalnych przestępcy stosują wszystkie trzy formy prowadzenia wywiadu. Uwarunkowane jest to przede wszystkim większą liczbą niewiadomych, zwłaszcza jeśli chodzi o skład rodziny i określenie czasu nieobecności domowników. Sprawca przed włamaniem ustala rytm dobowy funkcjonowania mieszkańców, aby się przekonać, kiedy w mieszkaniu nikogo nie będzie. Sprawdza zabezpieczenia i na podstawie obserwacji samego obiektu szacuje wartość mienia, które ma być przedmiotem zamachu przestępczego.

W przypadku obiektów handlowo-usługowych, biurowych, administracyjnych lub kulturowo-religijnych sytuacja jest łatwiejsza, gdyż sprawca zdaje sobie sprawę, że w nocy w sklepie czy biurze z reguły nikt nie przebywa. Dlatego przestępcy, którzy decydują się na włamanie do takich obiektów, prowadzą rozpoznanie w oparciu o obserwację samego obiektu i sprawdzenie zabezpieczeń, pomijając obserwację pracowników. Włamania do miejsc tego typu zdarzają się głównie nocą, kiedy w lokalach handlowo-usługowych nikogo nie ma, w związku z czym element obserwacji personelu występuje rzadziej i ma zazwyczaj związek ze zlokalizowaniem miejsca przechowywania pieniędzy.

Włamanie do obiektów gospodarczych takich jak piwnice, altany działkowe czy garaże rzadko poprzedza szczegółowy wywiad, dlatego przestępcy ograniczają się jedynie do samej obserwacji planowanego miejsca zamachu przestępczego bez szczegółowego rozpoznania taktycznego.

Poza wymienionymi metodami prowadzenia wywiadu przez sprawców włamań należy również zwrócić uwagę na inne formy rozpoznania, na temat których wiedzę można uzyskać jedynie z źródeł wykraczających poza materiał dowodowy zgromadzony w aktach zakończonych postępowań.

Na podstawie wywiadów i rozmów z funkcjonariuszami z Komendy Miejskiej Policji w Krakowie oraz wiedzy operacyjno-wywiadowczej ustalono, że sprawcy prowadzący rozpoznanie często korzystają ze środków masowego przekazu. Należy w tym przypadku uwzględnić zarówno prasę, telewizję, jak i Internet. Przykładem może być wywiad przed włamaniem nazwanym popularnie „na podwójne łzy" lub na „piórnik", którego mechanizm polega na przeglądaniu przez sprawcę lokalnej prasy w celu uzyskania informacji na temat zmarłych osób w wybranym mieście. Często taki nekrolog zawiera wzmianki określające tytuł zawodowy lub stanowisko w pracy zmarłego, pozwalając włamywaczowi oszacować zamożność pokrzywdzonego. Przestępcy zwracają uwagę nawet na okoliczności śmierci potencjalnej ofiary, wnioskując, że jeśli była to długa i ciężka choroba, zmarły mógł przeznaczyć większość swoich dóbr na leczenie, a włamanie może być nieopłacalne. Kolejnym etapem jest ustalenie adresu zamieszkania, co w dużym mieście nie jest łatwym zadaniem, dlatego w tym celu wywiadowcy posługują się starymi książkami telefonicznymi. W ten sposób uzyskują dokładne dane adresowe obiektu, do którego planują się włamać. Kiedy żałobnicy znajdują się na pogrzebie, sprawcy przystępują do działania. Z reguły dokonują wtedy kilku włamań, gdyż w tym czasie sąsiedzi również uczestniczą w uroczystościach żałobnych. Wspomniane powyżej określenie takiej metody dokonywania kradzieży, w której wywiad jest najistotniejszym elementem działania sprawcy, bierze się z reakcji pokrzywdzonych po odkryciu włamania w równie przykrych okolicznościach[11].

Również telewizja może być wykorzystana przez sprawców jako narzędzie do prowadzenia taktycznego rozpoznania. W ostatnich latach często emitowane programy z wywiadami publicystycznymi znanych osób posłużyły włamywaczom jako doskonałe rozpoznanie obiektów, które stały się w następstwie celem zamachu przestępczego. Przestępcy wykorzystywali popularne reportaże i rozmowy z celebrytami znanymi zarówno w skali regionalnej, jak i krajowej, które odbywały się na terenie ich posiadłości lub w domu. W minionych latach na południu Polski celem włamywaczy padły obrazy i dzieła sztuki, o których sprawcy dowiedzieli się, śledząc właśnie takie programy na ekranie własnego telewizora. Nie wychodząc z domu, mogli oszacować wartość znajdującego się tam mienia, wstępnie ustalić sposób zabezpieczenia obiektu lub rozkład pomieszczeń[12].

Również Internet stał się źródłem informacji dla włamywaczy, nie tylko w zakresie zdobywania wiedzy o nowych narzędziach i sposobach pokonywania

[11] Badania własne na podstawie wywiadów z funkcjonariuszami Wydziału Kryminalnego Komendy Miejskiej Policji w Krakowie w latach 2014–2015.
[12] Tamże.

zabezpieczeń, lecz także wykorzystywany jest jako element wywiadowczy[13]. Na portalach społecznościowych takich jak Facebook czy Instagram sprawcy uzyskują wiele danych o obiektach będących celem zamachu przestępczego, na podstawie których określają wartość mienia posiadanego przez pokrzywdzonego. Na publikowanych zdjęciach osoby takie często chwalą się nowo zakupionym towarem lub fotografują przy mieniu o dużej wartości, które może stanowić przedmiot zaboru. Właściciele kont społecznościowych posiadają liczne albumy ze zdjęciami prezentującymi zamieszkiwane obiekty zarówno w środku, jak na zewnątrz, publikują dane na temat szkół, do jakich uczęszczają, lub nawet wprost określają miejsce zamieszkania, zachęcając tym samym przestępców do działania[14].

Wywiad przed włamaniem do obiektów mieszkalnych

Przeprowadzona analiza uzyskanego materiału badawczego wykazuje zróżnicowanie metod wywiadowczych z wyszczególnieniem rodzaju obiektu mieszkalnego. Sprawcy częściej stosują wywiad w domach jednorodzinnych niż w przypadku mieszkań w blokach osiedlowych lub kamienicach. Ma to bezpośredni związek z przewagą możliwości logistycznych i kamuflażowych w trakcie wywiadu prowadzonego przed włamaniem do domu. Topografia, ukształtowanie terenu, rozmieszczenie obiektów oraz różnice konstrukcyjne umożliwiają sprawcy dokładną obserwację zarówno samego obiektu, jak i domowników, w przeciwieństwie do mieszkań w bloku, gdzie sama obecność włamywacza na klatce może zwrócić czyjąś uwagę.

Przestępcy, którzy planują włamanie do domu, najczęściej w pierwszej fazie działań wywiadowczych prowadzą obserwację wybranego obiektu przy użyciu pojazdu mechanicznego lub pieszo. Jeśli poruszają się pojazdem mechanicznym, zazwyczaj jest to samochód kradziony lub wynajęty z wypożyczalni na fałszywych dokumentach. Wywiadowca, będąc w pojeździe, może prowadzić dyskretną obserwację obiektu, a w razie konieczności wielokrotnie objeżdża całą okolicę, krążąc wokół wyznaczonego celu.Włamywacze, którzy poruszają się pieszo, aby nie wzbudzić podejrzeń częstym pojawianiem się w pobliżu planowanego miejsca włamania, stosują zwyczajowe elementy kamuflażu, tj. nakładają krótkie spodnie, sportowe obuwie, zakładają plecak lub słuchawki na uszy, pozorując trening biegacza. Jak relacjonowali funkcjonariusze policji zajmujący się zwalczaniem przestępczości przeciwko

[13] Powstają wciąż nowe techniki i sztuki manipulacji systemów zabezpieczających, o których sprawcy kradzieży z włamaniem dowiadują się ze stron internetowych poświęconym takim zagadnieniom, np. w przypadku zamków do drzwi jest to proceder zwany *locpicking* (angielski termin określający sztukę manipulacji zamkiem za pomocą odpowiednio dobranych narzędzi, takich jak np. wytrych, w celu niedestrukcyjnego otwarcia mechanizmu bez użycia klucza) lub *bumping* (termin określający sztukę manipulacji zamkiem za pomocą odpowiednio spreparowanego klucza, pozwalający na otwarcie wielu zamków, które posiadają mechanizmy zapobiegające tradycyjnemu *lockpickingowi*, www.toool.nl (The Open Organization of Lockpickers), wikipedia.org/wiki/Bumping.

[14] Badania własne na podstawie wywiadów z funkcjonariuszami Wydziału Kryminalnego Komendy Miejskiej Policji w Krakowie w latach 2014–2015.

mieniu, sprawcy najczęściej podają się za pracowników różnych instytucji lub firm, deklarują, że prowadzą różnego rodzaju usługi, w tym sprzedaż rozmaitych przedmiotów lub towarów. W sytuacji kiedy zastają nieletnich lub osoby starsze, podają się za krewnych lub znajomych rodziców. Jedna z grup przestępczych działających na południu Polski prowadziła rozpoznanie z udziałem swojego wywiadowcy, który podawał się za agenta nieruchomości. Sprawcy niepostrzeżenie mogli dokładnie sprawdzić wszystkie pomieszczenia, zapoznać się z ich rozkładem i przekonać, czy w mieszkaniach znajdują się wartościowe przedmioty. Jeśli sposób zabezpieczenia oglądanej nieruchomości zdaniem włamywaczy był do pokonania, przystępowano do włamania. W przeciwnym razie przestępcy umawiali się z właścicielem na kolejną wizytę pod pretekstem sporządzenia dodatkowych zdjęć, a w trakcie takiego spotkania niepostrzeżenie uchylali okna lub otwierali drzwi balkonowe, aby w dogodnym czasie dokonać kradzieży.

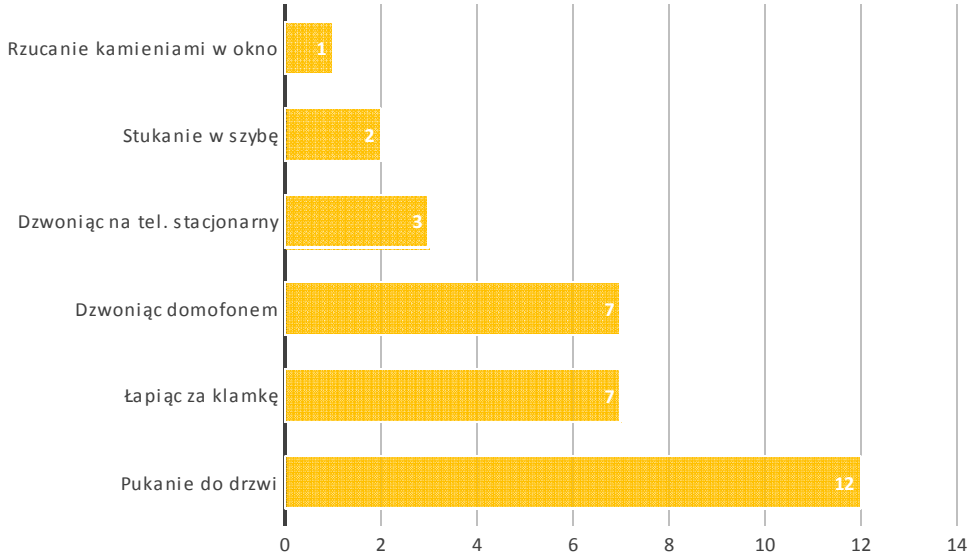
Sprawcy prowadzący wywiad wykorzystują również elementy znakowania obiektu w celu ustalenia dobowego rytmu przebywania domowników. Wywiadowca, wsuwając ulotkę pomiędzy drzwi a framugę lub wkładając do zamka kawałek papieru lub zapałkę, ustala, w jakich godzinach domownicy są nieobecni. Sposoby zweryfikowania przez sprawcę dogodnego czasu włamania są różne, przestępcy wykorzystują nawet włosy lub nitkę, aby przekonać się, kiedy drzwi zostały otwarte[15]. Wszystko zależy od finezji i pomysłowości oraz zaplecza technicznego sprawcy. Przestępcy przy użyciu telefonu komórkowego lub aparatu sporządzają dokumentację fotograficzną samego obiektu i okolicy, na podstawie której mogą zarówno wyznaczyć drogi dojścia i ewakuacji, jak i określić sposób zabezpieczenia domu lub mieszkania.

Jak już wspominano, w przypadku mieszkań sprawcy łatwiej jest ustalić skład osobowy rodziny, okres, w którym mieszkańcy są nieobecni, sposób zabezpieczeń czy istnienie systemów alarmowych. W trakcie wywiadu nakierowanego na domy jednorodzinne sprawcy wykorzystują najprostsze, a zarazem najskuteczniejsze metody rozpoznania, aby przekonać się, czy ktoś znajduje się w środku.Wywiadowca, dzwoniąc na telefon stacjonarny pokrzywdzonego, przy użyciu metody tzw. głuchego telefonu, sprawdza obecność mieszkańców w domu. W zależności od pory roku przestępcy wykorzystują kamienie lub kule śniegowe, rzucając je w okna i czekając, czy ktoś zareaguje. Nierzadko spotykaną metodą wywiadowczą jest wkładanie gazet lub ulotek między drzwi lub kładzenie ich na wycieraczce. W ten sposób sprawca z łatwością może ustalić, czy ktoś wchodził lub wychodził z mieszkania.

Zbliżona forma działań rozpoznawczych stosowana jest w blokach osiedlowych lub kamienicach. Aby potwierdzić chwilową absencję pokrzywdzonego, sprawcy używają domofonów lub po wejściu do klatki pukają do drzwi. Jeśli okaże się, że jednak ktoś jest w środku i otworzy drzwi, włamywacze podają się za roznoszących ulotki lub szukających najbliższego warsztatu samochodowego. Wyniki badań wykazały, że pukanie do drzwi jest najczęściej spotykaną metodą wywiadu, choć włamywacze również często wykorzystują sposób polegający na chwytaniu za klamkę, aby zweryfikować obecność mieszkańców (wykres 12). Należy jednak podkreślić, że

[15] Z. Bożyczko, *Kradzież z włamaniem*..., op. cit., s. 52.

przestępcy w swoich działaniach zarówno taktycznych, jak technicznych najczęściej wykorzystują dużą anonimowość życia mieszkańców, szczególnie na nowo powstałych osiedlach w dużych aglomeracjach miejskich.



Wykres 12. Sposób ustalenia dobowego rytmu obecności domowników

Źródło: badania własne.

Wywiad przed włamaniem do obiektów usługowo-handlowych i biurowych

W przypadku obiektów komercyjnych najbardziej znaczącym czynnikiem mającym wpływ na formę wywiadu prowadzonego przez włamywaczy jest przedmiot zaboru przestępczego oraz rodzaj obiektu usługowo-handlowego. Sprawcy muszą wiedzieć, czy włamanie do wybranego lokalu będzie opłacalne i czy włożona w to praca będzie równała się zyskowi. Ze względu na cel zamachu przestępczego musimy rozróżnić elementy taktyczne działania sprawców planujących włamanie do sklepów od tych, których celem zamachu przestępczego są hotele lub biura. Prowadzenie wywiadu w placówkach handlowych jest z reguły łatwiejsze niż w przypadku kradzieży hotelowych, których sprawcy są bardziej narażeni na wykrycie. Jak podkreślali funkcjonariusze operacyjni w trakcie prowadzonych rozmów, trudności w uzyskaniu zadowalającej wykrywalności tych przestępstw wynikają z tego, iż wielu takich czynów dokonują przestępcy wędrowni lub okazjonalni. Jednak w przypadku sprawców specjalizujących się w dokonywaniu kradzieży z włamaniem do hoteli realizacja zamiaru przestępczego poprzedzona jest starannym doborem miejsca, obiektu kradzieży, czasu, sposobu dokonania włamania oraz innymi czynnościami przygotowawczymi. Włamywacze w celach przestępczych wyjeżdżają do innych

miejscowości i tam starają się zamieszkać w hotelu. Aby przeprowadzić skuteczne rozpoznanie, meldują się w hotelu jako goście na podstawie sfałszowanych dokumentów tożsamości. Mogą przedostać się również na teren obiektu, wykorzystując nieuwagę personelu, lub zostają wprowadzeni przez gości hotelowych, udając, że im towarzyszą. Przebywając na terenie restauracji, recepcji lub holu hotelowego, sprawcy obserwują gości odznaczających się lepszym ubiorem, kosztownie wyglądającą biżuterią lub bardziej interesującym bagażem. Wykorzystując dużą rotację gości hotelowych i często działając w sposób kolektywny, niepostrzeżenie sprawdzają, pod jakim numerem pokoju zatrzymał się potencjalny pokrzywdzony, a w wielu przypadkach kradzież poprzedzona jest wejściem w posiadanie klucza hotelowego do określonego pokoju[16].

W odmienny sposób wywiad prowadzą sprawcy kradzieży sklepowych. Wyszukują obiekty, które znajdują się na rzadko uczęszczanej trasie, zwłaszcza nocą, a wokół nie ma zbyt wielu latarni. Prowadząc rozpoznanie przed włamaniem do sklepu, wywiadowca w pierwszej kolejności obserwuje obiekt z zewnątrz. Sprawdza, o której godzinie po zamknięciu personel opuszcza sklep oraz którymi drzwiami wchodzi i wychodzi. Na szybach wystawowych bardzo często jest umieszczona informacja i logotyp grupy ochrony odpowiadającej za bezpieczeństwo sklepu. Sprawca jest w stanie ustalić, w jakim czasie od włączenia alarmu pojawi się patrol interwencyjny i ile czasu ma na ucieczkę. Po dokonaniu zewnętrznych „oględzin" wywiadowca wchodzi do sklepu, udając klienta. Nie wzbudzając podejrzeń, rozgląda się w środku, zapamiętując, jakiezabezpieczenia posiada wybrany obiekt i gdzie znajdują się przedmioty będące celem planowanego zamachu przestępczego. Jak wykazały badania, sklepy zazwyczaj są najlepiej zabezpieczone i najczęściej wyposażone w dodatkowe zabezpieczenia elektroniczne, dlatego sprawca musi wcześniej opracować plan działania, na podstawie którego w możliwie najkrótszym czasie dostanie się do obiektu, dokona kradzieży i oddali się z miejsca przestępstwa. Kupując drobną rzecz lub rozmieniając pieniądze, włamywacz sprawdza, gdzie znajduje się kasa i jakiego jest typu. Po ustaleniu miejsca przechowywania pieniędzy lub asortymentu będącego celem włamania sprawcy najczęściej planują dokonanie kradzieży w późnych godzinach nocnych.

Wnioski

Analiza działań wywiadowczych współczesnych sprawców włamań w prowadzonych badaniach wykazała, że osoby przesłuchiwane rzadko przyznają się do prowadzenia wnikliwego i wszechstronnego przygotowania przed popełnieniem przestępstwa, chociaż sposób, w jaki dokonano włamania, ponad wszelką wątpliwość wskazywał, że wcześniej prowadzono szczegółowe rozpoznanie. Mimo wysokiego współczynnika stosowania przez sprawców różnych form wywiadu przestępcy zazwyczaj ograniczają się do ogólnego rozeznania na podstawie obserwacji obiektu, która pozostaje nadal desygnatem elementów taktycznych. Implikacją tego staje się

[16] Badania własne na podstawie wywiadów z funkcjonariuszami Wydziału Kryminalnego Komendy Miejskiej Policji w Krakowie w latach 2014–2015.

właściwa interpretacja i zrozumienie pojęcia wywiadu, którego nie należy traktować wyłącznie jako zaawansowanej procedury taktycznej opartej na wszechstronnych i szczegółowych „oględzinach" obiektu wraz z drobiazgowym przygotowaniem do planowanego zamachu przestępczego. Wielokrotnie zdarza się, że sprawca wchodzi w posiadanie wiedzy na temat wybranego obiektu, w którym może znajdować się mienie o wysokiej wartości, wyłącznie dzięki doraźnemu i powierzchownemu rozpoznaniu jako jednej z trzech form prowadzenia wywiadu, które zostały już zdefiniowane w niniejszym opracowaniu. Mimo skąpych danych włamywacz często decyduje się przystąpić do działania wyłącznie na podstawie obserwacji samego obiektu, bez uprzedniego sprawdzenia sposobu zabezpieczeń lub określenia dobowego rytmu przebywania pracowników czy domowników.

Niemniej jednak wyniki badań elementów taktycznych działania sprawców kradzieży z włamaniem pozwoliły w przybliżeniu określić sylwetkę współczesnego „wywiadowcy" i sposób jego działania. Do symptomatycznych elementów taktycznych w stadium przygotowawczym przestępstwa w ramach prowadzonego wywiadu należy zaliczyć:

- opracowanie planu działania,
- wytypowanie i rozpoznanie obiektu,
- dobór odpowiedniej liczby wspólników, jeśli przestępstwo dokonywane jest grupowo,
- przyswojenie odpowiedniej wiedzy koniecznej do dokonania przestępstwa, np. co do sposobu pokonywania zabezpieczeń,
- oszacowanie czasu dokonania przestępstwa i opracowanie strategii działań logistycznych w razie ucieczki,
- zabezpieczenie dróg dojazdowych oraz sposobów wykorzystania naturalnych osłon i barier umożliwiających dokonanie czynu,
- przygotowanie odpowiedniego rodzaju narzędzi przestępstwa, środków transportu itp.,
- przygotowanie fałszywego alibi lub kryjówki,
- pozyskanie poplecznikow i kooperantów jako pomocników w rozumieniu art. 18 § 1 i 3 k.k.

Stosowanie wywiadu przed dokonaniem przestępstwa dotyczy z reguły włamywaczy w dojrzałym wieku, odznaczających się większym stopniem specjalizacji i najczęściej karanych. Rozpoznanie najczęściej prowadzone jest przed włamaniem do obiektów mieszkalnych i handlowo-usługowych i występuje prawie zawsze, jeśli lokal jest wyposażony w zabezpieczenia elektroniczne lub specjalne, a celem czynu jest mienie o wyższej wartości. Wywiad prowadzony jest w formie obserwacji obiektu, obserwacji domowników lub pracowników oraz przez sprawdzenie sposobu zabezpieczeń. Przestępcy, którzy poprzedzają włamanie wywiadem, często używają wcześniej przygotowanych narzędzi podczas pokonywania zabezpieczeń. Do zbierania informacji na temat celu zamachu przestępczego włamywacze wykorzystują wszystkie dostępne nośniki środków masowego przekazu. W trakcie „oględzin" przed

dokonaniem włamania stosują różnorodne i czasami bardzo finezyjne sposoby znakowania obiektu[17].

Biorąc pod uwagę metody wywiadowcze sprawców włamań, należy również uwzględnić wywiad, który został przeprowadzony przez nadawcę. Osoba z bliskiego otoczenia pokrzywdzonego lub sama rodzina informuje sprawców, jakie środki zabezpieczające znajdują się w obiekcie, i dokładnie wskazuje, gdzie są przechowywane wartościowe rzeczy lub pieniądze. W takich przypadkach sprawcy mimo wszystko penetrują obiekt lub nawet go dewastują, aby nie skierować podejrzeń na nadawcę. Jednak z materiałów operacyjnych policji wynika, że obecnie wywiad za pośrednictwem nadawcy jest rzadziej stosowany i najczęściej prowadzony jest przez samych włamywaczy.

Wyniki przeprowadzonych badań upoważniają do stwierdzenia, że w działaniach wywiadowczych sprawców można odnaleźć potencjalne nośniki *modus operandi*. Oczywiście zakres ich występowania jest uwarunkowany wieloma zamiennymi, które pozostają w ścisłej korelacji. Do najistotniejszych należy zaliczyć rodzaj obiektu zamachu przestępczego, jego położenie oraz sposób zabezpieczenia, a także indywidualne cechy samego sprawcy, w szczególności wiek i stopień specjalizacji. Jednakże wypadkowa wszystkich korelatów taktycznych mających wpływ na przebieg przestępstwa w trakcie wywiadu prowadzonego przed dokonaniem włamania uniemożliwia stworzenie zamkniętego katalogu poszczególnych elementów *modus operandi*[18]. Nie należy zakładać, że działanie sprawców na etapie prowadzonego wywiadu cechuje szablonowe powtarzanie wybranych czynności rozpoznawczych. Słusznie zauważył A. Solarz, iż błędna i uproszczona interpretacja sposobu działania sprawcy sprowadza się do rejestracji *modus operandi* przestępcy przez czekanie „jedynie na idealne powtórzenie się wszystkich jego elementów i dopiero na tej podstawie opracowywanie wniosków co do osoby sprawcy”[19]. Sprawca kradzieży z włamaniem nie jest w stanie funkcjonować w „sterylnych” warunkach stworzonych przez siebie dla realizacji własnych celów. W trakcie prowadzonego wywiadu musi reagować na zmieniające się czynniki zewnętrzne lub wewnętrzne, których nie przewidział lub nie zakładał na etapie planowania przestępstwa. Przyjmuje się, że najbardziej wartościowe i znaczące w tworzeniu portretu psychologicznego sprawcy oraz w budowaniujego wzorca są indywidualne cechy samego przestępcy[20]. W sposób szczególny decydują o występowaniu w działaniu włamywacza elementu *constans*, ponieważ

[17] L. Markson, J. Woodhams, J.W. Bond, *Linking serial residential burglary: comparing the utility of modus operandi behaviours, geographical proximity,and temporal proximity*, „Journal of Investigative Psychology and Offender Profiling” 2010, t. 7 (2), s. 91–95.

[18] T. Hanausek, *Identyfikacja kryminalistyczna na podstawie badań modus operandi*, „Studia Kryminologiczne, Kryminalistyczne i Penitencjarne” 1991, t. 21, s. 283–284.

[19] A. Solarz, *Zagadnienie przestępczości zawodowej w Polsce*, Państwowe Wydawnictwo Naukowe, Warszawa 1967, s. 168–169.

[20] B.W. Ewart, G.C. Oatley, K. Burn, *Matching crimes using burglars' modusoperandi: a test of three models*, „International Journal of Police Science & Management” 2005, t. 7 (3), s. 160–162.

o ile zmianie ulegają uwarunkowania zewnętrzne powstałe na skutek oddziaływań autonomicznych, na które sprawca nie ma wpływu, o tyle psychika sprawcy, odpowiadająca za jego postępowanie, pozostaje stosunkowo stała[21].

Stworzona typizacja elementów wywiadowczych stanowi realny i miarodajny układ potencjalnych działań i zaniechań uwarunkowanych czynnikami obiektywnymi i subiektywnymi w oparciu o *modus operandi* włamywacza. Zamierzony przez sprawcę cel może być osiągnięty dzięki zastosowaniu różnych wariantów działań, przy zróżnicowaniu uwarunkowania pomiędzy wyżej wskazanymi komponentami. Dlatego trudno jest uściślić i wytypować ów jednoznaczny i charakterystyczny sposób prowadzenia czynności rozpoznawczych, w związku z tym w trakcie budowania konkretnego *modus operandi* sprawcy należy uwzględnić zmienną elementów taktycznych w stosunku do posiadanego wzorca. Stosowaniu wywiadu jako czynności poprzedzającej włamanie należy zatem poświęcić więcej uwagi, ponieważ możliwości wykorzystywania źródeł informacji o sposobie działania sprawcy kradzieży z włamaniem nie ograniczają się wyłącznie do czynności wykrywczych przy tworzeniu wersji kryminalistycznych[22], ale mogą być wykorzystane jako jeden z komponentów dowodu poszlakowego lub nawet jako podstawa do ustaleń na płaszczyźnie karnomaterialnej[23].

Streszczenie

Niniejszy artykuł ma na celu ukazanie zależności pomiędzy *modus operandi* a wywiadem prowadzonym przed włamaniem jako taktycznego elementu działania sprawców przestępstw przeciwko mieniu. Badaniem objęto 683 postępowania przeciwko oskarżonym o kradzież z włamaniem na podstawie art. 279 § 1 k.k. oraz pozostającego w zbiegu z nim art. 13 § 1 k.k., zakończone prawomocnym wyrokiem, należące do właściwości miejscowej wszystkich wydziałów karnych Sądu Rejonowego w Krakowie w latach 2010–2014. Autor wykorzystał również jako narzędzie badawcze rozmowy i wywiady z funkcjonariuszami Wydziału Kryminalnego Komendy Miejskiej Policji w Krakowie. Celem przeprowadzonych badań było dokładne zobrazowanie metod stosowania wywiadu jako czynności poprzedzającej włamanie w pryzmacie wykorzystania nośników *modus operandi* do identyfikacji sprawców kradzieży z włamaniem do obiektów mieszkalnych i komercyjnych.

Słowa kluczowe: *modus operandi*, wywiad przed włamaniem, kradzież z włamaniem, włamywacze

Summary

This paper evaluates the relationship between the modus operandi and the interview conducted before burglary as a tactical crime method against property. This research involved

[21] L. Tyszkiewicz, *Badania osobopoznawcze w prawie karnym*, Wydawnictwo Prawnicze, Warszawa 1975.

[22] P. Girdwoyń, *Wersje kryminalistyczne. O wykrywaniu przestępstw*, Wydawnictwo Prawnicze PWN, Warszawa 2001, s. 174–175.

[23] M. Całkiewicz, *Modus operandi sprawców zabójstw*, Wydawnictwo Poltext, Warszawa 2010, s. 11.

683 proceedings against the accused burglary pursuant to art. 279 § 1 of the Criminal Code and remaining under the confluence of the art. 13 § 1 of the Criminal Code, completed with the final judgment and remaning in the jurisdiction all of the Districts Court's in Kraków between 2010–2014. As an investigation tool author had used conversations and interviews provided by the Officers of the Criminal Investigation Department of the Municipal Police Headquarters in Kraków. The aim of this study was to illustrate and evaluate precisely the interview users method as the action precedingthe burglary in a prism of using modus operandi media to identify perpetrators of the residentials and commercial objects.

Keywords: modus operandi, interview before the burglary, burglary

Mariusz Michalski, Paweł Łabuz

KARNOPRAWNA INTERPRETACJA „ZAKŁADANIA" ZORGANIZOWANEJ GRUPY PRZESTĘPCZEJ I „KIEROWANIA" NIĄ

Criminal law interpretation of "establishment" and "targeting" of organized criminal group

Wprowadzenie

Przedmiotem rozważań jest artykuł Kodeksu karnego z typem kwalifikowanym w § 3 o znamieniu określającym czynność sprawczą polegającą na „zakładaniu" lub „kierowaniu" grupą lub związkiem mającym na celu popełnianie przestępstw. Bardzo często w środowisku organów ścigania podejrzany lub oskarżony o popełnienie przestępstwa z tego artykułu nazywany jest „liderem zorganizowanej grupy przestępczej".

Przez zakładanie związku należy rozumieć jego utworzenie, czyli doprowadzenie do powstania. Związek można uważać za utworzony z chwilą spełnienia wszystkich warunków koniecznych dla jego bytu. Za założycieli uważa się wszystkich, którzy brali udział w zakładaniu związku, tj. zarówno inicjatorów, jak i tych, którzy swoją działalnością organizatorską doprowadzili do jego powstania. Przez pojęcie „doprowadzili" należy rozumieć więcej niż „przyczynili się"; odpowiedzialności karnej za zakładanie związku może podlegać ten, kto uczestnicząc w jego założeniu, przyczynił się do tego w stopniu większym niż podżegacz lub pomocnik[1].

Sieciowa struktura organizacji przestępczych od wielu lat przysparza organom ścigania wielu problemów związanych nie tylko z określeniem jej budowy wewnętrznej, przypisaniem skali odpowiedzialności poszczególnym członkom organizacji (węzłom sieci), lecz także z precyzyjnym wytypowaniem struktury z całości relacji społecznych. Problemem jest także określenie, w jaki sposób i jakie reguły kierują doborem nowych węzłów w sieciach przestępczych, przyjęciem zasad wzajemnego sterowania czy rozliczania z realizacji zakładanych celów[2].

---

[1] B. Drozdowska, *Przestępczość grupowa nieletnich*, rozprawa doktorska napisana w Zakładzie Prawa Karnego Uniwersytetu Warszawskiego pod kierunkiem prof. dr. hab. Genowefy Rejman, Warszawa 2000, s. 82.

[2] M.A. Kędzierski, *Sieciowość współczesnych organizacji przestępczych funkcjonujących w obszarze przestępczości zorganizowanej i terroryzmu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10/14, s. 74.

Interpretacja prawno-kryminologiczna art. 258 § 3 kodeksu karnego

Przedstawiciele polskiej nauki prawa karnego zgadzają się natomiast zasadniczo co do tego, że czynność wykonawcza polegająca na „kierowaniu" nie oznacza samego stania na czele określonej struktury, ale przeciwnie – wymaga pewnej aktywności, której przejawem są konkretne działania przedsiębrane w ramach grupy albo związku. Chodzi zatem np. o wszelkiego rodzaju decyzje, wiążące polecenia wydawane członkom, czyli, ogólnie ujmując, o pewną faktyczną kontrolę nad działalnością danej struktury (lub jej samodzielnego fragmentu)[3].

Współdziałający ze sobą sprawcy o niższym stopniu zorganizowania lub w odniesieniu do których brak jest dowodów umożliwiających przedstawienie zarzutów dotyczących zakładania zorganizowanej grupy albo związku przestępczego, udziału w nim lub kierowania nim, mogą być ścigani w oparciu o inne instytucje prawa karnego, takie jak pomocnictwo, współsprawstwo, sprawstwo kierownicze czy polecające, bądź też, bez względu na formę zorganizowania, za popełnienie określonego przestępstwa, np. rozboju czy wyłudzenia[4].

Przestępczość zorganizowana nie została też jednoznacznie zdefiniowana na gruncie prawa międzynarodowego. Jednak podobnie jak w prawie krajowym, również na płaszczyźnie międzynarodowej[5], a także na gruncie prawa Unii Europejskiej zawarte zostały unormowania definiujące zorganizowane grupy i organizacje przestępcze.

Zakładanie to tyle co organizowanie, a więc wyszukiwanie kandydatów, składanie propozycji uczestnictwa, obmyślanie struktury i sposobu działania, ustalenie siedziby, uzgadnianie sposobu komunikowania się, wyłonienie przywódców, gromadzenie narzędzi, wprowadzanie systemu zabezpieczeń. Zakładać grupę lub związek przestępczy może jedna osoba, pozostałe zaś już tylko do niego następnie przystępują, bądź też założycielami może być wiele osób, przy czym każda z nich odpowiada za inny element organizacji, względnie też wykonują całość zadań wspólnie.

---

[3] J. Badziak, *Przestępstwo z art. 258 kodeksu karnego z 1997 r. – studium prawnodogmatyczne*, Partner Poligrafia, Łódź 2014, s. 152.

[4] *Krajowy program przeciwdziałania i zwalczania przestępczości zorganizowanej na lata 2012–2016*, Departament Analiz i Nadzoru MSWiA 2012, s. 5.

[5] Zgodnie z Konwencją Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjętą 15 listopada 2000 r. w Palermo i ratyfikowaną przez Polskę w 2001 r., zorganizowana grupa przestępcza oznacza posiadającą strukturę grupę składającą się z trzech lub więcej osób, istniejącą przez pewien czas oraz działającą w porozumieniu w celu popełnienia jednego lub więcej poważnych przestępstw, tzn. podlegających maksymalnej karze pozbawienia wolności w wysokości co najmniej czterech lat lub karze surowszej, dla uzyskania, w sposób bezpośredni lub pośredni, korzyści finansowej lub innej korzyści materialnej.

Na gruncie prawodawstwa Unii Europejskiej, zgodnie z decyzją ramową Rady Unii Europejskiej 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej, organizacja przestępcza została zdefiniowana jako zorganizowana grupa, istniejąca przez pewien czas, składająca się z więcej niż dwóch osób, działających wspólnie w celu popełnienia przestępstw.

Kierowanie polegać będzie na faktycznym sprawowaniu kontroli nad działalnością związku lub grupy, możliwości wydawania poleceń i podejmowania zasadniczych decyzji. Kierowanie może mieć charakter stały lub przejściowy, kolektywny lub jednoosobowy. Jeżeli struktura grupy lub związku jest bardziej złożona, odpowiedzialność za „kierowanie" powstaje już wtedy, gdy kierujący odpowiada za prawidłowe funkcjonowanie nawet tylko samodzielnego fragmentu tej struktury, który zdolny jest jednak do odrębnego funkcjonowania. Dla odpowiedzialności nie jest konieczne kierowanie całym związkiem lub grupą przestępczą. Sprawca odpowiada karnie już wtedy, kiedy uczestniczy w „zakładaniu", a nie dopiero wtedy, gdy grupę lub związek „założy"[6].

Przywódca zawsze umieszczany był w centrum, jako osoba stawiająca cele, sprawująca nad wszystkim kontrolę i ponosząca za wszystko odpowiedzialność. Podwładni traktowani są jako narzędzia, którymi posługuje się on w realizacji swoich celów. Niewiele zmian do teorii przywództwa wprowadziła koncepcja organiczna. Kierownik traktowany był w niej jako „mózg lub głowa" systemu organizacyjnego, podczas gdy pracownicy wykonawczy spełniali funkcję „organów", zdolnych do skomplikowanych wprawdzie, ale rutynowych działań, podejmowanych w dodatku nie samodzielnie, ale za sprawą koordynujących decyzji przełożonego. Koncepcja ta podkreślała znaczenie „organu sterującego" całością działań organizacji, formułując wytyczne dotyczące szczególnej jego ochrony. Bez organu sterującego, czyli bez przywódcy, organizacja traci bowiem możliwość przetrwania. Zarówno w mechanistycznej, jak i organicznej koncepcji przywództwa zasadnicze znaczenie ma hierarchia władzy organizacyjnej. System hierarchiczny jednoznacznie reguluje relacje między członkami organizacji, sprowadzając je do różnic w zakresie uprawnień decyzyjnych.

Przywódcy organizacji przestępczej przypominają przedsiębiorców. Muszą pokonywać wszelkie trudności, z jakimi borykają się normalni przedsiębiorcy, np. angażować odpowiedni personel i organizować produkcję, transport i dystrybucję towarów. Muszą oceniać np. możliwości zbytu swych produktów, by zapewnić popyt na nielegalne towary (analiza struktury nielegalnego rynku w społeczeństwie). Ponadto muszą zabezpieczyć swoją organizację przestępczą przed próbami rozbicia jej przez wymiar sprawiedliwości, np. przez utworzenie prywatnej armii. Muszą również osłabić polityczne i ekonomiczne struktury władzy w społeczeństwie za pomocą korupcji[7].

---

[6] *Komentarz do art. 259 kodeksu karnego* (Dz.U.97.88.553), w: A. Barczak-Oplustil, G. Bogdan, Z. Ćwiąkalski, M. Dąbrowska-Kardas, J. Majewska, J. Raglewski, M. Rodzynkiewicz, M. Szewczyk, A. Wróbel, A. Zoll, *Kodeks karny. Część szczególna*, t. II, Kantor Wydawniczy Zakamycze, Kraków 2006.

[7] H.J. Schneider, *Przestępczość zorganizowana z perspektywy kryminologii porównawczej*, w: B. Hołyst, E. Kube, R. Schulte (red.), *Przestępczość zorganizowana w Niemczech i w Polsce. Zwalczanie i zapobieganie*, Polskie Towarzystwo Higieny Psychicznej, Warszawa–Łódź–Münster 1996, s. 10–11.

Analiza ostatnich przemian w środowiskach przestępczych dowodzi, że osoby kierujące działalnością przestępczą czynią to w sposób pośredni – bez osobistego angażowania się w jakiekolwiek nielegalne przedsięwzięcia. Przywódcy grup nowego typu dystansują się od działalności kryminalnej, która w przeszłości dała im możliwość zaistnienia w grupie i zdobycia środków pozwalających na późniejsze rozszerzenie aktywności przestępczej, wyjście poza granice kraju. Kreują się oni na szanowanych obywateli, swój dobry wizerunek umacniają przez sponsorowanie popularnych imprez i akcji charytatywnych. Jednocześnie z powodzeniem pretendują do udziału w renomowanych organizacjach zrzeszających przedstawicieli świata biznesu, kultury i polityki.

Trafne jest orzeczenie Sądu Apelacyjnego w Lublinie wydane wprawdzie na tle przepisów kodeksu karnego z 1969 r., ale nadal zachowujące aktualność (z 27 stycznia 1998 r., II AKZ 34/98, Apel.-Lub. 1998, nr 1, poz. 9), zgodnie z którym pojęcie „kierowania" nie oznacza tylko sytuacji o charakterze statycznym, sprowadzającej się do sprawowania władztwa nad istniejącą strukturą.

Związek można uznać za utworzony z chwilą spełnienia wszystkich warunków koniecznych dla jego bytu. Za założycieli uważa się wszystkich, którzy brali udział w zakładaniu związku, tj. zarówno inicjatorów, jak i tych, którzy swoją działalnością organizatorską doprowadzili do jego powstania. Przez pojęcie „doprowadzalności" należy rozumieć więcej niż określenie „przyczynili się". Według J. Makarewicza[8] założycielem związku jest także ten, kto utworzył nowe ogniwo związane już z istniejącym ugrupowaniem, podporządkowane mu – z tym zastrzeżeniem, że musi ono wówczas samodzielnie wyczerpywać znamiona związku.

Za organizatorów należy uznać również osoby współdziałające przy powstaniu grupy lub związku, zwłaszcza przy ustalaniu celów, programu działania i wyłonieniu kierownictwa. Funkcje kierownicze sprawuje nie tylko ten, kto jednoosobowo kieruje związkiem lub grupą, ale także – zależnie od struktury organizacyjnej – członek kierownictwa, jak również osoby kierujące doniosłymi odcinakami działalności związku lub grupy. Sprawca kieruje związkiem, jeśli wydaje wiążące polecenia innym jego członkom. Moc wiążąca tych poleceń nie może wynikać tylko z dobrowolnego podporządkowania się autorytetowi, lecz musi być poparta sankcjami ustalonymi *expressis verbis*, czyli też występującymi w sposób dorozumiany, w ramach zasad działania związku. Nie należy utożsamiać kierowania w powyższym sensie ze sprawstwem kierowniczym, ponieważ te pojęcia się wzajemnie nie pokrywają[9].

W przypadku sprawstwa kierowniczego zarysowany model wykładni[10] prowadzi do odczytania znamion typu, w których określone jest zachowanie kierującego oraz

[8] Zob. J. Makarewicz, *Kodeks karny z komentarzem*, Lwów 1938, s. 433.

[9] K. Laskowska, *Teoretyczne i praktyczne podstawy odpowiedzialności z art. 258 k.k.*, „Prokurator" 2004, nr 1, s. 15.

[10] Wyrok SN z dnia 26 kwietnia 1982 r., Rw 268/82, OSNKW 1982, nr 10–11, poz. 83 (dotyczy art. 46 dekretu z dnia 12 grudnia 1981 r. o stanie wojennym, DzU Nr 29, poz. 154 z późn. zm. oraz pojęć „organizowanie" i „kierowanie"); wyrok SN z dnia 23 marca 1992 r., II KRN 433/91, OSNKW 1992, nr 7–8, poz. 48 (dotyczy pojęcia „związek" i „kierowanie"); wyrok

kierowanego (bezpośredniego wykonawcy). Zachowanie kierującego polega na czynnościach sterowania zachowaniem innej osoby (kierowanego), która bezpośrednio i osobiście wypełnia znamiona typu. Z istoty czynności wykonawczej kierującego wynika, iż musi on posiadać władztwo nad osobą kierowaną i jej zachowaniem, sięgające, jak podkreśla się w polskim piśmiennictwie i orzecznictwie, aż po możliwość odwołania w wybranym przez kierującego momencie akcji przestępnej[11]. Kierowanie nie musi wyczerpywać znamion sprawstwa kierowniczego. Szczególnie jest to widoczne na przykładzie grup o bardzo rozbudowanej strukturze wewnętrznej i zakonspirowanym kierownictwie (mafii). Taktyka ich działania zakłada z reguły daleko idące zakonspirowanie osób kierujących, które często nawet nie uczestniczą w popełnianiu poszczególnych przestępstw lub nawet nie decydują o przebiegu działań przestępczych w sposób umożliwiający zarzucenie im sprawstwa kierowniczego.

Klasyczna postać dokonanego sprawstwa kierowniczego sprowadza się do wypełnienia czynności kierowania przez kierującego oraz wypełnienia co najmniej przedmiotowych znamion czynu zabronionego przez kierowanego (bezpośredniego wykonawcę). W przypadku osiągnięcia przez zachowanie kierowanego jedynie stadium usiłowania kierujący odpowiadał będzie za usiłowanie[12]. Niezależnie od tego, czy podstawą odpowiedzialności będzie stadium dokonania czy usiłowania, w każdym przypadku kierującego uznaje się za sprawcę czynu zabronionego, popełnionego bezpośrednio przez osobę kierowaną, co wyraźnie wskazuje, że mamy tutaj do czynienia z pośrednim zamiarem popełnienia przestępstwa[13].

Odpowiedzialność założyciela lub kierującego związkiem wg K. Buchały pojawia się już z chwilą powołania grupy lub związku[14]. Pogląd ten należy oczywiście podzielić, gdy chodzi o odpowiedzialność założyciela, natomiast kierujący związkiem może ponosić odpowiedzialność – jak się zdaje – dopiero wówczas, gdy podejmie czynności mieszczące się w pojęciu kierowania, nie zaś już z chwilą samego założenia ugrupowania. W tym zakresie za trafny uznać należy raczej pogląd Z. Ćwiąkalskiego, który, powołując się na aprobowane przez siebie tezy orzeczenia Sądu

SA w Katowicach z dnia 7 grudnia 2000 r., II Aka 184/00, KZS 2001, z. 1, poz. 26 (dotyczy pojęcia „kierowanie zorganizowaną grupą przestępczą"); postanowienie SA w Lublinie z dnia 27 stycznia 1998 r., II Akz 34/98, OSA 1998, nr 9, poz. 47 (dotyczy statycznych i dynamicznych elementów pojęć „kierowanie" i „branie udziału" w zorganizowanej grupie przestępczej); postanowienie SA w Katowicach z dnia 15 stycznia 2003r., II AKz 1249/02, OSA 2003, nr 7, poz. 74 (dotyczy elementów pojęcia „kierowanie zorganizowaną grupą przestępczą").

[11] P. Kardas, *Regulacja współdziałania przestępnego jako podstawa zwalczania przestępczości zorganizowanej*, „Prokuratura i Prawo" 2002, nr 10, s. 74–75.

[12] Należy podkreślić, że usiłowanie sprawstwa kierowniczego będzie miało miejsce także wtedy, gdy bezpośredni wykonawca nie podejmie żadnych czynności zmierzających do wykonania czynu zabronionego, zarazem kierujący podejmie zachowanie stanowiące bezpośrednie zmierzanie do kierowania zachowaniem innej osoby mającym na celu wykonanie czynu zabronionego. Zob. szerzej P. Kardas, *Teoretyczne podstawy odpowiedzialności karnej za przestępne współdziałanie*..., s. 824 i n.

[13] P. Kardas, *Regulacja współdziałania przestępnego*..., op. cit., s. 75.

[14] K. Buchała, A. Zoll, *Kodeks karny, część ogólna*, Zakamycze, Kraków 1988, s. 475.

Apelacyjnego w Lublinie[15], jest zdania, iż kierowanie, określające pewną dynamikę sytuacji, oznacza nie tylko przewodzenie zorganizowanej grupie przestępczej, lecz również kierowanie jej konkretnymi działaniami[16].

Sprawcę możemy uznać za kierującego związkiem przestępczym lub zorganizowaną grupą przestępczą tylko wówczas, gdy wydaje on innym członkom tych struktur przestępczych wiążące ich polecenia, w tym polecenia wykonania czynu zabronionego, a zatem gdy jest sprawcą polecającym w rozumieniu art. 18 § 1 k.k. Moc wiążąca takich poleceń nie wynika jednakże wyłącznie z dobrowolnego podporządkowania się autorytetowi „przywódcy", ale musi zostać poparta sankcjami ustalonymi wyraźnie przez członków organizacji albo obowiązującymi w sposób dorozumiany i mieszczącymi się w ramach reguł działania grupy lub związku. Jakkolwiek każda zorganizowana grupa lub związek przestępczy odznacza się odmiennymi, indywidualnymi cechami, na które wpływ mają przede wszystkim geneza i okoliczności formowania się organizacji kryminalnej, to wyniki badań empirycznych przeprowadzonych wśród funkcjonariuszy organów ścigania zajmujących się zwalczaniem przestępczości zorganizowanej dowodzą, że do najsilniejszych powiązań łączących członków zorganizowanej struktury przestępczej funkcjonującej w polskich warunkach należy więź strachu. Uniemożliwia ona pojedynczej osobie odejście z grupy i podporządkowuje szeregowych członków organizacji jej kierownikowi. Co więcej, wyniki wspomnianych badań pozwalają sformułować wniosek, że koniecznym warunkiem „sprawnego" prowadzenia przez grupę lub związek przestępczej działalności jest posiadanie silnego, twardego i bezwzględnego przywódcy, który jest w stanie utrzymać strachem podległych sobie członków grupy w ryzach. Badania empiryczne przeprowadzone wśród „skruszonych" sprawców, którzy uzyskali status „świadka koronnego", dowodzą z kolei, że w znacznej części zorganizowanych struktur przestępczych ich lider ma władzę nieograniczoną, istotnym warunkiem przyjęcia do organizacji jest „wykonanie pierwszego poważnego zlecenia i stałe posłuszeństwo", a nieposłuszni i niepokorni członkowie grupy lub związku karani są sankcjami finansowymi **łożonymi** na rzecz szefa, odsunięciem od możliwości zdobywania środków finansowych, pobiciem, a częstokroć nawet fizyczną eliminacją krnąbrnego podwładnego. Lider zorganizowanej grupy lub związku przestępczego funkcjonującego na wspomnianych powyżej zasadach jawi się zatem jako potencjalny sprawca polecający. Co istotne, czynności składające się na kierowanie grupą lub związkiem przestępczym nie muszą wyczerpywać każdorazowo znamion sprawstwa kierowniczego w przypadku poszczególnych przestępstw popełnionych w ramach grupy lub związku. Z sytuacją taką będziemy mieć do czynienia w szczególności w obrębie wysoko zorganizowanych związków mafijnych. Jednym z elementów taktyki ich funkcjonowania jest zazwyczaj głęboka konspiracja „kierowników" organizacji. Nie tylko nie uczestniczą oni wówczas w realizacji czynności wykonawczych składających się

[15] Orzeczenie SA w Lublinie z dnia 27.01.1998 r.; II Akz 34/98.

[16] C. Sońta, *Zorganizowana grupa i związek przestępczy we współczesnym polskim prawie karnym*, rozprawa doktorska napisana w Zakładzie Prawa Karnego Uniwersytetu Warszawskiego pod kierunkiem prof. dr hab. Genowefy Rejman, Warszawa 2000, s. 87.

na poszczególne przestępstwa, ale nie decydują nawet o przebiegu przestępnej akcji w sposób umożliwiający przypisanie im sprawstwa kierowniczego popełnianego czynu zabronionego. Wykonanie takiego czynu zabronionego, z reguły gruntownie przygotowane, uwarunkowane jest jednak ich zgodą, a niejednokrotnie poleceniem, co może pozwolić na ukaranie wspomnianych „kierujących zorganizowaną grupą lub związkiem przestępczym" za sprawstwo polecające[17].

Wydaje się, że w przyszłości przywódca będzie miał niewiele wspólnego z tymi, których określa się dzisiaj tym mianem. Niektórzy nazywają go liderem, który nie kieruje bezpośrednio działaniami ludzi, ale raczej pracuje z nimi dla osiągnięcia wspólnych celów, który myśli z ludźmi, a nie sam. Przywódca bowiem powinien w przyszłości być przede wszystkim agentem zmiany kulturowej, co zbliża go do nauczyciela, stwarzającego sytuację, inspirującego, pomagającego podwładnym precyzować cele i zadania, uświadamiającego skutki zmiany kultury, współuczestniczącego w analizie i rozwiązywaniu grupowych i indywidualnych problemów[18].

Ze stopniem i kierunkiem zorganizowania grupy przestępczej ściśle związany jest podział funkcji i ról, jakie pełnią poszczególni członkowie. Jednym z najważniejszych kryteriów wyodrębnienia funkcji elementów zorganizowanej grupy przestępczej jest zakres, w jakim członek grupy może podejmować decyzje samodzielnie, jak również rodzaj zadań przez niego realizowanych. W większości zorganizowanych grup przestępczych wyróżnić można trzy rodzaje funkcji, jakie są pełnione przez jej członków:

- kierownicze – główne zadanie to organizowanie działalności przestępczej grupy, osoby pełniące takie funkcje zazwyczaj nie uczestniczą w popełnianiu przestępstw, stronią od kontaktu z wykonawcami;
- pośrednie – zajmowanie się bezpośrednią działalnością przestępczą;
- wykonawcze – wykonawcy poleceń.

Kierowanie[19] może mieć charakter stały lub przejściowy, kolektywny lub jednoosobowy. Jeżeli struktura grupy lub związku jest bardziej złożona, odpowiedzialność za „kierowanie" powstaje już wtedy, gdy kierujący odpowiada za prawidłowe funkcjonowanie nawet tylko samodzielnego fragmentu tej struktury, który zdolny jest jednak do odrębnego funkcjonowania. Dla odpowiedzialności nie jest konieczne kierowanie całym związkiem lub grupą przestępczą. O ile „zakładanie" jest czynnością

[17] M. Czyżak, *Sprawstwo polecające w zorganizowanej strukturze przestępczej*, „Prokuratura i Prawo" 2004, nr 6, s. 42–44.

[18] S.M. Kania, *Przywództwo w organizacji*, „Zeszyty Naukowe WSB", nr 2, Gdańsk 2003, s. 123–125.

[19] Kierowanie zorganizowaną grupą przestępczą polega na wydawaniu innym członkom grupy poleceń, których wykonanie wynika bądź z dobrowolnego podporządkowania się autorytetowi kierującego, bądź jest poparte także sankcjami ustalanymi czy to wyraźnie, czy w sposób dorozumiany w ramach zasad działania grupy. Funkcję kierowniczą sprawuje nie tylko kierujący grupą jednoosobowo, ale i osoby kierujące doniosłymi odcinkami działalności grupy choćby krótkotrwale, a nawet jednorazowo przy realizacji zadania (tak SA w Krakowie w wyroku z 2 listopada 2004 r., II Aka, 119/04, KZS 2005, z. 3, poz. 24).

rozciągniętą w czasie, mającą jednak co do zasady swój początek i koniec, którym jest „założenie" grupy lub związku przestępnego, o tyle „kierowanie" jest czynnością o charakterze względnie trwałym, co nie znaczy, iż kierującego nie może zastąpić w dowolnym momencie ktoś inny[20].

W poszukiwaniu odpowiedzi na pytanie o właściwy kierunek wykładni przedmiotowego znamienia[21] „kierowania zorganizowaną strukturą" w pierwszej kolejności należy się odwołać do ustawowej konstrukcji postaci zjawiskowej polegającej na kierowaniu wykonaniem czynu zabronionego przez inną osobę. Nie ulega wątpliwości, że sprawstwo kierownicze – bo o nim mowa – jako odrębna od jednosprawstwa i współwsprawstwa forma realizacji znamion czynu zabronionego charakteryzuje się tym, że sprawca samodzielnie nie wykonuje tego czynu, lecz współdziała z osobą będącą jego bezpośrednim wykonawcą[22].

Konkluzja

Funkcje, jakie są pełnione w grupie, nie zawsze przekładają się na role odgrywane w poszczególnych przestępczych działaniach grupy. Osoba piastująca funkcję kierowniczą w zorganizowanej grupie przestępczej kieruje działaniami przestępczymi. Dzieje się tak z reguły w zorganizowanych grupach przestępczych, które liczebnie można uznać za małe. W zorganizowanych grupach przestępczych, które są większe, niemal nie zdarza się, aby osoba pełniąca funkcję kierowniczą brała udział w działaniach na etapie wykonawczym. Osoby te uczestniczą tylko w planowaniu i przygotowaniu działań przestępczych. Natomiast do kierowania wykonaniem czynu przestępczego zostają wyznaczone osoby z niższego, a nawet najniższego szczebla. W takich przypadkach funkcja kierownicza całej zorganizowanej grupy[23] bardzo często jest niewidoczna i w odniesieniu do danego przestępstwa zyskała miano kierowania pośredniego lub częściowego.

Coraz częściej grupy działają w tzw. strukturach poziomych bez wyodrębnionych liderów. Powiązania przestępcze członków nie są zhierarchizowane, a mimo wyraźnego podziału ról przestępczych i występujących ścisłych powiązań członków występuje brak wyraźnego podporządkowania. Pewna swoboda we wzajemnych relacjach w tego typu grupach przejawia się między innymi w możliwości równoległego kooperowania ich członków z przedstawicielami innych grup przestępczych z tej samej branży oraz zaprzestania działalności w takiej grupie bez konsekwencji. Wynika to głównie z niestosowania przymusu, wydawania poleceń czy dyscyplinowania członków. Grupy takie, mimo działania w sposób w pełni zorganizowany, często w ocenie organów ścigania (np. prokuratury) nie są klasyfikowane jako zorganizowane grupy przestępcze. Takie stanowisko zostało przyjęte po ogłoszeniu wyroków

[20] G. Grochola, *Zorganizowana grupa przestępcza jako grupa społeczna. Ujęcie socjologiczno-prawne*, „Internetowy Przegląd Prawniczy TBSP UJ" 2013, nr 3–4 (13), s. 19.
[21] J. Badziak, op. cit., s. 93.
[22] Tamże, s. 94.
[23] G. Grochola, op. cit., s. 17.

w pewnych sprawach, w których sądy nie utrzymywały kwalifikacji art. 258 k.k., argumentując jak wyżej.

Współcześnie trudno jest dokonać w pełni adekwatnego i uniwersalnego opisu struktury zorganizowanych grup przestępczych czy budowy ich typowego modelu organizacyjnego. Kwestię tę komplikuje nie tylko fakt stosunkowo małej liczby źródeł zawierających przydatne analizy informacje, lecz także wielość możliwych aspektów charakterystyki struktur zorganizowanych grup przestępczych, takich jak przykładowo liczebność, skład etniczny, formy i rodzaje powiązań, sposoby zarządzania czy charakterystyka ich elementów składowych[24].

Według raportu Centralnego Biura Śledczego Komendy Głównej Policji za 2012 rok polskie grupy przestępcze kierowane były przez **817** zidentyfikowanych liderów, grupy międzynarodowe przez **127**, rosyjskojęzyczne przez **8**, cudzoziemców **7**. Według stanu na 31 grudnia 2014 roku, łączna liczba liderów pozostających w zainteresowaniu Centralnego Biura Śledczego Policji wynosiła **959**[25].

Streszczenie

W prezentowanej publikacji poruszono problematykę interpretacji art. 258 § 3 kodeksu karnego dotyczącego ustalenia i określenia lidera zorganizowanej grupy przestępczej. Na przykładzie dostępnej doktryny i orzecznictwa wyjaśniono kwestię analizy prawa karnego materialnego w odniesieniu do zakładania zorganizowanej grupy przestępczej i kierowania nią.

Słowa kluczowe: przestępczość zorganizowana, prawo karne, lider grupy przestępczej, związek przestępczy

Summary

The publication addresses the problem of interpretation of art. 258 § 3 of the Criminal Code on the findings and determine the leader of an organized criminal group. For example, the available doctrine and case law clarified the analysis of substantive criminal law setting up and managing an organized criminal group.

Keywords: organized crime, criminal law, the leader of a criminal group, the association

[24] M. Cichomski, *Struktury zorganizowanych grup przestępczych*, w: W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana: fenomen, współczesne zagrożenia, zwalczanie, ujęcie praktyczne*, Wyższa Szkoła Policji, Szczytno 2013, s. 66.

[25] Dane za stroną: http://cbs.policja.pl/cbs/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html (z dnia 19.05.2015).

Zbigniew Szachnitowski

CZY TĘCZÓWKA OKA BĘDZIE KOLEJNĄ BIOMETRYKĄ WYKORZYSTYWANĄ W POLSKIEJ KRYMINALISTYCE?

Will iris recognition be another biometric method used in Polish forensic science?

Wprowadzenie

Intencje twórców systemów monitoringu wizyjnego (CCTV[1]) przestrzeni publicznej i ich cele w ostatnich kilkunastu latach nie uległy zasadniczym zmianom. Nadal są one związane z zapewnieniem szeroko rozumianego bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia w określonym miejscu. Przyjęte niegdyś założenia co do ich funkcjonalności dalej są aktualne, a także dominuje przekonanie, iż tego typu działania mają charakter prewencyjny i skutecznie zniechęcają czy nawet odstraszają potencjalnych sprawców przed czynieniem przysłowiowego zła i łamania prawa pod okiem „Wielkiego Brata". Ponadto kiedy są skuteczne, powodują prawie natychmiastowe działania zapobiegawcze, takie jak szybka interwencja ograniczająca lub całkowicie neutralizująca wystąpienie niepożądanych zagrożeń. Istotny w tych działaniach jest także czynnik dowodowy – decydujący m.in. o nieuchronności kary dla sprawców za popełnione przez nich przestępstwa na podstawie zgromadzonego materiału fotograficzno-filmowego. Materiał ten zawiera czasem swoistą dokumentację techniczną zaistniałych przestępstw i wykroczeń z wizerunkami sprawców oraz utrwaleniem ich roli w zaistniałych zdarzeniach. Często można z nich także zaczerpnąć informacje na temat innych istotnych okoliczności zdarzenia, takich jak sposób działania sprawców, drogi poruszania się i użyte przez nich narzędzia. Warto jednak zauważyć, iż przydatność dowodowa wizerunków tychże sprawców w zależności od środków technicznych, jakimi w danym czasie dysponowali administratorzy systemów CCTV, jest zmienna i z upływem lat ulega ciągłej poprawie. Dotyczy ona w szczególności coraz większych możliwości technicznych kamer, które z każdym rokiem widzą więcej i dalej bez względu na warunki pracy, jakie panują w środowisku ich zamontowania. Praktyka jednak dowodzi, że nie wszyscy sprawcy napadów i kradzieży obawiają się ujawnienia swojej tożsamości za sprawą zamontowanego w danym miejscu systemu CCTV. Często znają ich ograniczenia, głównie natury jakościowej uzyskiwanych obrazów, a także zawężone możliwości dalszego

[1] CCTV – Closed Circuit Television – system dozoru wizyjnego wyznaczonej przestrzeni.

ich wykorzystania w charakterze dowodu. Stopniowo staje się niemal nawykiem również to, że przestępcy zmieniają swój wygląd, np. przez maskowanie twarzy, i zakładają rękawiczki, pamiętając również o unikaniu możliwości pozostawienia po sobie śladów na miejscach dokonywanych przestępstw. Bywa też, że informacja o napadzie, wydawane polecenia określające ich żądania oraz groźby użycia broni palnej podawane są wyłącznie pisemnie, np. na podsuniętej kasjerce w banku kartce papieru. Podobny sposób postępowania w przekonaniu sprawców zapewnia im anonimowość, a tym samym i bezkarność. Rzeczywiste trudności w pozyskiwaniu odpowiedniego materiału dowodowego, skutkujące brakiem możliwości ustalania tożsamości sprawców w takich przypadkach, stanowią często duże wyzwanie na przyszłość zarówno dla inwestorów, projektantów systemów monitoringu wizyjnego, jak i przedstawicieli organów ścigania. Stan taki jest nie do zaakceptowania i stwarza potrzebę prowadzenia poszukiwań w celu jakościowego udoskonalenia metod identyfikacji osób na podstawie zdjęć, wykraczających nawet poza standardy, jakimi dziś dysponuje kryminalistyka, i skłania do ich poszerzenia np. o takie metody, które aktualnie wykorzystuje biometria[2] przy uwierzytelnianiu tożsamości osób w systemach kontroli dostępu.

Wybrane biometryczne metody ustalania tożsamości osób

Dotychczasowe osiągnięcia biometrii dostarczyły niezwykle skutecznych metod uwierzytelniania osób, dających możliwość dokonania zarówno weryfikacji, jak i identyfikacji osób na podstawie cech biometrycznych. Podstawowe ich rodzaje (biometryki) to cechy fizyczne linii papilarnych palców, twarzy, tęczówki oka, naczyń krwionośnych palców i dłoni, geometria dłoni. Jednak najistotniejsze z punktu widzenia omawianych tu zagadnień są cechy fizyczne twarzy ludzkiej lub jej fragmentów i tęczówki oka. Zatem paletę dostępnych metod identyfikacji osób, oprócz tych stosowanych w kryminalistyce, dopełniają badania jeszcze jednego elementu składowego twarzy, którym są oczy. Od początku istnienia kryminalistyki odgrywały one istotną rolę, lecz tylko jako jeden z elementów rysopisu sprawców i osób poszukiwanych. Zasadę obligatoryjnego ich opisu poprzez wypełnienie pozycji w formularzu – *barwa i kształt oczu* – wprowadził już Alfons Bertillon[3] w utworzonym przez siebie rysopisie opisowym, tzw. portrecie mówionym (*fr*. *portrait parlé*). Stanowił on przez wiele lat sposób opisu człowieka, odnoszący się jednak prawie wyłącznie do jego cech grupowych, przy czym ich zespół traktowano wówczas jako argument przydatny

[2] Biometria to nauka zajmująca się pomiarami istot żywych, obecnie głównie w celach automatycznego uwierzytelniania tożsamości człowieka na podstawie tego, co w nim niepowtarzalne, czyli unikatowości jego wyglądu, indywidualnych cech fizycznych i charakterystycznego dla danego osobnika sposobu zachowania.

[3] Alfons Bertillon – antropolog, pracownik policji paryskiej pod koniec XIX wieku, twórca antropometrii kryminalistycznej, w tym:
– antropometrycznej kartoteki rejestracyjnej opartej na pomiarach ludzkiego ciała (wyszła z użycia),
– portretu opisowego (ciągle aktualny).

do identyfikacji przestępców. Podobnie miała się rzecz z portretem pamięciowym sprawców zdarzeń o charakterze kryminalnym. Poza odtworzeniem przybliżonej do widzianej u sprawcy twarzy, w tym ułożenia szpary ocznej, oraz poprawnym ustaleniem rozstawu oczu, bardzo rzadko udawało się sporządzającemu portret umieścić w obrębie samej gałki ocznej obraz jakichś charakterystycznych cech oczu danego osobnika, które wyróżniałyby go w sposób indywidualny spośród innych ludzi. Jak się powszechnie sądzi, nie pozwalają na to z reguły ograniczone właściwości percepcyjne ludzi, którzy nie są w stanie zapamiętać istotnych cech w obrębie samej gałki ocznej widzianego osobnika. Inną rzeczą jest także zdolność przekazania w formie relacji ustnych ekspertowi tych ewentualnie dostrzeżonych przez siebie cech w celu ich graficznego utrwalenia lub wyboru podobnych z przedstawionego katalogu/bazy danych. Aktualnie prowadzone prace nad programami komputerowymi, noszącymi nazwę systemów czwartej generacji, np. Evofitu[4], nie stanowią również remedium na ten rodzaj trudności, nowe metody wykonywania wizerunków przestępców skupione są bowiem na wyeliminowaniu konieczności reprodukcji poszczególnych cech twarzy, bazują zaś na automatycznym doborze kolejnych kompletnych wizerunków o możliwie najlepszym podobieństwie, aż do uzyskania zadawalającego świadka obrazu sprawcy, a nie tylko jego oczu.

Dziedziną badań kryminalistycznych wykorzystującą m.in. oczy jako przedmiot badań porównawczych jest antropometria[5] i antroposkopia[6]. W badaniach takich właśnie oczy i ich bezpośrednie sąsiedztwo stanowią jeden z najważniejszych elementów twarzy zestawianych ze sobą. Jednak poza nielicznymi wyjątkami miejsce usytuowania cech indywidualnych danego osobnika oraz ich rodzaj znajduje się raczej poza obrębem samej gałki ocznej i są to zazwyczaj tzw. cechy szczególne w postaci zmarszczek, bruzd, fałd skóry, znamion, blizn usytuowanych w okolicy oczodołu czy czoła. Taki rodzaj badań wykonywany jest rutynowo, np. w ramach identyfikacji osób na podstawie zdjęć, w tym uzyskanych z monitoringu wizyjnego. Zapewniają to m.in. obowiązujące normy i przepisy[7], w ramach których określone zostały bardzo szczegółowo wymogi techniczne stawiane przed elementami składowymi systemów CCTV przeznaczonych np. do zabezpieczenia imprez masowych i ochrony wartości pieniężnych. Parametry pracy tych urządzeń – głównie kamer – zapewniają uzyskanie takiej jakości obrazu, która umożliwia przeprowadzenie badań identyfikacyjnych utrwalonych wizerunków osób. Owe badania reprezentują dość obszerny rodzaj wykonywanych ekspertyz kryminalistycznych, w rezultacie których na bieżąco identyfikuje się sprawców wielu

[4] Evofit – system opracowany na Uniwersytecie Stirling w Szkocji.

[5] Antropometria (*sensu stricto*) – pomiary głowy i ciała oraz czaszki i szkieletu pozaczaszkowego.

[6] Antroposkopia – opis jakościowy głowy i ciała oraz czaszki i szkieletu pozaczaszkowego.

[7] Rozporządzenie MSWiA z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne (DzU Nr 166, poz. 1128) i rozporządzenie MSWiA z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej (DzU 2011 Nr 16, poz. 73), PN EN 50132-7:2013-04.

przestępstw o charakterze kryminalnym właśnie na podstawie wyglądu ich twarzy lub jej fragmentów, a także głównych elementów składowych, w tym np. nosa, ust czy małżowiny usznej. Rzadziej do podobnej identyfikacji dochodzi w przypadkach częściowego zasłonięcia twarzy, np. kominiarką, szalikiem bądź dużym kapturem. W okolicznościach starannego maskowania twarzy zarówno jej fotografia, jak i materiał wizyjny, uzyskany przez kamery monitoringu CCTV, zwykle nie obejmuje cech indywidualnych zarejestrowanego obrazu samej gałki ocznej, ale raczej wspomnianych już jej okolic i zestawu cech szczególnych usytuowanych w okolicach oczodołów i nasady nosa. Aby to osiągnąć, wystarczy dysponować rozdzielczością rzędu od ok. 80 pikseli przypadającą na szerokość identyfikowanej twarzy, to znaczy ok. 5 pix/cm. Według normy PN EN 50132-7:2013-04[8] pożądane parametry pracy kamery są możliwe do osiągnięcia jedynie w aplikacji „inspekcja"[9], która jednak jest niewystarczająca do identyfikacji człowieka na podstawie samej gałki ocznej.

Czyżby kryminalistyka oraz cała współczesna baza środków technicznych służących do utrwalania obrazu w sferze ochrony obiektów rzeczywiście była bezradna wobec przypadków dokładnego maskowania wyglądu twarzy?

Rozwiązaniem tego problemu, głównie w celu lepszej akwizycji cech, wydaje się możliwość wykorzystania dotychczasowych osiągnięć biometrii[10] w tworzeniu metod weryfikacji i identyfikacji ludzi w systemach kontroli dostępu (SKD). Jedną z istniejących metod, którą zapewne kryminalistyka w obecnej sytuacji byłaby zainteresowana, jest identyfikacja tęczówki oka na podstawie jej fizycznych cech biometrycznych. W przekonaniu autora warunkiem zapewnienia bezpieczeństwa i zrealizowania celów monitoringu wizyjnego, w tym uzyskania możliwości podjęcia czynności dowodowo-wykrywczych wobec osób dopuszczających się popełniania przestępstw, głównie w zamkniętej przestrzeni publicznej i ukrywających swoją tożsamość przez maskowanie i skrywanie rzeczywistego wyglądu, jest wykorzystanie adekwatnych do tych sytuacji środków technicznych i istniejących metod identyfikacji osób. Jeśli przedmiotem dalszych badań zmierzających do ustalenia tożsamości takich osób nie mogą być twarze

[8] PN EN 50132-7:2013-04 – wersja angielska, Systemy alarmowe, Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 7: Wytyczne stosowania.

[9] Inspekcja – rodzaj aplikacji, nazwany tak z angielskojęzycznej wersji oryginału normy od słowa *inspection* – to całkowicie nowa figura słowna w terminologii nazw używanych od niedawna w ochronie osób i mienia (w kryminalistyce dotąd nieznana), za którą, jak można domniemywać, kryje się najwyższy stopień możliwości identyfikacyjnych zarejestrowanego wizerunku osoby, przy co najmniej 400% skali wypełnienia ekranu obrazem postaci poddawanej identyfikacji; aplikacja ta została także uznana za wystarczającą dla dostarczania dowodów z monitoringu wizyjnego na potrzeby procesów sądowych.

[10] Metody biometryczne badają zarówno cechy fizyczne (np. tęczówka oka, siatkówka – dno oka, linie papilarne, układ naczyń krwionośnych w palcu lub na dłoni, kształt dłoni, kształt linii zgięcia wnętrza dłoni, kształt ucha, twarz, rozkład temperatur na twarzy, kształt i rozmieszczenie zębów, zapach, DNA itp.), jak i cechy behawioralne, tzn. związane z zachowaniem człowieka (np. sposób chodzenia, podpis odręczny, sposób pisania na klawiaturze komputera, głos).

czy nawet ich fragmenty z odsłoniętą szparą oczną, małżowiną uszną czy ustami, należałoby sięgnąć dalej, mianowicie po możliwość takiego rejestrowania obrazu tęczówki oka, by następnie móc go wykorzystać do badań identyfikacyjnych. Tym bardziej że od niedawna pojawiły się możliwości techniczne w tym zakresie, chociaż bardzo skomplikowane i wymagające dodatkowych nakładów finansowych, i ewentualne dążenia do zastosowania tej metody, jako pewnego rodzaju antidotum, wydają się uzasadnione, szczególnie wobec powszechnej opinii, iż bezpieczeństwo obywateli pozostaje w dzisiejszych czasach jedną z najważniejszych i najcenniejszych wartości.

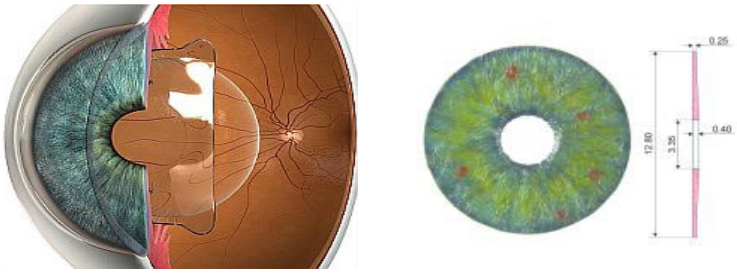
Badania tęczówki oka

Tęczówka oka to zabarwiona błona umiejscowiona za rogówką i przed soczewką. Jest okrągłego kształtu z otworem w środku – źrenicą, która działa podobnie jak przesłona aparatu fotograficznego. Głównym zadaniem tęczówki jest bowiem dozowanie ilości światła, które wpada do oka. Napięcie włókien mięśniowych sprawia, że źrenica zwęża się lub rozszerza, natomiast okazało się, że kolor tęczówki (traktowany przez wiele lat jako barwa oczu) zależy od ilości pigmentu (melaniny) na jej przedniej i tylnej powierzchni. Podstawą omawianej metody jest obserwacja, że struktura każdej tęczówki jest unikatowa, niepowtarzalna nawet u bliźniaków oraz w prawym i lewym oku tej samej osoby. Nie zmienia się ona także podczas całego życia człowieka[11], a jej uszkodzenia należą do niezwykle rzadkich przypadków. Cechy te sprawiają, że jest to jedna z najbardziej trwałych cech biometrycznych człowieka. Bogactwo form i zabarwień tęczówki sprawia również, że stanowi ona jedną z najbardziej dyskryminatywnych charakterystyk osobniczych o praktycznie zerowym prawdopodobieństwie powtórzenia się w identycznej postaci. Choć, jak wspomniano, tęczówka każdego człowieka ma małe rozmiary (o średnicy od 10 do 12 mm), odznacza się dużą liczbą cech indywidualnych – od 200 do aż 260, czyli kilkakrotnie większą, niż zwykle wyznacza się punktów charakterystycznych (np. minucji) na pojedynczej odbitce linii papilarnych palców. Warto przy tym zaznaczyć, że ekstrakcja cech indywidualnych, w tym także określenie ich wartości dowodowej[12], mającej wpływ na ogólną ocenę dalszej ich przydatności do badań identyfikacyjnych, możliwa jest wyłącznie przy użyciu metod automatycznego rozpoznania. Nie ma w niej bowiem miejsca dla biegłego, np. na przeprowadzenie dodatkowych badań lub ostateczną weryfikację decyzji systemu, jak dzieje się to w badaniach daktyloskopijnych poprzedzonych wskazaniami systemu AFIS[13] (Automated Fingerprint Identification System).

[11] Zespół naukowców z University of Notre Dame pod kierownictwem prof. inżynierii komputerowej Kevina Bowyera twierdzi jednak, że tęczówka oka jest wrażliwa na procesy starzenia się i nawet w przeciągu trzech lat może zmienić swoją strukturę do tego stopnia, że system biometryczny nie jest w stanie jej poprawnie zidentyfikować, co powoduje, iż z czasem systemy do jej rozpoznawania będą w przypadku tej samej, skanowanej przez czytnik osoby generować coraz więcej błędów.

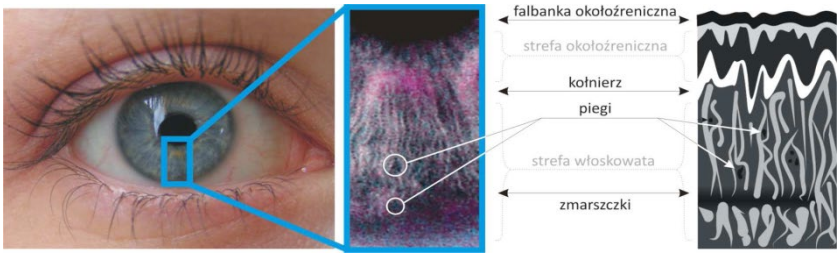
[12] Wartość dowodowa to określenie, w jakim stopniu ustalenia dokonane przy użyciu danej metody służą udowodnieniu popełnienia przestępstwa w konkretnej sprawie.

[13] AFIS – system automatycznej identyfikacji daktyloskopijnej.



Ryc. 1. Obraz tarczki tęczówki oka i jej usytuowanie w gałce ocznej

Źródło: www.biometriclabs.pl.



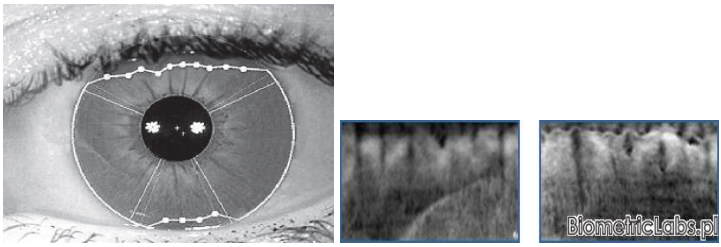
Ryc. 2. Struktura wewnętrzna tęczówki oka oraz strefy usytuowania jej cech charakterystycznych

Źródło: www.biometriclabs.pl.

Wobec złożoności i pełnej automatyzacji poszczególnych etapów tego rodzaju identyfikacji biometrycznej warto przybliżyć chociaż najważniejsze z nich. Bazą dla większości istniejących metod rozpoznawania tęczówki jest algorytm opracowany przez J. Daugmana[14]. Podstawowymi cechami charakterystycznymi tej metody są: silnie rozbudowany deskryptor tęczówki, nazywany również kodem tęczówki (*iris code*), oraz statystyczny charakter podejmowania decyzji. Wspomniany deskryptor stanowi wektor 2048 binarnych elementów, pozwalających na poprawne odzwierciedlenie nawet bardzo złożonych form zawartych w danych wejściowych w postaci poplątanej siateczki tkanki łącznej oraz innych, dostrzegalnych także przez człowieka elementów, takich jak: bruzdy, dołki, prążkowanie, włókna kolagenowe, zacienione pola (tzw. krypty), plamki, pierścienie. Stanowią one kod wydzielonego obrazu oka odpowiadającego wyłącznie obszarowi położenia tęczówki, czyli pierścienia obejmującego od zewnątrz źrenicę i otoczonego rogówką oraz powiekami. Ponadto obszar tęczówki, który podlega dalszemu przetwarzaniu, zostaje zawężony do zbioru ośmiu współśrodkowych wycinków pierścieni o jednakowej szerokości. Zatem treść obrazu

[14] K. Ślot, *Wybrane zagadnienia biometrii*, Wydawnictwa Komunikacji i Łączności, Warszawa 2008.

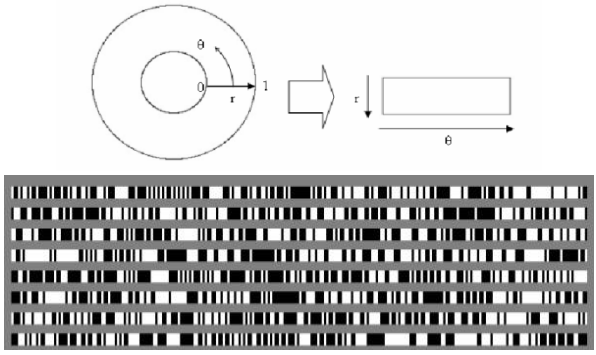
zawarta w tych ośmiu pasach obszaru tęczówki zostaje odwzorowana na współrzędne biegunowe, co staje się podstawą do automatycznego wyznaczenia kodu tęczówki.



Ryc. 3. Typowy obraz tęczówki wraz z automatycznie zlokalizowanymi zakłóceniami

Źródło: http://www.pwpw.pl/kwartalnik_archiwum.html?id=30&magCid=118.

Dalsze czynności to już porównanie kodu tęczówki, wyznaczonego dla aktualnie analizowanego obrazu oka, z kodami znajdującymi się w przygotowanej wcześniej bazie danych. Ważnym wyróżnikiem technologii rozpoznawania tęczówki jest także możliwość pełnego przeszukania takiej bazy danych, bez żadnych ograniczeń liczby zawartych w niej rekordów. Natomiast miarą podobieństwa dwóch automatycznie porównywanych ze sobą kodów tęczówki jest liczba różnic, występujących między odpowiadającymi sobie bitami porównywanych wektorów.



Ryc. 4. Graficzny obraz algorytmu J. Daugmana i kod tęczówki

Źródło: http://sequoia.ict.pwr.wroc.pl/~witold/aiarr/2009_projekty/teczowki3/.

Instytucje prawne zaczęły wykorzystywać tę metodę od 1994 r., kiedy to więzienie w hrabstwie Lancaster w Pensylwanii jako pierwsze zaopatrzyło się w system identyfikacji więźniów oparty na rozpoznawaniu wzoru tęczówki. Z kolei w hrabstwie Berkshire podobny system używany był do identyfikacji pracowników więzienia. Międzynarodowe lotnisko Charlotte/Douglas w Karolinie Północnej oraz lotnisko we Frankfurcie

w Niemczech pozwalają osobom, które często podróżują, zarejestrować swoje wzory tęczówek, ułatwiając w ten sposób wszelkie procedury związane z wejściem na pokład samolotu. Obecnie skuteczność systemów biometrycznych mierzy się dwoma parametrami: FAR[15] i FRR[16]. Im niższe są ich wartości procentowe, tym system jest odpowiednio bezpieczniejszy i bardziej użyteczny. Wartość obu tych wskaźników dla tęczówki oka[17] wynosi 0,0005% (dla porównania: w przypadku linii papilarnych FAR wynosi 0,2000%, a FRR 0,0100%). Powyższe ustalenia tłumaczą pojawienie się również planów częstszego niż dotychczas zastosowania skanera tęczówki w dziedzinie transakcji bankowych, w zakresie kontroli granicznej oraz porządku publicznego. To duże zainteresowanie biometrią tęczówki oka w ostatnim czasie wynika też z wysokiego poziomu bezpieczeństwa i niezawodności jej stosowania. Walory te okazały się decydujące również dla wykorzystania tej metody wraz z czytnikami odbitek palców w procedurach identyfikacji osób, które są już stopniowo wdrażane do codziennej praktyki w wielu krajach na całym świecie. Pierwszym krajem i aktualnie najbardziej zaangażowanym technologicznie w tworzenie kolejnych wersji takich systemów są Stany Zjednoczone Ameryki, w tym Departament Obrony (DoD) USA. Został tam stworzony pionierski, wielomodułowy system do walki z terroryzmem w celu umożliwienia pełnej identyfikacji osób na podstawie ich cech biometrycznych. Nazywa się on DoD ABIS[18] i bazuje na trzech rodzajach danych biometrycznych człowieka: liniach papilarnych palców i dłoni, cechach twarzy i tęczówce oka, oraz obejmuje swym zasięgiem głównie środowiska spoza USA podejrzewane o działalność terrorystyczną. System ten umożliwia członkom sił zbrojnych USA na terenach poszczególnych obszarów ich aktywności militarnej szybką identyfikację osób uznanych za zagrożenie dla zachowania bezpieczeństwa narodowego Stanów Zjednoczonych, a także w przypadku pojawienia się ich na terenie USA pod zmienionymi nazwiskami i dysponujących pakietem często fałszywych dokumentów, mających uwierzytelnić ich nową tożsamość. Dodatkowo system ten jest kompatybilny z innymi elementami bezpieczeństwa narodowego, takimi jak zintegrowany system identyfikacji daktyloskopijnej IAFIS (ang. Integrated Automated Fingerprint Identification System) używany przez FBI, i może być dostępny z każdego zakątka świata przez całą dobę. W uzasadnionych przypadkach korzystają z niego także inne instytucje tego

[15] FAR (ang. False Acceptance Rate) – wskaźnik fałszywej akceptacji, określa bezpieczeństwo systemu, wyrażone prawdopodobieństwem zakwalifikowania danej próbki jako tożsamej z wzorcem, mimo iż nie mu odpowiada, np. w systemach kontroli dostępu, gdy wskaźnik FAR wynosi 0,0005%, oznacza on prawdopodobieństwo błędnego uwierzytelnienia (weryfikacji, identyfikacji) 5 nieuprawnionych osób na 1 mln osób poddanych takiej próbie przez dostarczenie ich określonej biometryki.

[16] FRR (ang. False Rejection Rate) – wskaźnik fałszywego odrzucenia, określający użyteczność systemu, wyrażoną prawdopodobieństwem niezakwalifikowania danej próbki, która jest tożsama z wzorcem, i ostateczne odrzucenie jej, mimo iż odpowiada ona wzorcowi.

[17] M. Szczepanik, I. Jóźwiak, *Metody wykrywania człowieczeństwa w systemach biometrycznych*, „Zeszyty Naukowe Politechniki Śląskiej" 2014, z. 68 (1905), seria: Organizacja i Zarządzanie.

[18] ABIS – automatyczny system identyfikacji biometrycznej (ang. Automated Biometrics Identification System).

kraju reprezentujące państwowe i lokalne organy ścigania. Przedstawiony przykład funkcjonującego systemu zapewne także na potrzeby kryminalistyki potwierdza zasadność podejmowanych i u nas w kraju naukowych inicjatyw w podobnym zakresie.

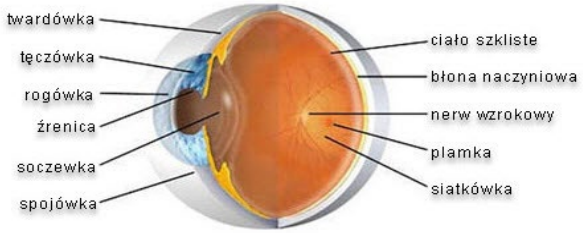
Moc argumentów za stosowaniem omawianej tu metody biometrycznej stawia ją co najmniej na równi z metodą identyfikacji daktyloskopijnej na podstawie odbitek palców. Natomiast do istotnych jej wad należy nadal duży koszt skanerów (kamer) oraz ciągle jeszcze wymuszona, statyczna poza pojedynczych osób, które poddawane są skanowaniu tęczówki oka, a także stosunkowo duża wymagana rozdzielczość obrazu samej tęczówki. Warto zaznaczyć, że w większości stosowanych systemów wynosi ona od 100 do 140 pikseli przypadających na promień tęczówki. Z zapowiedzi przedstawicieli polskiej nauki[19] wynika jednak, że niedogodności te w niedalekiej przyszłości (w ciągu trzech lat) mają być usunięte m.in. za sprawą stworzenia systemu, który będzie umożliwiał identyfikację ludzi poruszających się w niedużych skupiskach. System w założeniu ma radzić sobie z kilkoma osobami (3–4) jednocześnie, np. przechodzącymi przez bramki wejść na stadiony lub do biurowców. Identyfikacja ta opierać się będzie na wynikach automatycznej analizy cech biometrycznych różnych części i elementów ciała ludzkiego równocześnie oraz struktury pokrywającej je skóry, tj. obrazu twarzy, obrazu tęczówki oka czy małżowiny usznej, utrwalonych na seriach zdjęć wykonanych przez kamery przechodzącym osobom. Spotykane więc coraz częściej przypadki różnych sposobów maskowania twarzy, stosowanych głównie przez sprawców zakłóceń porządku publicznego oraz napadów rabunkowych (w tym z bronią lub niebezpiecznym narzędziem w ręku), pewnie za sprawą wprowadzenia do ochrony obiektów podobnych technologii doczekają się także skutecznej i przekonującej metody ich zwalczania. Warto też podkreślić, że tęczówka oka stanowi biometrykę, która w odróżnieniu np. od linii papilarnych może być wykorzystywana w celach identyfikacyjnych jedynie w odniesieniu do osób żywych. Od momentu śmierci człowieka ulega ona szybkiej degradacji (zaledwie w ciągu 5 sekund) wraz z postępującym procesem mętnienia rogówki w początkowym okresie, a następnie dochodzi do jej całkowitego zniszczenia wraz z postępującym rozkładem gałki ocznej. Nim to jednak nastąpi, do 20 godzin po śmierci można zbadać reakcję źrenic na środki farmakologiczne oraz pośmiertną pobudliwość elektryczną tęczówki[20]. Są to jednak dodatkowe jej funkcje, jakie może spełniać dla wyjaśnienia istotnych okoliczności śmierci człowieka. Ponadto dzięki analizie płynu z ciała szklistego[21] gałki ocznej można również ustalić czas zgonu, lecz w odleglejszej nieco perspektywie

[19] Naukowcy z Politechniki Łódzkiej pod kierownictwem dr. inż. Kamila Grabowskiego pracują nad specjalnymi bramkami, które szybko rozpoznają tożsamość przechodzących przez nie osób. System ten będzie sprawdzał tożsamość na podstawie serii fotografii wykonanych przez kamery zainstalowane na bramce. Na tej podstawie komputer przeanalizuje różne cechy biometryczne – obraz twarzy, tęczówki oka czy małżowiny usznej.

[20] B. Sygit, *Dorobek nauki w badaniach nad ustrojem człowieka wykorzystywany w praktyce śledczej i sądowo-lekarskiej*, „Problemy Współczesnej Kryminalistyki" 2003, t. VII, część druga.

[21] Ciało szkliste składa się z przejrzystej, galaretowatej substancji, która wypełnia całą, dość dużą jamę między tylną stroną soczewki a siatkówką. Spełnia głównie funkcję mechaniczną,

minionego czasu, do 120 godzin po śmierci, na podstawie stężenia w nim potasu, a także przyczynę śmierci, spowodowanej np. zatruciem narkotykami.



Ryc. 5. Budowa gałki ocznej

Źródło: https://sites.google.com/site/zmysly123/link4.

Doszukując się jeszcze innych znaczeń kryminalistycznych w stanie gałek ocznych denata, można również w pewnych specyficznych okolicznościach pokusić się o ustalenie np. *modus operandi* sprawcy, które wynika z pewnych przesądów i często przyjmuje formę bardzo charakterystycznych uszkodzeń. Poza przypadkami, gdy same gałki oczne stają się przedmiotem przestępstwa, bywa, że po popełnieniu czynu głównego są zakrywane lub atakowane przez sprawców, np. przestrzeliwane, wydłubywane, a następnie czasem nawet konsumowane[22] lub ukrywane w pobliżu miejsca zdarzenia, bądź nacinane żyletką. Zabiegi te według przedstawicieli świata przestępczego dokonywane są, aby zatrzeć ostatni obraz ofiary i udaremnić rozpoznanie sprawcy, a czasem są też wyrazem ucieczki sprawcy przed błagalnymi spojrzeniami swych ofiar proszących o darowanie życia. Taki sposób postępowania i korzystania z podobnych – powtarzalnych wzorców zachowań sprawców względem swoich ofiar, a także rodzaju użytych narzędzi, czyni ich w pewien sposób wyróżnialnymi w sferze danego rodzaju czynów przestępnych.

Zakończenie

Celem niniejszego opracowania jest przedstawienie aktualnych możliwości identyfikacyjnych, jakie dają ludzkie oczy, a także zwiększenie zainteresowania kryminalistyków innymi metodami identyfikacji ludzi, które stały się możliwe dzięki rozwojowi technologii wykorzystywanych np. w biometrii. W aktualnej sytuacji, w obliczu coraz częstszych przypadków maskowania twarzy przez sprawców, konieczne wydaje się poszerzenie bazy środków technicznych i systemowych, jakimi obecnie dysponuje kryminalistyka, o rozwiązania współcześnie już funkcjonujące, np. w systemach zabezpieczeń obiektów, ale również i te, które są jeszcze w fazie

utrzymując przyleganie siatkówki do nabłonka barwnikowego; jego funkcja optyczna w odróżnieniu od funkcji kryminalistycznej jest mało znacząca.

[22] Akt opisany jako „Hannibal Lecter", którego w ostatnim czasie dopuścił się Matthew Williams względem swojej ofiary, konsumując jedną z jej gałek ocznych i część twarzy.

studium laboratoryjnego, wszystkie z nich bowiem odpowiadają na społeczne oczekiwania w świecie rosnących zagrożeń i walki z przestępczością.

Streszczenie

Niniejszy artykuł ma na celu zapoznanie czytelników z jedną z technologii biometrycznych – rozpoznawaniem tęczówki oka, o którą w przyszłości mogą być uzupełnione metody automatycznej identyfikacji osób wykorzystywane w kryminalistyce. Metodyka analizy tęczówki oka człowieka została pierwotnie opracowana na potrzeby systemów kontroli dostępu. Teraz, po rozwiązaniu wielu problemów technicznych, trwają prace nad wdrożeniem jej także do wielu różnych obszarów działalności człowieka związanych z bezpieczeństwem, gdzie naukowcy poszukują niezawodnego sposobu ustalania tożsamości osób na podstawie ich cech fizycznych, i gdzie standardem jest zerowa stopa tolerancji błędu. Niniejsze opracowanie jest streszczeniem współczesnej wiedzy na temat teoretycznych możliwości wykorzystania wspomnianej biometryki także w kryminalistyce z podaniem przykładów praktycznego zastosowania tej technologii, w innych krajach używanej w sektorze bezpieczeństwa i automatycznych systemach identyfikacji biometrycznej. Na zakończenie warto podkreślić fakt, że dotychczasowe wyniki i doświadczenia w wykorzystaniu tęczówki oka do uwierzytelniania wybranych danych biometrycznych człowieka stawiają ją na czele dostępnych metod identyfikacyjnych, obok badań DNA i linii papilarnych palców.

Słowa kluczowe: biometria, technologie biometryczne do uwierzytelniania tożsamości osób, rozpoznawanie tęczówki oka, kod tęczówki

Summary

This article aims at familiarizing the readers with one of the biometric technologies – iris recognition of the human eye, which may be used in future to develop automatic identification methods used in forensic science. Concept of iris of the eye was originally developed for access control systems. At present, after solving a lot of technical problems, research work are continued to put this technology into many different areas of people activities connected with security, where scientists are looking for reliable way to identify people by unique physical features, and where the standard is a zero error rate. This publication is a summary of knowledge about the theoretical possibility of using this biometric method in the Polish forensic science with examples of practical use of this technology, in another countries used for security, and as automated biometric identification systems. In conclusion worth to emphasize fact, that current results and experiences in the use of iris of the human eye put this biometric technology to authenticate identity at the forefront of the available methods for use in identification or verification modes, in addition to DNA testing, and fingerprints.

Keywords: biometrics, biometric technologies to authenticate person's identity, iris recognition technology, iris code

SPRAWOZDANIA

Katarzyna Julia Furman

SPRAWOZDANIE Z III MIĘDZYNARODOWEJ KONFERENCJI NAUKOWEJ „MIEJSCE ZDARZENIA"

III Międzynarodowa Konferencja naukowa poświęcona czynnościom kryminalistycznym na miejscu zdarzenia odbyła się w dniach 18 i 19 marca 2015 r. podczas XVII Międzynarodowych Targów Analityki i Technik Pomiarowych EuroLab oraz IV Międzynarodowych Targów Techniki Kryminalistycznej CrimeLab. Organizatorami Konferencji było Centralne Laboratorium Kryminalistyczne Policji oraz Polskie Towarzystwo Kryminalistyczne.

Trzecie spotkanie z tego cyklu w znacznej części poświęcone było omówieniu zagadnień związanych z wchodzącą w lipcu br. nowelizacją Kodeksu postępowania karnego w kontekście zmian w procesie dowodowym. Niewątpliwie trafnie dobrana tematyka stanowiła odzew na zapotrzebowanie środowiska przygotowującego się na zmiany w procedurze karnej.

Tematowi przewodniemu podporządkowany był program konferencji – w pierwszym dniu skupiono się na zagadnieniach roli technika kryminalistyki, w drugim zaś na plan pierwszy wysunął się temat roli biegłego oraz organów procesowych.

Jak podkreślali sami organizatorzy: „przedsięwzięcie jest skierowane do przedstawicieli sądownictwa i prokuratury, teoretyków i praktyków kryminalistyki, naukowców, kadry kierowniczej Policji, techników kryminalistyki, studentów prawa oraz szkół policyjnych, a także przedstawicieli biznesu z kraju i ze świata[1]".

Międzynarodowy charakter konferencji podkreślały nie tylko osoby samych prelegentów (m.in. Jeremy Smith – Humberside Police, Fernando Viegas – Policia Judiciara, Professor Chi Chung Yu – Department of Forensic Science, College of Criminal Justice, Sam Houston State University, Maria Kambosos – Forensic Science Institute of BKA – Instytut Kryminalistyki Krajowego Urzędu Kryminalnego, Professor Peter Bilous – Washington University), ale również szerokie ujęcie prezentowanych tematów.

Interesujący i uzasadniony był dobór tematyki poszczególnych sesji oraz wystąpień prelegentów w ramach sesji – ukazujący zarówno praktyczne, jak i teoretyczne aspekty nauki kryminalistyki i procesu karnego.

[1] http://www.miejscezdarzenia.edu.pl/index.php/pl/.

Poszczególne sesje poświęcone były: zmianom w podejściu do badań kryminalistycznych wynikających z nowelizacji Kodeksu postępowania karnego, zabezpieczaniu dowodów na miejscu zdarzenia i roli technika kryminalistyki w tym procesie, pokazowi oględzin miejsca zdarzenia, zasadom działania techników kryminalistyki w polskim i brytyjskim systemie prawnym, jak również roli biegłego w kontradyktoryjnym procesie karnym i sędziowskiej ocenie opinii biegłego. Taki zakres tematyczny sprawił, iż treść wystąpień znajdowała się w zainteresowaniu wszystkich adresatów konferencji.

W roli moderatorów wystąpili przedstawiciele świata nauki i praktyki kryminalistycznej.

Praktycy i teoretycy mieli możliwość poznania najnowszych technik, które mogą być wykorzystywane w czynnościach na miejscu zdarzenia. Duży nacisk położony został podczas wystąpień prelegentów na zagadnienie jakości pracy oraz doskonalenia zawodowego techników kryminalistyki, jak również w aspekcie międzynarodowym poruszono zagadnienie akredytacji czynności podejmowanych podczas oględzin miejsca zdarzenia w Europie.

Wszystkie sesje cieszyły się dużym zainteresowaniem, zaś udział w konferencji ułatwiało usytuowanie miejsca jej odbywania bezpośrednio na poziomie targów, którym towarzyszyła. Dyskusje stanowiły dobre forum wymiany doświadczeń i wątpliwości związanych z codzienną pracą osób związanych z kryminalistyką.

Partnerami konferencji byli: GE Healthcare (partner strategiczny), ThermoFisher Scientific, PerkinElmer, EC TestSystems, zaś patronat medialny nad wydarzeniem objęło czasopismo: „Policja 997" oraz dwumiesięcznik „LAB (Laboratoria Aparatura Badania)".

Cieszy fakt, iż udało się stworzyć cykliczne wydarzenie na tak wysokim poziomie naukowym i merytorycznym, które integruje środowisko.

Opracowała:
dr Katarzyna Julia Furman
Członek Zarządu Warszawskiego Oddziału Polskiego Towarzystwa Kryminalistycznego

Mieczysław Goc, Katarzyna Julia Furman

KOMUNIKAT Z OBRAD VI SYMPOZJUM KRYMINALISTYCZNEGO POLSKIEGO TOWARZYSTWA KRYMINALISTYCZNEGO

W dniach 24–26 czerwca 2015 r. w Toruniu gościli uczestnicy Międzynarodowej Konferencji Naukowej – VI Sympozjum Kryminalistycznego Polskiego Towarzystwa Kryminalistycznego pt. ***Kryminalistyka – jedność nauki i praktyki***. Obrady odbywały się w Hotelu Copernicus.

Organizatorami tego międzynarodowego wydarzenia naukowego, adresowanego zarówno do przedstawicieli nauki, jak i praktyki kryminalistyki i procesu karnego, byli: Polskie Towarzystwo Kryminalistyczne, Wydział Prawa i Administracji Uniwersytetu Warszawskiego, Wydział Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, Centralne Laboratorium Kryminalistyczne Policji oraz Polska Wytwórnia Papierów Wartościowych.

Konferencje PTK należą do największych tego rodzaju krajowych przedsięwzięć kryminalistycznych, gromadzących zwykle kilkuset uczestników, spośród pracowników naukowych uniwersyteckich katedr kryminalistyki i szkół policyjnych, ekspertów laboratoriów kryminalistycznych, pracowników i funkcjonariuszy policji, ABW i innych służb, prokuratorów, sędziów oraz wszystkich tych, dla których kryminalistyka stanowi teoretyczną podbudowę zawodu.

Konferencje te noszą tradycyjną nazwę: „Sympozja Kryminalistyczne", nawiązującą do pierwszej konferencji zorganizowanej w 1978 r. w Krakowie przy współudziale Instytutu Ekspertyz Sądowych im. prof. dra Jana Sehna. Po wieloletniej przerwie Polskie Towarzystwo Kryminalistyczne, wychodząc naprzeciw postulatom środowiska, postanowiło reaktywować ideę ogólnopolskich konferencji kryminalistycznych i w 1999 r. zorganizowało w Bystrej Śląskiej konferencję pn. ***II Sympozjum Kryminalistyczne – Kryminalistyka na przełomie wieków***. W następnych latach odbyły się kolejne konferencje z tego cyklu. Ostatnia, pn. ***V Sympozjum Kryminalistyczne – Kryminalistyka – mity a rzeczywistość***, odbyła się w dniach 28–30 maja 2009 r. w Ciechocinku.

Hasłem wiodącym obecnej VI Konferencji było ***Kryminalistyka – jedność nauki i praktyki***. Oddawało ono trafnie problematykę, która była przedmiotem obrad.

Program konferencji obejmował pięć sesji tematycznych:

Sesja I: Aktualne kierunki i metody badań kryminalistycznych.

Sesja II: Biegły w procesie sądowym – przewodniczący.

Sesja III: Dowody naukowe a kryminalistyka.

Sesja IV: Kryminalistyka w ramach nowego modelu procesu karnego.

Sesja V: Kryminalistyczna problematyka współczesnej przestępczości.

Organizatorzy przewidzieli również sesję plakatową, która była okazją do zaprezentowania zagadnień w formie zwięzłych prezentacji, wykresów oraz zdjęć.

Wykład inauguracyjny zatytułowany: *Tendencje w rozwoju kryminalistyki – tworzenie modelu „narodowego" czy współtworzenie europejskiej przestrzeni kryminalistycznej?* wygłosił prof. Henryk Malewski, reprezentujący Litewskie Towarzystwo Kryminalistyczne.

Wszystkie przedstawione referaty były starannie dobrane. W swych wystąpieniach prelegenci umiejętnie łączyli zagadnienia naukowe z praktycznymi, dzięki czemu były one niezwykle interesujące i istotne z punktu widzenia odbiorcy. Wiele uwagi poświęcono konsekwencjom zmian procedury karnej, które weszły w życie w lipcu tego roku (prof. dr hab. Jan Widacki, prof. dr hab. Bogusław Sygit, dr Damian Wąsik, mgr Marta Janocha, dr hab. prof. nadzw. Anna Koziczak), jak również sytuacji biegłych (dr Magdalena Tomaszewska-Michalak), a zwłaszcza dylematom ustawy o biegłych, która od lat nie może się doczekać uchwalenia (prof. dr hab. Ewa Gruza, prof. dr hab. Tadeusz Tomaszewski, prof. dr hab. Piotr Girdwoyń).

Najobszerniejszy panel tematyczny wypełniły referaty poświęcone problematyce nowych technik i metod badawczych w ekspertyzie kryminalistycznej. Mówiono m.in. o nowatorskich metodach klasycznych i technicznych badań dokumentów (prof. dr hab. Tadeusz Widła, mgr Krzysztof Przybysz, mgr Ewelina Jakielaszek) oraz nowych rodzajach zapisów, w tym e-pisma i podpisów biometrycznych (mgr Andrzej Łuszczuk, dr Mieczysław Goc, dr Tomasz Dziedzic), o problematyce badań komputerowych (mgr Bartosz A. Adamus), badań chemicznych (dr Marcin Gawryś), wykorzystania skaningowej mikroskopii elektronowej (dr Anna Łasińska), badań fonoskopijnych (dr Rafał Korycki), poligraficznych (dr hab. prof. nadzw. Ryszard Jaworski), badań mikrośladów (dr hab. prof. IES Jolanta Wąs-Gubała). Wskazywano na trudności i problemy związane z prawidłową i skuteczną realizacją działań procesowych i operacyjnych (prof. nadzw. dr hab. Adam Taracha), w tym związanych ze zwalczaniem zorganizowanej przestępczości gospodarczej (dr Piotr Herbowski), opiniowaniem w sprawach wypadków komunikacyjnych (dr Małgorzata Żołna) oraz użycia broni palnej (mgr Daniel Mańkowski), czy też rolą antropologa sądowego w postępowaniu karnym (mgr Andrzej Czubak).

Sporo miejsca podczas konferencji poświęcono także problematyce dowodów naukowych w kryminalistyce, odnosząc się do tych zagadnień zarówno z punktu widzenia teorii nauki (prof. dr hab. Jerzy Kasprzak, dr hab. prof. UWM

Jarosław Moszczyński), jak i kazuistyki (prof. dr hab. Józef Wójcikiewicz, dr hab. prof. UMK Violetta Kwiatkowska-Wójcikiewicz).

Prócz przedstawicieli polskiej nauki i praktyki mogliśmy również wysłuchać gości zagranicznych, m.in. z Litwy, Słowacji, Wielkiej Brytanii oraz Stanów Zjednoczonych.

Zagraniczni goście mówili o problematyce biegłych-ekspertów w swoich krajach („Problems of selection, evaluation, certification of persons intending to become registered forensic experts in Lithuania" – doc. dr Gabrielė Juodkaitė-Granskienė) i systemie badań kryminalistycznych („System badań kryminalistycznych w policji litewskiej: tradycje oraz aktualia" – Genrikas Nedveckis, naczelnik Centrum Badań Kryminalistycznych Policji Litewskiej), kontradyktoryjności w amerykańskim procesie karnym („Fixing problems in the adversarial judicial system in the USA", prof. Peter Bilous, dyrektor Forensic Science Program Department of Chemistry & Biochemistry), możliwej współpracy państw w zakresie kryminalistyki („Forensic science in an adversarial criminal justice system: are recent legal and organisational developments in England and Wales relevant to Poland or international criminal justice cooperation between our countries?" – prof. Tim Wilson, dr Chris Wood, Northumbria University), a także o problematyce ekspertyz narkotykowych („Investigation of emerging drug related deaths and automobile crashes using forensic science methods" – dr Michael F. Rieders, Forensic Toxicologist and Lab Director NMS Labs).

Ważnym wydarzeniem konferencji była sesja okolicznościowa, podczas której podpisano umowę o współpracy pomiędzy Litewskim Towarzystwem Kryminalistycznym a Polskim Towarzystwem Kryminalistycznym. Sesję tę wieńczył wykład gościa specjalnego konferencji, prof. Henry'ego Lee – światowej sławy amerykańskiego kryminalistyka, eksperta m.in. w sprawie O.J. Simpsona, śledztwie po zamachu na World Trade Center, sprawie waszyngtońskiego snajpera, a także w badaniu okoliczności zamachu na prezydenta Stanów Zjednoczonych Johna Kennedy'ego. Profesor Henry Lee jest również wykładowcą akademickim (University of New Haven oraz East China University of Political Science and Law), a także prowadzi centrum badawcze – Henry C. Lee Institute of Forensic Science.

Konferencja cieszyła się ogromnym zainteresowaniem środowiska naukowego oraz przedstawicieli praktyki kryminalistycznej. Uczestniczyło w niej ponad 180 osób. Ze względu na ograniczone ramy czasowe spośród nadesłanych 60 referatów do wygłoszenia wybrano te, które były najbardziej reprezentatywne dla problematyki poszczególnych sesji tematycznych. Wszystkie zgłoszone referaty, po nadesłaniu pełnych tekstów i uzyskaniu pozytywnych recenzji, zostaną opublikowane w materiałach pokonferencyjnych. Streszczenia referatów oraz abstrakty plakatów opublikowano w materiałach konferencyjnych. Konferencja była okazją do poznania nie tylko polskich, ale również ważnych światowych zagadnień i osiągnięć kryminalistyki.

Patronat honorowy nad konferencją objął Komendant Główny Policji, patronat medialny miesięcznik „Policja 997", wydawany przez Komendę Główną Policji, oraz kwartalnik „Człowiek i Dokumenty", wydawany przez Polską Wytwórnię Papierów Wartościowych, a partnerem strategicznym była firma SHIM-POL.

Opracowali:
dr Mieczysław Goc, dr Katarzyna Julia Furman
Polskie Towarzystwo Kryminalistyczne

Henryk Malewski

XI MIĘDZYNARODOWA KONFERENCJA NAUKOWO-PRAKTYCZNA „KRYMINALISTYKA I EKSPERTOLOGIA[1] SĄDOWA: NAUKA, STUDIA, PRAKTYKA", WILNO, 25–27 CZERWCA 2015 R.

Od roku 1999 kryminalistycy na Litwie organizują tradycyjną międzynarodową konferencję naukowo-praktyczną pod tytułem „Kryminalistyka i ekspertyza sądowa: nauka, studia, praktyka". Konferencje te miały być platformą do dyskusji i wymiany doświadczeń pomiędzy przedstawicielami nauki kryminalistycznej i środowiskami zawodów prawniczych, organów ścigania oraz wymiaru sprawiedliwości na Litwie. Szczególne miejsce na tym forum przewidziano dla kryminalistyki akademickiej. Już od pierwszej konferencji ten dyskurs został przeniesiony na poziom międzynarodowy w ramach dążenia do integracji środowisk kryminalistycznych krajów europejskich[2]. Od pierwszych konferencji wśród uczestników zagranicznych zawsze była pokaźna grupa znanych kryminalistyków polskich. Wśród nich można wymienić prof. Zdzisława Kegla, prof. Tadeusza Tomaszewskiego, prof. Huberta Kołeckiego, którzy wielokrotnie uczestniczyli w tych spotkaniach, oraz wielu innych kryminalistyków polskich z podstawowych ośrodków akademickich, a także laboratoriów kryminalistycznych. Retrospektywa tych konferencji została przedstawiona w informacji dr Grażyny Kędzierskiej w pierwszym numerze czasopisma „Zagadnienia Społeczne" oraz w czasopiśmie „Law and Forensic Science"[3]. Informacje na ten temat były zamieszczane też w czasopismach rosyjskich[4],

[1] Ekspertologia sądowa (forensic Expertology – ang.; gerichtliche Expertology – niem.; судебная экспертология – ros.) – formująca się dyscyplina naukowa o ekspertyzie sądowej, wiadomościach specjalnych oraz o podmiotach je stosujących w postępowaniu przygotowawczym i procedurach sądowych.

[2] H. Malewski, *10 Międzynarodowa konferencja naukowa: Kryminalistyka i ekspertyza sądowa: nauka, studia, praktyka*, „Zagadnienia Społeczne" 2014, nr 2(2), s. 253–262.

[3] Zob. G. Kędzierska, *IX międzynarodowa konferencja: Kryminalistyka i ekspertyza sądowa: nauka, studia, praktyka*, „Zagadnienia Społeczne" 2014, nr 1(1), s. 247–252; H. Malewski, *International Scientific-Practical Conference "Criminalistics and Forensic Examination Science, Studies, Practice"*, „Law and Forensic Science" (w druku).

[4] Г. Малевски, *IX Международная научно-практическая конференция «Криминалистика и судебная экспертиза: наука, обучение, практика»* (г. Вильнюс, Литва, 21–22 июня 2013 г.). Пресс-релиз. // „Эксперт-криминалист" 2013, № 3, s. 28–29.

ukraińskich[5], a nawet włoskich[6].

Zarząd Litewskiego Towarzystwa Kryminalistycznego w 2014 r. postanowił wprowadzić zmianę w tytule konferencji i zamiast „ekspertyzy" pojawiło się słowo „ekspertologia". We wschodnioeuropejskiej szkole kryminalistyki pojęcie to oznacza nową dyscyplinę naukową poświęconą ekspertyzie sądowej. Tym samym podkreśla się nie tylko znaczenie ekspertyzy sądowej, ale też jej naukowy charakter.

XI międzynarodowa konferencja „Kryminalistyka i ekspertologia sądowa: nauka, studia, praktyka" odbyła się w dniach 25–27 czerwca 2015 r. w Wilnie na Uniwersytecie im. Michała Romera. Organizatorami konferencji byli: Litewskie Towarzystwo Kryminalistyczne, Centrum Ekspertyzy Sądowej Ministerstwa Sprawiedliwości Republiki Litewskiej i Uniwersytet im. Michała Romera. W konferencji uczestniczyło ponad 60 osób z Polski, Litwy, Łotwy, Estonii, Ukrainy, Czech, Słowacji, Słowenii, Węgier, Rosji. Z różnych względów nie dojechali przedstawiciele Włoch i Kazachstanu, chociaż ich publikacje są zawarte w przygotowanej przed konferencją książce. W obradach brało udział niemało osób, których publikacje są zawarte we wspomnianej książce (np. prof. dr Václav Krajník ze Słowacji) czy też takie jak prof. dr hab. Jarosław Berent z Polski, którzy nie zgłosili referatów.

Jak zawsze przed konferencją został wydany tom artykułów naukowych, które były rozszerzoną wersją większości wygłoszonych podczas niej referatów. W tomie[7] zamieszczono 31 artykułów naukowych, dwa artykuły biograficzne o członkach honorowych Litewskiego Towarzystwa Kryminalistycznego[8] oraz 7 streszczeń referatów, które autorzy pragnęli opublikować w jednym z czasopism wciągniętych do bazy danych *Scopus*. Tradycyjnie teksty były publikowane w językach litewskim, angielskim, rosyjskim i polskim.

Równolegle z konferencją w Wilnie w dniach 24–26 czerwca 2015 r. w Toruniu odbyło się VI Sympozjum Kryminalistyczne PTK „Kryminalistyka – jedność nauki i praktyki". W pierwszym dniu tej konferencji została podpisana umowa o współpracy Polskiego Towarzystwa Kryminalistycznego i Litewskiego Towarzystwa Kryminalistycznego. Ma ona między innymi pozwolić w przyszłości na unikanie kolizji terminów organizowanych „bratnich" konferencji.

XI międzynarodowa konferencja „Kryminalistyka i ekspertologia sądowa: nauka, studia, praktyka" tradycyjnie rozpoczęła się powitaniem uczestników

---

[5] H. Malevski, G. Juodkaitė-Granskienė, M. Shepitko, *10 (Extraordinary) International Scientific And Practical Conference „Criminalistics and Forensic Examination: Science, Studies, Practice"*, „Криминалистъ первопечатный" 2014, № 9, s. 177–181.

[6] Attualita Grafologica, Trimestrale dell' Associazione Grafologica Italiana, 101, Anno XXV n. 4 Ottobre–Dicembre 2006, s. 16.

[7] *XI Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika (XI Criminalistics and Forensic Science: science, studies, practice)*, Vilnius 2015.

[8] W tomie zostały zamieszczone artykuły biograficzne poświęcone prof. dr. hab. Mariuszowi Kulickiemu (Polska) i doc. dr Ona Danutė Dambrauskaitė (Litwa).

i gości przez prezesa Litewskiego Towarzystwa Kryminalistycznego panią doc. dr Gabrielė Juodkaitė-Granskienė, która między innymi wspomniała o podpisaniu w Toruniu umowy o współpracy PTK i LTK. Konferencję swoją obecnością zaszczycili Kanclerz Ministerstwa Sprawiedliwości Republiki Litewskiej pan Arūnas Kazlauskas oraz sędzia Sądu Najwyższego Litwy pani prof. dr Rima Ažubalytė, którzy w imieniu swoim i przełożonych życzyli uczestnikom owocnych obrad, podkreślając znaczenie nauki kryminalistycznej i ekspertyzy sądowej w procesie zwalczania i prewencji przestępstw oraz w działalności wymiaru sprawiedliwości.

Podczas części oficjalnej rozpoczynającej się konferencji prof. Henrykowi Malewskiemu został wręczony srebrny medal im. Herberta Mannsa za znaczące osiągnięcia i popularyzację nauki kryminalistycznej, ustanowiony przez Kongres Kryminalistyczny. Medal wręczył prezydent tej międzynarodowej organizacji pozarządowej prof. dr hab. Valery Shepitko (Ukraina).

Merytoryczna część konferencji rozpoczęła się od referatu prof. H. Malewskiego (Litwa) „Kryminalistyka, ekspertologia sądowa i nauki prawa procesowego – koegzystencja, konkurencja czy komplementarność?". Celem tego referatu było pokazanie w kontekście historycznym złożonych powiązań wyżej wymienionych dyscyplin naukowych, zmian granic i zakresu tych nauk, co powodowało i powoduje powstawanie między nimi obszarów „napięć". Jednym z podstawowych zadań naukowców jest dążenie do wypracowania modelu komplementarności w rozwoju tych ważnych dla zwalczania i prewencji przestępczości nauk. Referat prof. V. Shepitko i dr. M. Shepitko (Ukraina) „Konsolidacja wiedzy kryminalistycznej w warunkach przemian historycznych i globalizacji we współczesnym świecie" współbrzmiał z referatem prof. H. Malewskiego, wygłoszonym na VI Sympozjum Polskiego Towarzystwa Kryminalistycznego „Kryminalistyka – jedność nauki i praktyki" w Toruniu. Autorzy w historycznej perspektywie przedstawili proces rozwoju nauki kryminalistycznej oraz podkreślili konieczność konsolidacji wiedzy kryminalistycznej we współczesnym świecie z wykorzystaniem w tym celu różnorodnych form współpracy. Interesujący referat „Biegły w nowym modelu polskiego kodeksu postępowania karnego" przygotowany we współautorstwie z dr. hab. I. Sołtyszewskim wygłosił dr K. Krassowski (Polska). Autorzy dokonali analizy zmian przewidzianych w polskim procesie karnym i dotyczących wykorzystywania wiadomości specjalnych, które wchodzą w życie z dniem 1 lipca 2015 r. Pierwszą sesję konferencji zakończyło wystąpienie doc. dr G. Juodkaitė-Granskienė (Litwa) z referatem „Reglamentacja ekspertyzy sądowej według standardów europejskich", w którym podkreśla się znaczenie tworzonych przez ENFSI i inne struktury Unii Europejskiej norm, regulacji i standardów w dziedzinie ekspertyzy sądowej.

W drugim dniu konferencji została wygłoszona większość referatów oraz zaprezentowane plakaty. Pierwszy referat o projekcie naukowo-badawczym dotyczącym realizacji naukowej koncepcji europejskiej wizji kryminalistyki 2020 na Litwie wygłosił prof. dr V.E. Kurapka (Litwa, współautorzy: prof. dr

S. Matulienė, prof. dr Eglė Bilevičiūtė, S. Stankevičiūtė). Wspomniany wielowątkowy projekt badawczy dotyczy analizy zapotrzebowania na stosowanie wiedzy kryminalistycznej przez różnorodne podmioty na Litwie, poziomu regulacji działalności biegłych oraz kierunków i mechanizmów współtworzenia europejskiej przestrzeni kryminalistycznej. W określonym zakresie wspomniany referat współbrzmiał z problematyką badań dotyczących oczekiwań polskich środowisk prawniczych wobec funkcjonowania biegłych sądowych, które zostały przedstawione na VI Sympozjum PTK przez dr M. Tomaszewską-Michalak (współautor P. Rybicki). Interesujący referat o współczesnej terminologii nauki kryminalistycznej przedstawił prof. dr hab. V. Tishchenko (Ukraina), który zaznaczył, że istnieje potrzeba uporządkowania terminologii i pojęć kryminalistycznych, szczególnie z uwagi na konieczność poprawnego ich stosowania. Współczesna kryminalistyka w tempie ekspresowym przyswaja nowe metody i technologie, co jest też powiązane z wprowadzaniem do piśmiennictwa kryminalistycznego nowych pojęć i terminów. Dr K. Krassowski (Polska) wygłosił referat o warunkach współpracy policji krajów UE ze szczególnym uwzględnieniem istniejącej w tym obszarze bazy prawnej. Kończąc swoje wystąpienie, dr K. Krassowski stwierdził, że nie wykorzystujemy w dostatecznym zakresie tych możliwości, które stwarza współczesna baza prawna Unii Europejskiej, nie tylko w dziedzinie zwalczania przestępczości czy jej prewencji, lecz także w dziedzinie szeroko pojmowanych naukowych badań kryminalistycznych. Koledzy z Łotwy dr E. Nimande i dr V. Terehovičs od dłuższego czasu zajmują się problematyką teorii nauki kryminalistycznej[9] i na konferencję przygotowali referat o teoretycznych podstawach i zakresie stosowania kryminalistycznych metodyk śledczych. Następny referat, oparty na wspólnych międzynarodowych badaniach empirycznych, przedstawił dr B. Šalna (Litwa), a współautorami byli A. Kowalczyk z Polski oraz L. Lyvienė z Litwy. Badanie dotyczyło identyfikacji na podstawie głosu osoby mówiącej w kilku różnych językach (ojczystym i obcym). Prof. dr hab. Irina Perepechina z Moskiewskiego Państwowego Uniwersytetu im. M. Łomonosowa (Rosja) w swoim referacie powiązała problematykę wykorzystywania współczesnych technologii naukowych (badania DNA) w wykrywaniu przestępstw z problematyką wykładania kryminalistyki i innych nauk sądowych na studiach prawniczych. Jej zdaniem dydaktyka kryminalistyczna nie nadąża za współczesnym rozwojem nauki, a to może mieć negatywne skutki dla praktyki. Dr G. Žalkauskaitė (Litwa) poświęciła swój referat analizie semantycznej pojęć „pogróżka" i „terroryzowanie" (*mobbing*), których rozgraniczenie ma decydujące znaczenie w kwalifikacji prawnej czynu. Autorka, jako biegła z dziedziny badań lingwistycznych, przedstawiła wyniki swoich refleksji na ten temat, opartych na wykonanych ekspertyzach sądowych. Doc. dr Marek Fryštak (Czechy) analizował problematykę badania zapachów (osmologia) i jego wykorzystywanie w procedurze karnej Czech. Analizując wartość dowodową opinii osmologicznej, autor podkreśla, że jest to jeden ze środków dowodowych, który

[9] В.Н. Терехович, *Теория криминалистики. Общая часть*, Рига 2015.

w czeskich procedurach karnych nie jest jednoznacznie oceniany, chociaż jego wykorzystanie nierzadko okazuje się znaczące nie tylko dla wykrycia sprawcy. Mecenas K. Kurapka (Litwa) swoje rozważania poświęcił kodeksowej regulacji stosowania wiadomości specjalnych w procedurach administracyjnych oraz wynikającym z tego praktycznym problemom. Prof. dr R. Burda (Litwa) zaprezentował referat na temat bulwersującej sprawy mordu siedmiu funkcjonariuszy litewskich w Miednikach 31 lipca 1991 r., który oceniał z pozycji zarówno prawa krajowego, jak i międzynarodowego w powiązaniu z problematyką kryminalistyczną[10]. Martin Laca (Słowacja) wygłosił opracowany wspólnie z prof. dr. J. Metenką referat o znaczeniu oględzin miejsca zdarzenia w czynnościach dochodzeniowo-śledczych. Zaprezentowany tekst był oparty na badaniach empirycznych, przeprowadzonych na Słowacji w ramach realizacji międzynarodowego projektu naukowo-badawczego. Interesujący referat, oparty na badaniach empirycznych, przedstawiła dr Danijela Frangež (Słowenia, współautor prof. dr Darko Maver); dotyczył on spraw wykorzystywania seksualnego nieletnich. Wspomniane studium było oparte na analizie akt spraw karnych oraz wynikach badań ankietowych prokuratorów i śledczych. Z dużym zaciekawieniem wysłuchano referatu dr. K. Krassowskiego (Polska) o wykorzystywaniu dronów w zwalczaniu przestępczości. Ten temat wpisywał się w problematykę adaptowania i wykorzystywania nowych technologii w kryminalistyce. Nowych technologii dotyczył też referat doc. dr J. Juškevičiūtė (Litwa, współautorzy: prof. dr V.E. Kurapka, prof. dr S. Matulienė, I. Ilgauskienė). Autorka przedstawiła założenia oraz pierwsze wyniki międzynarodowego projektu badawczego, którego podstawowym celem jest opracowanie urządzenia wykrywającego na odległość określone związki chemiczne (materiały wybuchowe czy też narkotyki).

Kilka referatów dotyczyło doskonalenia czynności dochodzeniowo-śledczych. Historia kryminalistyki zna niemało przykładów sytuacji, kiedy ktoś, z tych czy innych przyczyn, przyznaje się i przyjmuje winę za niepopełniony czyn. Jak często mamy do czynienia z takimi zdarzeniami, jakie są tego motywy i okoliczności, jakie mamy możliwości i co wskazuje, że osoba bierze na siebie odpowiedzialność za niepopełnione przestępstwo – tej problematyce był poświęcony artykuł dr Olesi Vashchuk (Ukraina). Według autorki, im wcześniej da się ustalić fakt nieprawdziwego samooskarżenia, tym większe są szanse na ustalenie prawdziwego sprawcy przestępstwa. W referacie podkreśla się szczególne znaczenie wiedzy psychologicznej, której zastosowanie w takich

[10] O popełnienie tego czynu oskarża się funkcjonariuszy ówczesnej jednostki specjalnej milicji (ros. – ОМОН, отряд милиции особого назначения) z Rygi, która jednoznacznie opowiedziała się za władzą sowiecką i uczestniczyła w szeregu akcji przeciwko strukturom odradzających się i dążących do niepodległości państw bałtyckich (Łotwy i Litwy). Obecnie na Litwie duże kontrowersje wywołał wyrok uniewinniający dowódców wileńskiego OMON-u za przestępstwa wojenne i przeciwko ludzkości, gdyż według składu orzekającego zebrane dowody nie pozwalają uznać ich czynów za inkryminowane zbrodnie. Proces odbywał się bez udziału oskarżonych.

okolicznościach jest niezbędne. Prokurator J. Baltrunienė (Litwa) analizowała czynniki sytuacyjne w przemycie papierosów, które mają znaczący wpływ na poziom i dynamikę przestępczości przemytniczej. R. Šlepetys (Litwa, współautorzy: dr Ž. Navickienė, prof. dr V.E. Kurapka, prof. dr S. Matulienė) mówił o konieczności sprawnego planowania czynności dochodzeniowo-śledczych od początku postępowania przygotowawczego, co ma zapewnić efektywność procesu wykrywczego i dowodowego.

Drugiego dnia konferencji odbyła się sesja plakatowa, na której zaprezentowano sześć plakatów. Przedstawicielki Litewskiego Centrum Ekspertyzy Sądowej D. Bartkevičienė i J. Volkovska przygotowały plakat o współczesnych technologiach badania cząsteczek tonerów w wydrukach dokumentów. Litewscy medycy sądowi dr M. Jakubėnienė i L. Gogelis przedstawili wyniki badań porównawczych stężenia alkoholu we krwi i innych nośnikach biologicznych. G. Gardonyi oraz D. Petretei (Węgry) poinformowali o współczesnych technologiach i urządzeniach stosowanych w badaniu obrazów. L. Levulytė i V. Žuraulis (Litwa) podzielili się swoimi refleksjami na temat zmniejszania ryzyka pomyłki przy określaniu szybkości samochodu dzięki zastosowaniu metod fotogrametrycznych. J. Sedlačkova i J. Provaznik (Czechy) dokonali analizy zwalczania przestępczości narkotykowej ze szczególnym uwzględnieniem znaczenia współpracy międzynarodowej. Plakat dr R. Włodarczyk (Polska) był poświęcony wybranym zagadnieniom tanatologii oraz casusom, w których tylko wiedza i doświadczenie medyków sądowych pozwoliły rozstrzygnąć przyczyny śmierci gwałtownej i tym samym uniknąć błędnych decyzji w zaszeregowaniu zdarzenia i kwalifikacji czynu. Trzeba zaznaczyć, że sesja plakatowa cieszyła się dużym zainteresowaniem i uczestnicy konferencji nie tylko często dyskutowali z autorami prezentacji, ale też wypowiadali się i porównywali sytuację ze stanem we własnych krajach.

W czasie ostatniej sesji trzeciego dnia konferencji zostały wygłoszone dwa referaty i odbyła się godzinna dyskusja. Biegła Joanna Zemlik (Polska) poruszyła problematykę przemocy w stosunku do dzieci, których ochronę zdrowia często można zapewnić tylko po wykryciu śladów przemocy przez lekarza, wychowawcę czy nauczyciela. Musi to spowodować odpowiednie postępowanie wyjaśniające, a wiedza specjalna medyków może się przyczynić nie tylko do ustalenia stanu faktycznego, ale też ustalenia okoliczności oraz przyczyn powstania urazów. Rozważania autorki były poparte przykładami z praktyki. Biegła z Litewskiego Centrum Ekspertyzy Sądowej R. Tamošiūnaitė zaprezentowała referat o problemach prokuratorów w szykowaniu materiałów na ekspertyzę pismoznawczą, co jest skutkiem coraz mniejszej ilości godzin z kryminalistyki na studiach prawniczych.

Ponad godzinną programowo przewidzianą dyskusję poprowadzili prof. dr S. Matulienė, doc. dr G. Juodkaitė-Granskienė i prof. dr H. Malewski, który zaznaczył, że w czasie poprzednich sesji nie było zbyt wiele czasu na dyskusje, a tylko na krótkie pytania i odpowiedzi, co nie znaczy, że w pierwszych dniach

nie było dyskusji. Bardzo gorące dyskusje były prowadzone w warunkach nieformalnych. Początkowo w wystąpieniach uczestników dominowały sprawy ogólnoteoretycznych zagadnień kryminalistyki i potrzeby aktywizacji współpracy międzynarodowej. Jednak dużo uwagi poświęcono sprawom ekspertyzy sądowej i prawnym aspektom reglamentacji działalności biegłego, a także problematyce doskonalenia czynności dochodzeniowo-śledczych.

Organizatorzy konferencji podziękowali wszystkim uczestnikom oraz wyrazili nadzieję, że w następnym roku ponownie spotkamy się na zamiejscowej XII konferencji międzynarodowej „Kryminalistyka i ekspertologia sądowa: nauka, studia, praktyka" w jednym z sąsiednich krajów.

Fot. 1. Uczestnicy XI Międzynarodowej Konferencji Naukowej „Kryminalistyka i ekspertologia sądowa: nauka, studia, praktyka", Wilno, 25–27 czerwca 2015 r.

Fot. 2. Sędzia Sądu Najwyższego Litwy prof. dr Rima Ažubalytė oraz moderatorzy pierwszej sesji plenarnej prof. dr Henryk Malewski (Litwa) i prof. dr hab. Valery Shepitko (Ukraina)

Opracował:
prof. dr Henryk Malewski
Litewskie Towarzystwo Kryminalistyczne

KOMUNIKATY

UCHWAŁA II KONGRESU NAUK SĄDOWYCH

1. Uczestnicy Kongresu z zadowoleniem przyjmują fakt zwołania po raz drugi w historii Polski, spotkania adresowanego do wszystkich biegłych i rzeczoznawców.
2. Wprowadzenie w Polsce, w szerszym zakresie zasady kontradyktoryjności powoduje dalsze zwiększenie roli biegłych i rzeczoznawców, ułatwi sądom weryfikowanie nieprawidłowych, czy błędnych ekspertyz, ale nakłada też zwiększoną odpowiedzialność za opinie, w tym i karną, cywilną i zawodową.
3. Uczestnicy Kongresu krytycznie oceniają projekt Ustawy o biegłych sądowych, który nie uwzględnia krytycznych i pragmatycznych wniosków, jakie zgłosiły Stowarzyszenia i Organizacje zrzeszające biegłych sądowych. Dlatego powinno się, w imieniu wszystkich biegłych i rzeczoznawców, a nie tylko poszczególnych organizacji, nadal krytycznie monitorować dalsze etapy procesu legislacyjnego tej ustawy.
4. Istnieje potrzeba stałego rejestrowania i monitorowania wniosków i postulatów środowiska biegłych i rzeczoznawców poprzez forum internetowe na stronie internetowej www.2kns.pl, podobnie jak to zrobiono przed I KNS.
5. Wzorem instytucji i organizacji polskich i międzynarodowych szerszego upowszechnienia i praktycznego stosowania wymagają zasady etycznego postępowania biegłych i rzeczoznawców, a zawarte w kodeksach etycznych tych instytucji i organizacji.
6. Uczestnicy Kongresu uznają celowość organizowania takich imprez w przyszłości, co 2–4 lata.

Uczestnicy II Kongresu Nauk Sądowych

Warszawa, Uniwersytet Warszawski, 20 czerwca 2015 r.

REGULAMIN PRZYZNAWANIA NAGRÓD POLSKIEGO TOWARZYSTWA KRYMINALISTYCZNEGO W KONKURSIE IM. PROF. TADEUSZA HANAUSKA NA PRACĘ ROKU Z DZIEDZINY KRYMINALISTYKI

§ 1

Nagrody i wyróżnienia Polskiego Towarzystwa Kryminalistycznego (PTK) za Pracę Roku z Dziedziny Kryminalistyki, przyznawane corocznie, począwszy od 1999 roku, za najlepsze prace o tematyce kryminalistycznej napisane przez polskich i zagranicznych autorów. Nagrody przyznawane będą z funduszy własnych Polskiego Towarzystwa Kryminalistycznego. Nagrody mogą mieć postać finansową, rzeczową lub formę wyróżnienia potwierdzonego dyplomem.

§ 2

Konkurs na najlepsze prace z dziedziny kryminalistyki ma na celu popularyzację tej nauki, pobudzanie inicjatywy do podejmowania indywidualnych lub zespołowych prac naukowo – badawczych, naukowo-popularyzacyjnych, monograficznych i innych prac z tej dziedziny oraz oddziaływanie na poziom tych prac.

§ 3

W celu nadania wysokiej rangi Konkursowi oraz zapewnienia odpowiednich kryteriów i procedur przyznawania nagród powołuje się Kapitułę Konkursu i Jury Konkursu. Zadaniem Kapituły jest dbanie o wysoki poziom konkursów, określanie ogólnych zasad organizacji konkursów i przyznawania nagród, a także pomoc w pozyskiwaniu zewnętrznych środków finansowych na nagrody. Zadaniem Jury konkursowego jest dokonanie oceny nadesłanych prac konkursowych oraz wnioskowanie do Rady Naukowej o przyznanie nagrody lub nagród oraz wyróżnień autorom najwyżej ocenionych prac. Za udział w pracach Kapituły i Jury ich Członkowie nie otrzymują wynagrodzenia.

§ 4

Kapituła Konkursu jest stałym, honorowym kolegium, w skład którego wchodzą Przewodniczący Rady Naukowej PTK – jako Przewodniczący Kapituły, Prezes PTK, Prezesi Honorowi PTK oraz przedstawiciele organów i instytucji zasłużonych dla rozwoju kryminalistyki i popularyzacji jej osiągnięć, którzy przyjęli zaproszenie Prezesa PTK i Przewodniczącego Rady Naukowej PTK do udziału w pracach Kapituły.

§ 5

Nagrody przyznawane są przez Radę Naukową Polskiego Towarzystwa Kryminalistycznego (PTK) na wniosek powoływanego w tym celu Jury Konkursowego. Rada Naukowa określa rodzaj i wysokość nagród oraz wnioskuje do Zarządu Głównego o przyznanie środków na ten cel.

§ 6

Jury Konkursowe powoływane będzie corocznie, w pierwszym kwartale roku następującym po roku, za który mają być przyznane nagrody. W skład Jury powinno wchodzić co najmniej 5 osób, w tym przewodniczący lub wiceprzewodniczący Rady Naukowej PTK. Jury jest wybierane przez Radę Naukową Polskiego Towarzystwa Kryminalistycznego spośród członków Rady i innych osób, które cieszą się uznaniem w polskim środowisku kryminalistycznym.

§ 7

W Konkursie mogą być brane pod uwagę wszystkie prace o tematyce kryminalistycznej, wyróżniające się wysokim poziomem naukowym lub szczególnym znaczeniem dla praktyki. Pracami zgłaszanymi na Konkurs mogą być prace naukowe, magisterskie, dyplomowe i inne opracowania.

§ 8

Prace biorące udział w Konkursie powinny być opublikowane w roku, za który przyznawana jest nagroda. W przypadku prac doktorskich, magisterskich i dyplomowych powinny być one obronione w roku, za który przyznawana jest nagroda, przy czym nie jest wymagane ich opublikowanie. W przypadku prac habilitacyjnych nagroda może być przyznana za rok, w którym został zakończony przewód habilitacyjny.

§ 9

Kandydatury prac konkursowych mogą być zgłaszane przez Zarządy Oddziałów Polskiego Towarzystwa Kryminalistycznego oraz członków Rady Naukowej i Zarządu Głównego PTK, a także przez kierowników właściwych placówek, w których praca została przygotowana lub obroniona (dziekanów, dyrektorów instytutów, laboratoriów, kierowników katedr i zakładów, komendantów szkół itp.), a także przez promotorów i recenzentów prac. Wraz ze zgłoszeniem powinien zostać przekazany egzemplarz pracy z krótką charakterystyką uzasadniającą zgłoszenie do Konkursu, w przypadku zaś prac habilitacyjnych, doktorskich i magisterskich – dodatkowo ich recenzje. Prace nadesłane na Konkurs są archiwizowane w bibliotece PTK i nie są zwracane autorom.

§ 10

Jury Konkursu zgłosi Radzie Naukowej wniosek o przyznanie nagrody lub nagród oraz wyróżnień najpóźniej do końca czerwca danego roku. Rada Naukowa na posiedzeniu podejmie uchwałę o przyznaniu nagród większością głosów.

§ 11

W każdym roku można będzie przyznać jedną lub więcej nagród. W zależności od liczby zgłoszonych prac i ich poziomu, możliwe będzie przyznanie nagród w różnych kategoriach, takich jak najlepsza opublikowana monografia, najlepsza praca naukowa bądź magisterska itp. Jeśli zgłoszone prace nie będą spełniały kryteriów Konkursu lub będą reprezentowały niski poziom, można nie przyznać żadnej nagrody lub nagrody pierwszej.

§ 12

Laureaci Konkursu, którzy otrzymali nagrodę pieniężną lub rzeczową, otrzymają także dyplom. Wysokość nagród i ich rodzaj ustala Rada Naukowa w porozumieniu z Zarządem Polskiego Towarzystwa Kryminalistycznego.

§ 13

Nagrody są wręczane uroczyście w obecności Prezesa Polskiego Towarzystwa Kryminalistycznego, członków Kapituły Konkursu i Rady Naukowej oraz zaproszonych gości.

§ 14

Wszelkie zmiany oraz sprawy nieuregulowane w niniejszym regulaminie rozstrzyga Zarząd Główny PTK po konsultacji z Radą Naukową.

Zarząd Główny i Rada Naukowa
Polskiego Towarzystwa Kryminalistycznego

REGULAMIN KONKURSU NA NAGRODĘ PROFESORA BRUNONA HOŁYSTA DLA WYRÓŻNIAJĄCYCH SIĘ MŁODYCH KRYMINALISTYKÓW

1. Polskie Towarzystwo Kryminalistyczne ogłasza konkurs na nagrodę Profesora Brunona Hołysta dla wyróżniających się w pracy naukowej lub zawodowej młodych naukowców i praktyków z dziedziny kryminalistyki.
2. Nagroda jest fundowana corocznie przez Profesora Brunona Hołysta, który przekazuje na ten cel Polskiemu Towarzystwu Kryminalistycznemu odpowiednie środki finansowe. Za zgodą Rady Naukowej PTK i akceptacją Fundatora, środki finansowe na fundusz nagrodowy mogą być również przyjmowane od innych osób prawnych lub fizycznych.
3. Nagroda jest przyznawana przez Radę Naukową jednemu lub dwóm laureatom na zasadzie konkursu, na podstawie wniosku Komisji Konkursowej, w którym przedstawiane jest nazwisko proponowanego laureata lub laureatów oraz wysokość nagrody. Laureaci w chwili przyznania stypendium nie powinni przekroczyć 35 roku życia.
4. Do przedstawienia zgłoszeń na konkurs uprawnieni są: Fundator stypendium, Zarządy Oddziałów Polskiego Towarzystwa Kryminalistycznego, członkowie Rady Naukowej i Zarządu Głównego PTK, kierownicy właściwych placówek, w których publikacja lub praca została przygotowana, wdrożona lub obroniona (opiekunowie naukowi, rektorzy, dziekani, dyrektorzy instytutów, laboratoriów, kierownicy katedr i zakładów, komendanci szkół itp.), a także osoby ubiegające się o nagrodę. Wraz ze zgłoszeniem powinien zostać przekazany egzemplarz pracy z krótką charakterystyką uzasadniającą zgłoszenie do Konkursu. W przypadku innych przedsięwzięć mających stanowić podstawę zgłoszenia należy dołączyć dokumentację lub opis pozwalający na ocenę ich istoty, wartości i przydatności dla nauki i praktyki kryminalistycznej.
5. Komisja Konkursowa składa się z pięciu osób, cieszących się uznaniem i autorytetem w polskim środowisku kryminalistycznym. Jednym z członków Komisji powinien być przewodniczący lub wiceprzewodniczący Rady Naukowej PTK. Komisję Konkursową powołuje na dwuletnią kadencję Rada Naukowa PTK, wyznaczając jej przewodniczącego.
6. Nagrodę otrzyma osoba lub osoby, których dorobek naukowy lub zawodowy Komisja Konkursowa uzna za wybitny, wyróżniający się spośród dorobku osób zgłoszonych do Konkursu. Dorobek ten może obejmować pracę doktorską lub inne opracowanie o tematyce kryminalistycznej bądź też znaczące

osiągnięcie praktyczne polegające m.in. na opracowaniu lub rozwinięciu nowej metody badań kryminalistycznych, wprowadzeniu do praktyki kryminalistycznej innowacyjnego rozwiązania technicznego lub organizacyjnego, zrealizowaniu projektu naukowego o priorytetowym znaczeniu dla nauki i praktyki kryminalistycznej. Uwzględniane w konkursie publikacje lub inne prace powinny być przygotowywane lub realizowane w okresie poprzedzającym przyznanie nagrody.

7. Przyznane nagrody są wypłacane jest jednorazowo w ramach środków przekazanych na ten cel przez Fundatora. Laureat lub laureaci otrzymują także dyplomy okolicznościowe.
8. Zgłoszenie wniosku Radzie Naukowej przez Komisję Konkursową, o którym jest mowa w p. 3, powinno nastąpić nie później niż do dnia 15 września każdego roku, w którym przyznawana jest nagroda. Uchwała Rady Naukowej o przyznaniu nagrody powinna być podjęta najpóźniej do dnia 15 października tego roku. Posiedzenie Rady Naukowej PTK zwołuje jej Przewodniczący. Rada Naukowa podejmuje uchwałę w głosowaniu, większością głosów. W razie równej liczby głosów rozstrzygający jest głos prowadzącego obrady.
9. Dyplom przyznający nagrodę wręczany jest uroczyście w obecności Fundatora lub jego przedstawiciela, Prezesa Polskiego Towarzystwa Kryminalistycznego, członków Rady Naukowej oraz zaproszonych gości.
10. W przypadku nie przyznania nagrody w danym roku środki zwiększają fundusz nagrodowy w następnych latach.
11. Prace nadesłane na Konkurs są archiwizowane w bibliotece PTK i nie są zwracane autorom. Prace te mogą być wykorzystywane w działalności statutowej PTK, jeżeli ich autor nie wniesie zastrzeżenia.
12. W sprawach nie uregulowanych w niniejszym regulaminie lub wymagających zmian decyzje podejmuje Rada Naukowa, a w razie braku jej kompetencji Zarząd Główny lub inny organ władzy PTK, zgodnie ze statutem.

Zarząd Główny i Rada Naukowa
Polskiego Towarzystwa Kryminalistycznego

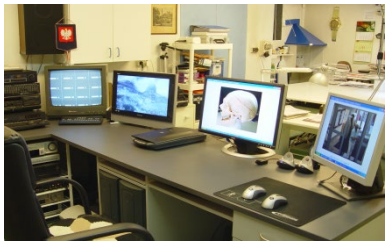
ZAKRES BADAŃ POLSKIEGO TOWARZYSTWA KRYMINALISTYCZNEGO

POLSKIE
TOWARZYSTWO
KRYMINALISTYCZNE
Rok założenia 1973

ORGANIZACJA POŻYTKU PUBLICZNEGO
www.kryminalistyka.pl

Polskie Towarzystwo Kryminalistyczne jest stowarzyszeniem o zasięgu ogólnokrajowym, działającym od ponad 40 lat, mającym status organizacji pożytku publicznego. PTK prowadzi aktywną działalność popularyzującą wiedzę kryminalistyczną i wspomagającą wymiar sprawiedliwości. Prowadzi szkolenia kryminalistyczne, prace naukowo-badawcze oraz działalność wydawniczą. W strukturach Towarzystwa funkcjonuje dobrze wyposażone laboratorium kryminalistyczne (CBS PTK) wykonujące ekspertyzy dla organów procesowych i innych instytucji oraz osób prywatnych z różnych dziedzin i specjalności kryminalistycznych, a w tym m.in.:

- **badania dokumentów** (badanie pisma i badania techniczne - pełny zakres)
- **badania audiowizualne, systemów monitoringu i fotograficzne,**
- **badania komputerowe**
- **badania fonoskopijne,**
- **badania daktyloskopijne i traseologiczne,**
- **badania mechanoskopijne,**
- **badania biologiczne (w tym DNA),**
- **badania fizykochemiczne,**
- **badania narkotyków,**
- **badania broni i balistyczne,**
- **badania wypadków drogowych,**
- **badania antropologiczne i antroposkopijne** (w tym identyfikacja osób na zdjęciach, taśmach wideo i innych nośnikach obrazu; identyfikacja przedmiotów zarejestrowanych na ww. nośnikach itp.),
- **badania wariograficzne** (do celów procesowych i pozaprocesowych),
- **inne badania** (kominiarskie, znaków probierczych, gleboznawcze itp.).



Jako jeden z nielicznych ośrodków kryminalistycznych wykonujemy badania wieku pisma oraz chronologii zapisów.

Szczegółowe informacje na stronie internetowej **www.kryminalistyka.pl**
kontakt: biuro@kryminalistyka.pl
tel. 22 692 43 85

REGULAMIN
PUBLIKOWANIA PRAC W „PROBLEMACH WSPÓŁCZESNEJ KRYMINALISTYKI”

1. „Problemy Współczesnej Kryminalistyki” są periodykiem naukowym wydawanym 1-2 w roku przez Katedrę Kryminalistyki Uniwersytetu Warszawskiego i Polskie Towarzystwo Kryminalistyczne.
2. W „Problemach Współczesnej Kryminalistyki” publikowane są prace: teoretyczne, eksperymentalne, syntetyzujące i analityczne oraz kazuistyczne z zakresu kryminalistyki i dziedzin pokrewnych, a także recenzje i sprawozdania z konferencji, zjazdów i zebrań naukowych.
3. Teksty prac winny być sporządzone czcionką znormalizowaną (Times New Roman), jednostronnie, na arkuszach formatu A-4, z marginesem 2,5 cm z lewej i 2,5 cm z prawej strony, z zachowaniem półtora odstępu między wierszami (30 wierszy na stronie). Zapis winien być dokonany podstawowym krojem pisma bez wyróżnień.
4. Opracowania teoretyczne nie powinny przekraczać 20, a kazuistyczne 15 stron maszynopisu wraz z rycinami, tabelami, wykazem piśmiennictwa i streszczeniem.
5. Nadsyłane prace będą recenzowane.
6. Na pierwszej stronie, przed tytułem i właściwym tekstem pracy, należy umieścić imię i nazwisko Autora (Autorów), tytuł pracy w języku polskim.
7. Praca winna być zakończona słowami kluczowymi i streszczeniem w języku polskim i angielskim nieprzekraczającym 15 wierszy maszynopisu.
8. Liczbę tabel i rycin winno się ograniczyć do minimum niezbędnego dla zrozumienia tekstu.
9. Ryciny i tabele oznacza się numeracją arabską.
10. Przypisy powinny zawierać nazwisko i pierwszą literę imienia Autorów pracy, tytuł czasopisma oraz kolejno – rok, numer tomu i pierwszą stronę pracy. Przy pozycjach książkowych należy podać pełny tytuł dzieła, wydawcę, rok i miejsce wydania. Przypisy umieszcza się na dole strony, na której przypis jest przywoływany.
11. Redakcja zastrzega sobie prawo dokonywania w pracy niezbędnych poprawek stylistycznych i skrótów bez porozumienia z Autorem.
12. Za prace publikowane w „Problemach Współczesnej Kryminalistyki” nie są wypłacane honoraria autorskie. Autorzy zobowiązują się do podpisania umowy nieodpłatnego przeniesienia majątkowych praw autorskich do publikacji na Wydawcę. Do artykułu należy dołączyć dane, które umożliwią

sporządzenie umowy, tj. nazwisko, imię, imię ojca i matki, datę i miejsce urodzenia, PESEL, miejsce zamieszkania. Wzór umowy znajduje się na stronie internetowej Polskiego Towarzystwa Kryminalistycznego www.kryminalistyka.pl

13. Na końcu pracy należy zamieścić: adres mailowy, numer telefonu i adres zamieszkania Autorów, na które kierowana będzie korespondencja.
14. Prace nie spełniające opisanych powyżej warunków nie będą opracowywane do czasu dokonania przez Autora niezbędnych uzupełnień i poprawek.
15. Prace niezakwalifikowane do druku nie są zwracane Autorom.
16. Prace w formie elektronicznej należy wysyłać na adres Redakcji: redakcja.pwk@gmail.com

PROCEDURA RECENZOWANIA PRAC W „PROBLEMACH WSPÓŁCZESNEJ KRYMINALISTYKI”

Wydawca:
Katedra Kryminalistyki Wydziału Prawa i Administracji Uniwersytetu Warszawskiego
Polskie Towarzystwo Kryminalistyczne, e-mail: redakcja.pwk@gmail.com

Rada Naukowa:
prof. dr hab. Jerzy Kasprzak
prof. UWr. dr hab. Maciej Szostak
prof. dr Henryk Malewski (Litwa)

Sekretarz Redakcji
dr Katarzyna Julia Furman

Redakcja Naukowa:
prof. dr hab. Ewa Gruza
prof. dr hab. Tadeusz Tomaszewski
dr Mieczysław Goc

Lista recenzentów:
prof. UWM dr hab. Bronisław Młodziejowski
prof. UWM dr hab. Jarosław Moszczyński
dr Wacław Brzęk
dr hab. Elżbieta Kozłowska-Żywucka

Procedura recenzowania prac naukowych nadsyłanych do publikacji w „Problemach Współczesnej Kryminalistyki”:

1. Procedura recenzowania artykułów w jest zgodna z zaleceniami Ministerstwa Nauki i Szkolnictwa Wyższego.
2. Przekazanie tekstu do publikacji w Problemach Współczesnej Kryminalistyki (PWK) jest jednoznaczne z wyrażeniem przez Autora/Autorów zgody na wszczęcie procedury recenzowana artykułu.
3. Nadesłane materiały poddawane są wstępnej ocenie formalnej przez Radę Naukową i Redakcję Naukową PWK, zwłaszcza pod kątem ich zgodności

z wymaganiami wydawniczymi, jak również z obszarami tematycznymi wydawnictwa.

4. Standardowo artykuły recenzowane przez dwóch niezależnych recenzentów, którzy nie są członkami Rady Naukowej i Redakcji Naukowej oraz nie są zatrudnieni etatowo w jednostkach wydającej czasopismo. Z uwagi na wąskie grono ekspertów z niektórych dziedzin, czy specjalności kryminalistycznych, zwłaszcza z zakresu techniki kryminalistycznej, dopuszcza się odstępstwa od zasady niezależnej recenzji, czyli powoływanie specjalistów spośród pracowników UW i PTK.
5. Nadesłane artykuły nie są przekazywane recenzentom z tej samej placówki, z której pochodzi Autor/Autorzy.
6. Prace recenzowane są anonimowo. Recenzenci nie znają nazwisk Autorów. Autor/Autorzy są informowani o wyniku procedury recenzenckiej z zachowaniem zasady poufności recenzji. W sytuacjach spornych powoływany jest kolejny recenzent.

ISSN 1643-2207