WDROŻENIE METOD I INSTRUMENTÓW ZAPOBIEGANIA PRZESTĘPCZOŚCI W ORGANIZACJACH

AUTORZY:

Adrian DONE, London Business School
Bartosz JANASZEK, Executive Education Center
Marcin KIELISZCZYK, Executive Education Center
Silvia KING, IESE Business School
Radosław KOSZEWSKI, Executive Education Center
Massimo MAORET, IESE Business School
Lucien RANDAZZESE, SRI International

KONSULTACJE NAUKOWE:

Joanna CYGLER, Szkoła Główna Handlowa
Agata KOSIERADZKA-FEDERCZYK,
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Gabriela JYŻ, Naczelny Sąd Administracyjny
Jan KOWALCZYK, BBS Banner Sp. z o.o.

AUTORZY:

Bartłomiej ORĘZIAK, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Marcin WIELEC, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Alina KLONOWSKA, Uniwersytet Ekonomiczny w Krakowie
Magdalena MAŁECKA-ŁYSZCZEK, Uniwersytet Ekonomiczny w Krakowie
Małgorzata SNARSKA, Uniwersytet Jagielloński
Joanna WYROBEK, Uniwersytet Ekonomiczny w Krakowie
Remigiusz ROSICKI, Uniwersytet im. Adama Mickiewicza w Poznaniu
Tomasz JEDYNAK, Uniwersytet Ekonomiczny w Krakowie
Artur MEZGLEWSKI, Akademia Sztuki Wojennej

WDROŻENIE METOD I INSTRUMENTÓW ZAPOBIEGANIA PRZESTĘPCZOŚCI W ORGANIZACJACH

Redakcja: Radosław Koszewski, Bartłomiej Oręziak, Marcin Wielec

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI | **Warszawa 2021**

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

FUNDUSZ SPRAWIEDLIWOŚCI

Współfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

RECENZENCI *dr hab. Bartosz Majchrzak, prof. UKSW*
dr hab. Andrzej Szymański, prof. UO

OPRACOWANIE REDAKCYJNE *Teresa Naumiuk*
PROJEKT OKŁADKI, SKŁAD, ŁAMANIE *Bogusław Słomka*

WYDANIE 2

ISBN 978-83-66344-36-5

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI
ul. Krakowskie Przedmieście 25, 00-071 Warszawa
SEKRETARIAT tel.: (22) 630-94-53, fax: (22) 630-99-24, e-mail: wydawnictwo@iws.gov.pl

DRUK, OPRAWA *„Elpil", ul. Artyleryjska 11, 08-110 Siedlce*

Spis treści

Słowo wstępne

Niniejszy raport stanowi podsumowanie prac badawczych przeprowadzonych w ramach trzeciego etapu projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" Instytutu Wymiaru Sprawiedliwości, a więc także trzecią pracę z cyklu poświęconego zagadnieniu przeciwdziałania przestępczości w kluczowych obszarach polskiej gospodarki.

Podjęte badania wpisują się w nurt działań służących zwalczaniu przyczyn przestępczości oraz ograniczaniu czynników ryzyka jej występowania. Celem prac badawczych podsumowanych w niniejszym raporcie jest analiza procesów wdrażania metod i instrumentów w zakresie zapobiegania przestępczości w wybranych organizacjach na świecie, a wynikiem przeprowadzonych prac – wskazanie istotnych czynników decydujących o sukcesie transformacji ukierunkowanej na wyeliminowanie czynników ryzyka występowania przestępczości, wśród których jako najważniejszy wskazuje się zmianę kultury organizacji, zarówno w instytucjach publicznych, jak i w strategicznych podmiotach gospodarczych.

Pierwsza część niniejszej publikacji (raport) stanowi podsumowanie specyfiki sposobów wdrażania metod oraz instrumentów zapobiegających przestępczości w czterech obszarach: finanse, ubezpieczenia, energetyka i zarządzanie ludźmi w organizacjach. W większości przypadków identyczne metody i instrumenty sprawdzają się w każdym z przedstawionych obszarów. Poszczególne branże różnią się jednak od siebie sposobem zarządzania, kulturą, a także strukturą organizacyjną, co z kolei oznacza, że w każdej z nich należy zwrócić uwagę na odmienne elementy związane z wdrażaniem poszczególnych metod i instrumentów służących zapobieganiu przestępczości.

Druga część niniejszej publikacji stanowi rezultat prac analitycznych podejmowanych przez Zespół Implementacyjny w ramach projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" Instytutu Wymiaru Sprawiedliwości. W ramach poszczególnych rozdziałów tematycznych wybrani eksperci przedstawili zagadnienia problemowe związane z rynkiem finansowym, energetycznym, ubezpieczeniowym oraz z zarządzaniem ludźmi w organizacji w wymiarze Transforming People and Organizations. Celem było naukowe, kompleksowe i innowacyjne spojrzenie na obszar przeciwdziałania przyczynom przestępczości oraz wsparcie, rozwój, a także uszczelnienie wyżej wskazanego systemu.

Monografia naukowa poświęcona jest niezwykle doniosłej i aktualnej problematyce, która niewątpliwie zasługuje na szczególną uwagę z punktu widzenia zapobiegania przyczynom przestępczości w finansach, energetyce, ubezpieczeniach oraz w zarządzaniu ludźmi w organizacji w aspekcie wdrożenia metod i instrumentów zapobiegania przestępczości w organizacjach.

CZĘŚĆ PIERWSZA

RAPORT

AUTORZY:

Adrian DONE, London Business School
Bartosz JANASZEK, Executive Education Center
Marcin KIELISZCZYK, Executive Education Center
Silvia KING, IESE Business School
Radosław KOSZEWSKI, Politechnika Warszawska
Massimo MAORET, IESE Business School
Lucien RANDAZZESE, SRI International

KONSULTACJE NAUKOWE:

Joanna CYGLER, Szkoła Główna Handlowa
Agata KOSIERADZKA-FEDERCZYK,
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Gabriela JYŻ, Naczelny Sąd Administracyjny
Jan KOWALCZYK, BBS Banner Sp. z o.o.

1. Wprowadzenie

Badania przeprowadzone na dwóch wcześniejszych etapach projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" poświęcono analizie przyczyn przestępczości w wybranych obszarach gospodarki, jak również identyfikacji wektorów stanowiących największe zagrożenie dla przynależących do nich organizacji. Wysiłki badawcze ukierunkowano na wypracowanie metod przeciwdziałania odpowiednio zidentyfikowanym rodzajom zagrożeń przy wykorzystaniu najlepszych standardów i praktyk dostępnych na świecie. W konsekwencji podsumowane w niniejszym raporcie prace badawcze dotyczyły sposobów wdrażania metodyki opracowanej na wcześniejszych etapach projektu.

1.1. Model Kottera

Uczestnicy seminariów zgodnie stwierdzili, że wdrożenie w organizacjach metod przeciwdziałania przestępczości nie jest odosobnionym, jednorazowym wysiłkiem. Mamy raczej do czynienia z ciągłym procesem, za którego przebieg ponoszą odpowiedzialność zarówno zarządy, jak i wszyscy pozostali pracownicy. Proces ten nieodłącznie wiąże się z koniecznością zmiany dotychczasowych paradygmatów, czyli zbioru przekonań rzutujących na sposób postrzegania organizacji przez jej pracowników – wizji strategicznej, wektorów zagrożeń, jak również codziennych operacji, relacji z klientami, kontrahentami i dostawcami oraz sposobów reagowania w razie wystąpienia nieprzewidzianych okoliczności. W tej perspektywie uczestnicy docenili szczególne znaczenie, jakie dla kształtu oraz efektów prac badawczych miał

ośmioetapowy model zmiany (ang. *8-Step Process For Leading Change*), który w publikacji z 1996 r.[1] zaproponował prof. John Kotter. Składa się on z ośmiu następujących po sobie etapów, które w omawianym podczas seminariów kontekście przybrały opisaną poniżej formę (celowo zachowano oryginalną formę trybu rozkazującego 2. osoby liczby pojedynczej):

1. Stwórz poczucie nieuchronności zmiany!
2. Utwórz silną koalicję na rzecz zmiany!
3. Wypracuj wizję przewodnią!
4. Rozpowszechnij jej założenia i cele!
5. Przekaż konieczne pełnomocnictwa zespołowi przewodzącemu zmianie!
6. Sformułuj plan szybkiej realizacji krótkoterminowych celów!
7. Ugruntuj osiągnięte rezultaty w celu zwiększenia wiarygodności procesu zmiany!
8. Zadbaj o utrwalenie wyników w kulturze organizacji!

Proces zmian należy rozpocząć od ustalenia czynników stanowiących źródło słabości organizacji (tj. częściowej lub całkowitej niezdolności) w zakresie realizacji celów operacyjnych. Kluczową rolę odgrywa w tym kontekście przekonanie decydentów o nieuchronności zmiany *status quo*, które zagraża organizacji bardziej niż podjęcie działań zmierzających do jego zmiany, które to działania również w nieodłączny sposób wiążą się z niepewnością. Omawiane problemy były rozważane w ramach pierwszego etapu projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości". Drugi etap procesu wdrażania zmian wymaga zaś zgromadzenia grupy osób przynależących do organizacji, posiadających dostateczną zdolność decyzyjną i podzielających oddanie wspólnej idei poprawy sytuacji, w jakiej znalazła się dana organizacja. Grupa ta, określana mianem *koalicji na rzecz zmiany*, powinna, jeśli to konieczne, posiadać zdolność do funkcjonowania poza dotychczasową hierarchią organizacji, porzucając dawne schematy postępowania. W trakcie dyskusji seminaryjnej wskazano na sieć nieformalnych powiązań jako jedno z narzędzi doboru właściwych osób. Kolejny, trzeci etap procesu poświęcono na wypracowanie nadrzędnej wizji przyszłych wysiłków na rzecz zmiany, jak również na stworzenie strategii jej realizacji. Niezbędnym

[1] J.P. Kotter, *Leading Change*, Harvard Business School Press, Boston, Mass, 1996.

elementem tego procesu jest podejmowanie nieustannych wysiłków zmierzających do jak najszerszego zakomunikowania wypracowanej wizji i strategii oraz bieżących działań podejmowanych na ich podstawie. Dzięki podejmowanym działaniom koalicja staje się naturalnym punktem odniesienia i wzorem właściwych postaw dla wszystkich pozostałych pracowników. Działania te, choć wskazane jako czwarty etap procesu, mają charakter przekrojowy i ciągły, przez co w sposób decydujący rzutują na powodzenie kolejnych faz. Etap piąty służy umocowaniu koalicji do dokonywania wszelkich zmian systemowych i strukturalnych niezbędnych do realizacji zestawu przyjętych strategii. Na tym etapie należy zadbać o usunięcie wszelkich przeszkód, co niesie za sobą m.in. konieczność marginalizacji roli odgrywanej przez oponentów zmian. Jeśli przesłanki przyświecające idei dokonania transformacji są prawidłowe, wówczas należy uznać, iż takie osoby w istocie działają na szkodę organizacji. Etapy szósty i siódmy stanowią właściwą część procesu wprowadzania zmian. Postuluje się, aby efekty wykonanej pracy były widoczne, a pracownicy odpowiednio motywowani w zamian za swoje zaangażowanie. Zdolność koalicji do dyskontowania krótkoterminowych sukcesów jest jednocześnie czynnikiem, który wpływa na zdolność organizacji do budowania wiarygodności całego procesu oraz stwarza pole do dokonywania dalszych zmian. Na ostatnim etapie transformacji należy zadbać o osadzenie wprowadzonych zmian w kontekście kultury danej organizacji. Cel ten można osiągnąć dzięki jasnemu sformułowaniu i przedstawieniu zależności między wprowadzonymi zmianami a sukcesem organizacji, który osiągnięto dzięki wprowadzonym zmianom. Strategia sukcesji – doboru następców, którzy podzielają wypracowaną wizję oraz nowy zestaw wartości organizacji – to jedna z metod, bez których nie uda się zagwarantować trwałości dokonanych zmian.

1.2. Reforma polityki bezpieczeństwa publicznego

Na podstawie założeń *modelu Kottera* dokonano wielu skomplikowanych procesów transformacji dotyczących zarówno wielkich, jak i mniejszych organizacji[2]. Jedną z nich zapoczątkowano w 2011 roku, w stolicy amerykańskiego

[2] J.P. Kotter, *Leading Cchange: Why Transformation Efforts Fail*, „Harvard Business Review", 2007, t. 85, nr 1, s. 96–103.

stanu Georgia, Atlancie. Przy pełnym zaangażowaniu tamtejszego Wydziału Policji, lokalnej społeczności oraz przedsiębiorców działających w obszarze wysokich technologii, dokonano tam bezprecedensowego procesu wdrożenia najnowocześniejszych rozwiązań technologicznych, organizacyjnych oraz prawnych na rzecz zwalczania i ograniczania przestępczości[3]. Reforma polityki zapewnienia bezpieczeństwa publicznego stanowiła podczas wszystkich czterech seminariów sektorowych przedmiot wnikliwej analizy oraz szerokiej dyskusji, które moderowała Silvia King – członkini wąskiego zespołu ekspertów przewodniczących procesowi wdrożenia zmian w Atlancie. Wykazano, że źródłem sukcesu podjętych działań było wypracowanie szerokiego konsensusu społecznego (wpisującego się w 2. etap modelu Kottera) opartego na skutecznej komunikacji społecznej dotyczącej zakresu i potencjalnych implikacji planowanych działań (etap 4. ww. modelu). Przyjęto tezę, według której bezpieczeństwo publiczne jest kluczowym czynnikiem rozwoju ekonomicznego państwa. Jego utrzymanie wymaga jednak znaczących nakładów finansowych, dzięki którym można dokonywać inwestycji w nowoczesne instrumenty zapewniające bezpieczeństwo obywatelom. Poza tym konieczne są jednak nakłady na edukację i tworzenie kultury sprzyjającej wykorzystaniu tych instrumentów.

Należy wziąć pod uwagę fakt, iż nowoczesne instrumenty zapewniające bezpieczeństwo obywatelom, jednocześnie ograniczają ich poczucie prywatności. Dla przykładu: osoby przebywające w obszarze objętym przez systemy monitoringu mogą, z jednej strony, czuć się bezpieczne, a, z drugiej strony, odczuwać dyskomfort wynikający z ciągłego pozostawania pod obserwacją. Konieczne jest zatem wypracowanie takich rozwiązań zapewniających bezpieczeństwo, które zyskają wystarczającą akceptację społeczeństwa za cenę częściowej utraty prywatności. Zagadnienia dotyczące wykorzystania nowoczesnych instrumentów technologicznych do walki z przestępczością szeroko omówiono podczas seminariów.

[3] *Atlanta Police Department: History of the APD*, b.d., http://www.atlantapd.org/about-apd/apd-history (dostęp: 31.01.2019).

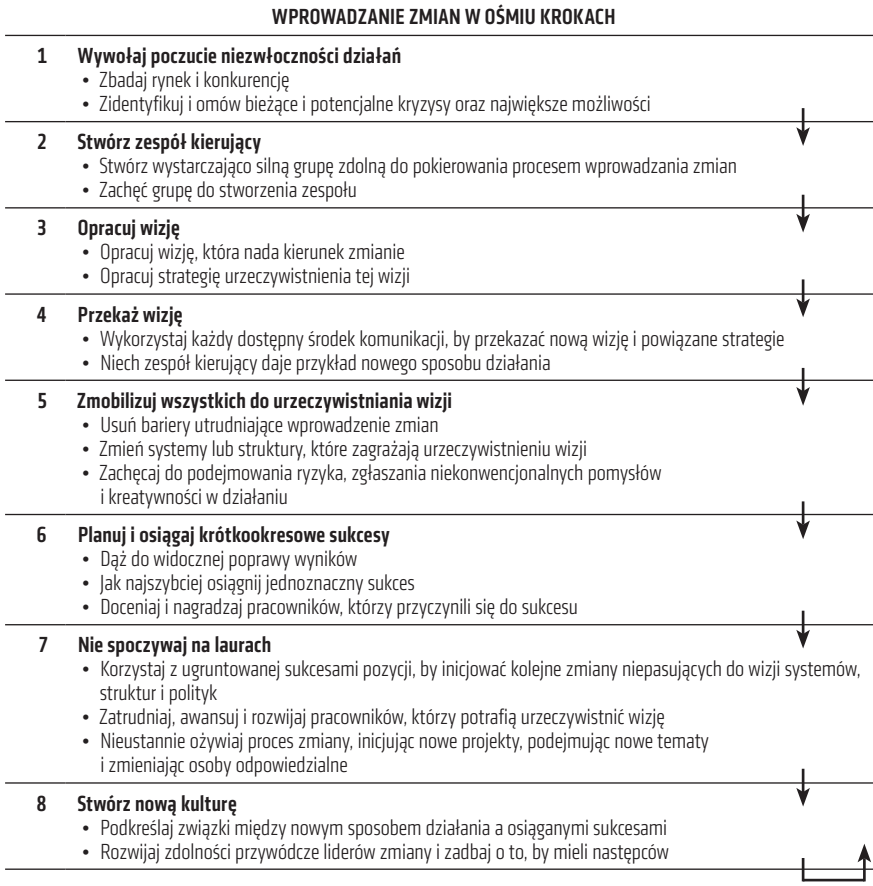
1.3. Antropologiczna teoria motywacji do przeprowadzenia zmiany

Podczas wszystkich czterech seminariów z zainteresowaniem przyjęto koncepcję zastosowania antropologicznej teorii motywacji do przeprowadzenia zmiany autorstwa profesora IESE Business School Juana Antonia Péreza Lópeza. Zgodnie z tą teorią istnieją trzy podstawowe rodzaje motywacji[4]: zewnętrzne (ang. *extrinsic*), wewnętrzne (ang. *intrinsic*) i transcendentne (ang. *transcendent*).

Motywacje zewnętrzne w przeważającej mierze opierają się na bodźcach materialnych. Pracownicy muszą za swój wysiłek otrzymać należyte wynagrodzenie, tak aby mogli spełniać swoje potrzeby materialne. Z kolei motywacje wewnętrzne zapewniają pracownikom możliwość rozwoju intelektualnego – dzięki nim podejmują określone działania nie ze względu na wynagrodzenie, ale dążąc do zaspokojenia potrzeby zdobywania wiedzy (samorealizacja). Na gruncie motywacji transcendentnych dana osoba realizuje powierzone działania nie z uwagi na własną korzyść, lecz ze względu na dobro innych ludzi. Ten rodzaj motywacji może wydawać się kontrowersyjny, ponieważ zakłada, że jedne osoby realizują określone działania, a inni ludzie są ich beneficjentami. Jednakże dyskusja podczas seminariów, a w szczególności podczas seminarium poświęconego zarządzaniu ludźmi w organizacjach, dowiodła że ten rodzaj motywacji jest również obecny w organizacjach nastawionych na osiąganie wymiernych korzyści materialnych, co z kolei wynika z faktu, iż motywacje transcendentne stanowią część ludzkiej natury, a więc występują wszędzie tam, gdzie zatrudnia się ludzi. Uczestnicy seminariów byli również zainteresowani dalszym rozwijaniem wątku motywacji transcendentnych w perspektywie wprowadzania nowych rozwiązań technologicznych, w tym sztucznej inteligencji. Jednak dyskusję na ten temat odłożono na czwarty etap seminariów organizowanych w ramach projektu, których przedmiotem będą wyzwania dotyczące promowania postaw praworządności w obliczu rozwoju technologicznego i społecznego.

[4] J.A. Pérez López, *Teoría de la acción humana en las organizaciones*, Rialp, Madrid 1991.

Rysunek 1. Model Kottera



Źródło: Kotter J.P., *Leading Change: Why Transformation Efforts Fail*, „Harvard business review", 2007, t. 85, nr 1, s. 96–103

2. Seminarium jako narzędzie badawcze

Zgodnie z założeniami projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości", przyjęta metodyka badawcza, bazująca na seminarium jako metodzie ekstrakcji wiedzy, wymagała właściwej organizacji i adekwatnego przygotowania nie tylko ze strony organizatorów i zaproszonych ekspertów, lecz również wszystkich uczestników seminariów. Wszystkie te elementy pozwoliły na przeprowadzenie kompleksowych analiz dotyczących problematyki wdrażania innowacyjnych rozwiązań zorientowanych na przeciwdziałanie przestępczości w organizacjach, co z kolei stanowiło temat przewodni seminariów zorganizowanych w listopadzie 2018 roku.

Seminaria zorganizowane w ramach niniejszego etapu prac poświęcono kwestii wdrażania w organizacjach aktywnych w sektorze energetycznym, finansowym, ubezpieczeniowym oraz obszarze zarządzania ludźmi w organizacjach zmian nastawionych na zapobieganie przyczynom przestępczości. Zakres tematyczny seminariów miał charakter uniwersalny, tj. interesujący dla przedstawicieli organizacji należących do każdego z reprezentowanych sektorów.

W następnej części niniejszego rozdziału przedstawiono zakres zagadnień poruszanych w ramach poszczególnych paneli seminariów; następna część zawiera natomiast opis kompetencji zaproszonych ekspertów, a także ocenę treści merytorycznej wystąpień, jak również organizacji seminariów dokonaną na podstawie oceny uczestników.

2.1. Faza wstępna

Faza wstępna przeprowadzonych prac badawczych objęła szereg czynności o charakterze organizacyjnym i koncepcyjnym dotyczących działań przygotowawczych. Sformułowanie przeznaczonych dla uczestników zaleceń miało na celu ułatwienie przeprowadzenia indywidualnych działań przygotowawczych przed rozpoczęciem dyskusji oraz analizy złożonej problematyki, z jaką mamy do czynienia w przypadku kwestii wdrażania nowatorskich rozwiązań. Z uwagi na wieloaspektowy charakter rozważanej tematyki, zarówno zalecenia, jak i wybór materiałów przygotowawczych miały za zadanie zainteresować i skłonić uczestników do przeprowadzenia gruntownej analizy indywidualnej uwzględniającej możliwie wszystkie aspekty rozważanej tematyki.

2.1.1. Wybór studium przypadku

Proces wdrażania zmian w organizacjach jest jednym z najbardziej krytycznych elementów w funkcjonowaniu przedsiębiorstwa. Z uwagi na istotę rozważanych zagadnień, zaproszeni eksperci dokonali selekcji studiów przypadków oraz innych materiałów pomocniczych opierając się na standardach najbardziej uznanych szkół biznesu, takich jak IESE Business School. W procesie selekcji wyłoniono trzy studia przypadków poruszające w szerokim ujęciu tematykę wdrażania zmian w organizacjach, przy uwzględnieniu zróżnicowanych uwarunkowań charakteryzujących sektor operacyjny przedsiębiorstwa. Studium przypadku *Cythia Carrol at Anglo American*[5] bezpośrednio dotyka problematyki procesu wdrażania zmian mających na celu promowanie postaw praworządności w organizacji oraz powiązanych z nimi barier i problemów. Problem eliminacji barier został bardziej szczegółowo poruszony w historii przypadku *Jerry Sanders*[6], na podstawie której uczestnicy mogli zapoznać się z wykorzystaniem sieci nieformalnych do wprowadzania zmian. Ostatnim z wybranych studiów przypadków był

[5] G. Mukunda, L. Mazzanti, A. Sesia, *Cynthia Carroll at Anglo American (A)*, 2013, Harvard Business School Case 414–019.

[6] M.D. Burton, K. Lawrence, *Jerry Sanders*, „Harvard Business Review Case Study", 1998, Leadership & Managing People, s. 18.

Shouldice Hospital[7] poruszający problematykę zarządzania operacjami jako krytycznego elementu nie tylko w funkcjonowaniu organizacji, ale również integralnej części procesu wprowadzania zmian. Wybrane przez ekspertów studia przypadków dla grup złożonych z przedstawicieli poszczególnych sektorów zostały zawarte w poniższej tabeli (zob. tabela 1).

Tabela 1. Spis studiów przypadków wybranych przez zaproszonych ekspertów dla grup złożonych z reprezentantów poszczególnych sektorów

SEKTOR	STUDIUM PRZYPADKU
SEKTOR FINANSOWY	• *Cynthia Carroll at Anglo American (A)*
SEKTOR UBEZPIECZEŃ	
SEKTOR ENERGETYKI	• *Jerry Sanders*
ZARZĄDZANIE LUDŹMI W ORGANIZACJACH	• *Jerry Sanders* • *Shouldice Hospital*

Odniesienia do wybranych studiów przypadków można znaleźć w rozdziale poświęconym tematyce seminariów (zob. rozdział 2.2.6).

2.1.2. Indywidualna analiza studium przypadku

Z uwagi na wysoki poziom złożoności omawianej podczas seminariów tematyki, zaproszeni eksperci stworzyli szereg zaleceń przeznaczonych dla uczestników, które pełniły funkcję pomocniczą podczas procesu samodzielnej analizy wybranych studiów przypadków. Ten kluczowy dla powodzenia prac badawczych proces zmierzał do tego, aby uczestnicy opanowali odpowiedni warsztat pojęciowy – warunek niezbędny do prowadzenia dyskusji w trakcie seminariów. Podczas formułowania poszczególnych zaleceń położono szczególny nacisk na analizę jakościową problematyki poruszanej przez wybrane studia przypadków. W szczególności stworzono listę pytań pomocniczych dotyczących sieci nieformalnych i ich roli w procesie wprowadzania zmian, co z kolei miało zwrócić uwagę uczestników na różnorodność przeszkód pojawiających się w trakcie procesu wprowadzania zmian. Prof. Massimo

[7] J.L. Heskett, *Shouldice Hospital Limited*, 1983, Harvard Business School Case 683–068.

Maoret zalecił również lekturę uzupełniającą w obszarze modelu zarządzania zmianą, aby umożliwić uczestnikom wypracowanie właściwego warsztatu pojęciowego.

2.2. Seminaria

Założenia organizacyjne i przebieg seminariów w ramach etapu listopadowego nie odbiegały od formuły przyjętej na potrzeby wcześniejszych części. Etapy pracy oraz cele analizy przeprowadzonej przez uczestników zostały uwzględnione w rozdziałach 2.2.1–2.2.4. W rozdziałach 2.2.5 oraz 2.2.6 zawarto odpowiednio opis kompetencji zaproszonych ekspertów i zakres tematyczny seminariów z uwzględnieniem poszczególnych paneli tematycznych.

2.2.1. Praca w grupach

W ramach listopadowego etapu prac uczestnicy mieli możliwość lepszego zrozumienia procesów zachodzących podczas zarządzania operacjami w ramach gry strategicznej, opracowanej przez zespół wykładowców IESE Business School, znanej pod nazwą *Lego Game*. Uczestników podzielono na dwie grupy: członkowie jednej z nich wcielili się w role pracowników szczebla produkcyjnego, członkowie drugiej w role menedżerów fabryki, sprawujący nadzór nad przebiegiem procesu produkcji. Prof. Adrian Done zadbał o prawidłowy przebieg ćwiczenia, którego zadaniem było m.in. uświadomienie uczestnikom różnic w postrzeganiu łańcucha wartości organizacji w zależności od pełnionej funkcji. Wnioski i spostrzeżenia uczestników symulacji stały się przedmiotem dyskusji i wnikliwej analizy grup plenarnych.

W ramach pracy grupowej uczestnicy dokonali ponadto wspólnej analizy problematyki wdrażania zmian w organizacjach, którą poprzedziło stosowne wprowadzenie prof. Done'a. Omówiono zestaw typowych problemów, z którymi mierzą się organizacje usiłujące wdrożyć innowacje na rzecz zapobiegania przyczynom przestępczości. Podobnie jak w przypadku wcześniejszych etapów projektu, uczestników podzielono na grupy liczące nie więcej niż 9 osób, aby optymalne wykorzystać doświadczenie i potencjał każdego uczestnika na potrzeby prowadzonych badań.

2.2.2. Praca w grupach nad studium przypadku

Jednym z elementów pracy w grupach była wspólna analiza problematyki wdrażania metod zapobiegania przestępczości w organizacjach na gruncie wybranych studiów przypadku. Właściwe przygotowanie uczestników do pracy grupowej było efektem przeprowadzonej przez każdego z uczestników indywidualnej analizy poszczególnych studiów przypadków, której wyniki zaprezentowali poszczególni uczestnicy. Dla zapewnienia warunków sprzyjających swobodnej wymianie poglądów, uczestnicy zostali podzieleni na małe grupy liczące od 5 do 9 osób. Wykorzystanie wszechstronnego doświadczenia i kompetencji wszystkich uczestników zmierzało do zapewnienia dokładności i całościowości przeprowadzonej analizy poprzez porównanie wniosków wynikających z analizy poszczególnych studiów przypadków dokonanej przez każdego z uczestników. Warto pokreślić, że dyskusja, którą przeprowadzono podczas niniejszego etapu i w ramach której na każdy z wybranych studiów przypadków poświęcono ok. 30 min., nie była nastawiona na wypracowanie przez wszystkich uczestników wspólnego stanowiska, lecz stanowiła etap przygotowawczy do analizy przeprowadzonej w ramach dyskusji plenarnej.

2.2.3. Praca w grupach plenarnych

Wnioski i spostrzeżenia uczestników sformułowane na podstawie doświadczeń zdobytych w trakcie gry symulacyjnej *Lego Game* zasadniczo stanowiły przedmiot dyskusji i wnikliwej analizy w ramach pracy w grupach plenarnych. Z uwagi na wieloaspektowy charakter przeprowadzonego ćwiczenia, dyskusja dotyczyła szeregu czynników mających wpływ na efektywność funkcjonowania organizacji i ich zdolność do absorbowania zmian. Pośród nich znalazły się takie zagadnienia, jak mechanizmy kształtowania się nieformalnych sieci powiązań, współpracy między pracownikami różnych szczebli w hierarchii organizacyjnej, mechanizmów budowania koalicji na rzecz zmian, jak również metod osiągania optymalnego wykorzystania zasobów na rzecz właściwego ukierunkowania procesu wprowadzania zmian i innowacji.

Dyskusja plenarna była ponadto zwieńczeniem przeprowadzonych wcześniej analiz, włączając w to pracę grupową nad studiami przypadków oraz

innymi zagadnieniami, a także wyniki pracy indywidualnej uczestników. Aby zapewnić sprawny przebieg dyskusji, zaproszeni eksperci pełnili role moderatorów, a także służyli swoją wiedzą ekspercką w zakresie obecnie panujących na świecie trendów dotyczących wdrażania metod przeciwdziałania przestępczości. Połączenie różnorodnych doświadczeń i spostrzeżeń uczestników ze wszystkich grup seminaryjnych pozwoliło na kompleksową analizę złożonych zagadnień, co nie byłoby możliwe bez odpowiedniego przygotowania uczestników na wcześniejszych etapach pracy grupowej. Rezultatem opartej na studium przypadku analizy było opracowanie wniosków i zaleceń końcowych dotyczących procesu wprowadzania zmian w organizacjach, które z kolei zostały podsumowane w dalszych rozdziałach tego raportu (zob. rozdziały 2.3.3 i 3). Zważywszy na tematykę seminariów realizowanych w ramach trzeciego etapu projektu, przedstawione studia przypadków miały na celu przeprowadzenie analizy czynników wpływających na proces wdrażania metod zapobiegających przestępczości w instytucjach publicznych i przedsiębiorstwach. Wybrane studia przypadków dotyczyły konkretnych, autentycznych historii wdrażania zmian, które charakteryzuje szczególna konfiguracja oryginalnych czynników i okoliczności wpływających na podejmowane decyzje, zachowania oraz motywację osób zaangażowanych w daną sytuację, wartości zaangażowanych środków finansowych itd. Tym samym, celem przywołanych historii było przedstawienie problematyki złożoności czynników decyzyjnych i nakreślenie metodologii podejmowania decyzji w zakresie wdrażania innowacyjnych rozwiązań w organizacjach, co pozwoliło na wypracowanie metodyki poszukiwania rozwiązań dla problemów podobnych do tych, które przedstawiono w wybranych studiach przypadków.

2.2.4. Dyskusja panelowa

Kolejnym elementem przeprowadzonych seminariów była dyskusja panelowa mająca na celu przedstawienie oraz analizę skutecznych sposobów wdrożenia metod i instrumentów zapobiegania przestępczości w Polsce. Pierwszy etap dyskusji miał na celu przybliżenie uczestnikom seminariów problematyki skutecznego wdrażania zmian w organizacjach na rzecz przeciwdziałania przestępczości poprzez zastosowanie uznanej metodyki wprowadzania zmian

opartej na *modelu Kottera*. Przedstawiona metodyka została następnie omówiona na przykładzie reformy polityki bezpieczeństwa w Atlancie, stolicy amerykańskiego stanu Georgia, obejmującej najnowocześniejsze rozwiązania technologiczne, organizacyjne i prawne na rzecz zwalczania i ograniczania przestępczości. Drugi etap panelu dyskusyjnego poświęcono analizie skutecznego sposobu wdrażania zmian na gruncie omawianej metodyki i jej zastosowania w kontekście występujących w Polsce uwarunkowań społeczno-kulturowych. Odpowiedzi panelistów na pytania zadawane przez uczestników pozwoliły pogłębić tematykę, sprostować zaistniałe niejednoznaczności oraz dokonać analizy skuteczności zaproponowanej metodyki wdrażania zmian za pomocą wspólnej dyskusji ekspertów i uczestników.

2.2.5. Profile prelegentów

W niniejszym rozdziale zaprezentowano sylwetki zaproszonych ekspertów ze szczególnym uwzględnieniem ich kompetencji i doświadczenia, w tym udokumentowanego dorobku naukowego.

Do udziału w wykładach zaproszono wybitnych ekspertów z różnych dziedzin o ugruntowanej międzynarodowej pozycji w obszarze nauki i praktyki gospodarczej. Ich dokonania są powszechnie znane i doceniane. Wszyscy pracowali na rzecz rządów lub międzynarodowej praktyki gospodarczej. Wielu z nich wykłada na czołowych uniwersytetach na świecie. W poniższym rozdziale zawarto skrócony opis kompetencji i biogramy prelegentów. Opis szczegółowy i listy wybranych publikacji, zamieszczono w załączniku (zob. załącznik A).

Adrian Done

Biogram prof. Done'a można znaleźć w raporcie z seminariów październikowych pt. „Raport z przeprowadzenia badań wraz z organizacją seminariów w zakresie zapobiegania przyczynom przestępczości: metody zapobiegania przestępczości".

Silvia King

Biogram dr King został znajduje się w raporcie z seminariów wrześniowych pt. „Raport z przeprowadzenia badań wraz z organizacją seminariów

w zakresie zapobiegania przyczynom przestępczości: identyfikacja przyczyn przestępczości w wybranych obszarach gospodarki w Polsce i na świecie".

Massimo Maoret

Massimo Maoret pełni funkcję adiunkta (*Assistant Professor*) w Katedrze Zarządzania Strategicznego (*Strategic Management Department*) IESE Business School, gdzie prowadzi programy z zakresu strategii konkurencyjnej, wdrażania strategii, teorii organizacji i zarządzania zmianą organizacji.

Jego zainteresowania badawcze koncentrują się wokół zagadnienia sieci nieformalnych powiązań (ang. *social networks*) oraz ich wpływu na produktywność (także wynik finansowy) małych, średnich i dużych organizacji (lecz również drużyn sportowych czy formacji wojskowych). Jest indywidualnym stypendystą programu grantów badawczych Komisji Europejskiej im. Marii Skłodowskiej-Curie (*European Commission Marie Skłodowska-Curie Fellow*). Uzyskał stopień doktora nauk o zarządzaniu (*Ph.D. in Management*) z Boston College (Massachusetts, USA) w 2013 roku, (M.S.) z dziedziny nauk o organizacji (*Organization Science*) z tego samego uniwersytetu oraz *Laurea Specialistica* z obszaru nauk komputerowych i zarządzania z Universita' di Bologna.

Lucien Randazzese

Dr Randazzese pełni funkcję dyrektora Center for Innovation Strategy and Policy w SRI International. Posiada dwadzieścia lat doświadczenia badawczego w zakresie polityki naukowej i technologicznej, ekonomiki i innowacji w badaniach naukowych oraz strategii i planowania w biznesie. Brał udział w projektach dla sektora prywatnego, rządowego oraz akademickiego z Ameryki Północnej, Europy, Azji i Bliskiego Wschodu.

W swojej pracy koncentruje się na pomaganiu organizacjom w optymalizacji procesów inwestycyjnych i zarządczych związanych z nauką i technologią. Jako lider zespołów projektowych opracowywał regionalne strategie przeprowadzania badań naukowych, pomagał tworzyć strategie o krajowym zasięgu w zakresie nauki, technologii i innowacji (ang. *Science, Technology and Innovation*, STI), a także przygotowywał plany biznesowe i dokonywał ich oceny dla licznych podmiotów. W pracach poświęconych zrozumieniu procesu rozwoju technologii posługiwał się m.in. zaawansowaną tekstową

analizą eksploracyjną (ang. *text mining*), wykorzystując techniki uczenia maszynowego.

Karierę rozpoczął jako inżynier mikroelektronik w firmie International Business Machines Corporation (IBM). Przed dołączeniem do zespołu SRI International, dr Randazzese zajmował się doradztwem strategicznym, pracując w sektorze telekomunikacyjnym, energetycznym, medialnym, cyberbezpieczeństwa, inżynierii oprogramowania oraz finansowym, które mierzyły się w owym czasie z wyzwaniami związanymi z gwałtownym postępem technologicznym. Wcześniej był pracownikiem naukowym Uniwersytetu Harvarda (Massachusetts, USA).

Otrzymał stopień doktora inżynierii i polityki publicznej z Carnegie Mellon University. Za swoją dysertację został uhonorowany nagrodą *Herbert A. Simon Doctoral Dissertation Award in Behavioral Research*. Posiada tytuł bakałarza mikroelektroniki, który uzyskał na Rochester Institute of Technology.

2.2.6. Zakres tematyczny seminariów

W zakresie merytorycznym każde z seminariów zostało podzielone na szereg następujących po sobie części, określonych mianem paneli tematycznych. Poniżej zawarto szczegółowy opis każdego z nich.

Managing operations: simulation exercise

W ramach tego panelu uczestnicy wzięli udział w ćwiczeniu symulacyjnym określanym przez IESE Business School mianem *Lego Game*. Ćwiczenie polegało na składaniu klocków Lego® według określonego planu produkcji w taki sposób, aby otrzymać wskazany produkt finalny. Wykonywane przez uczestników czynności były symulacją procesu zachodzącego na linii produkcyjnej i obiegu dokumentów w organizacji, która to symulacja w praktyce pozwoliła zaobserwować funkcjonowanie elementów metodologii *Lean Management* na przykładzie prostego procesu biznesowego, jak również przeanalizować wpływ zajmowanego w organizacji stanowiska na postrzeganie określonego problemu. Wykazano, iż wymiana informacji między zarządzającymi organizacją a osobami zajmującymi niższe szczeble w hierarchii pracowniczej jest konieczna dla zapewnienia efektywności procesów biznesowych (łańcucha

wartości), która z kolei w istotny sposób wpływa na skalę możliwych nadużyć (powierzchni ataku na organizację). Wprowadzono alternatywną definicję zarządzania jakością jako przekrojowego wysiłku całej organizacji w celu wytworzenia i dostarczenia produktu pożądanej jakości, w przeciwieństwie do jego powszechnej, lecz błędnej, interpretacji jako wydzielonej komórki w strukturze organizacji.

Uczestnicy seminariów poświęconych sektorowi finansowemu, ubezpieczeniowemu, energetycznemu i zarządzaniu ludźmi w organizacjach podkreślali, że w ich organizacjach występują ścisłe procedury mające na celu ograniczenie przestępczości, w tym kradzieży, oszustw, obniżania jakości produktów i usług itp. Symulacja wykazała jednak, że nawet w przypadku prostych procesów biznesowych występują błędy wynikające nie z celowego działania, lecz z braku pełnego zrozumienia poszczególnych procesów (przede wszystkim operacyjnych). We wszystkich czterech grupach seminaryjnych uczestnicy symulacji podejmowali decyzje mające na celu usprawnienie procesu operacyjnego, a które tak naprawdę jeszcze bardziej go komplikowały. Dopiero przeprowadzenie kilku iteracji, symulacji pozwoliło uczestnikom – którymi, dla przypomnienia, byli doświadczeni menedżerowie i urzędnicy – dostrzec swoje błędy i przeprowadzić faktyczne działania naprawcze.

Symulacja uświadomiła uczestnikom seminariów następujące fakty:

1. W okresie wdrożeń nowych rozwiązań nie jest możliwe pełne zrozumienie procesów zachodzących w organizacji. Dochodzi wówczas do niemożliwych do przewidzenia sytuacji, które mogą skutkować nadużyciami – w przypadku niepodjęcia działań zaradczych prowadzą one do stałej niegospodarności, a w skrajnych przypadkach do celowych kradzieży, oszustw etc.
2. Im bardziej skomplikowane są proces produkcyjny i obieg dokumentów, tym trudniej jest je kontrolować i tym łatwiej dochodzi do przestępstw przeciwko mieniu organizacji. Należy więc dążyć do ciągłego obniżania kosztów i ograniczania przestrzeni do nadużyć w drodze maksymalnego możliwego upraszczania procesów operacyjnych.
3. Wydzielenie w organizacji komórki odpowiedzialnej za kontrolę jakości może prowadzić do zdjęcia odpowiedzialności za jakość produktu z innych pracowników zaangażowanych w realizację łańcucha wartości organizacji. Innymi słowy, wśród pracowników dochodzi do

wytworzenia fałszywego przekonania o panowaniu nad utrzymaniem wysokiej jakości produkcji (produktu materialnego, usługi), podczas gdy w rzeczywistości jakość produktów jest co najwyżej średnia, a koszt jej utrzymania – wysoki. Wniosek o zastąpienie wydzielonej komórki odpowiedzialnej za kontrolę jakości dzięki samodyscyplinie wszystkich pracowników organizacji wywołał początkowo kontrowersje wśród uczestników seminariów. Jednak w części podsumowującej grę symulacyjną wszyscy uczestnicy zgodzili się, że jest to rozwiązanie optymalne.

4. Pełniejsze wykorzystanie zasobów organizacji skutkuje ograniczeniem możliwości popełniania przestępstw przez jej pracowników. Dzieje się tak w wyniku uproszczenia mechanizmów kontroli nad poszczególnymi etapami produkcji i ułatwienia nadzoru nad pracownikami odpowiedzialnymi za ich realizację.

Wdrożenie w organizacji zmian wynikających z wniosków z *Lego Game* może okazać się uciążliwe ze względu na konieczność redukcji zasobów zaangażowanych w ramach procesów operacyjnych. Ograniczeniu podlegać może liczba zatrudnionych pracowników, ilość materiałów potrzebnych do produkcji etc., co z kolei prowadzi do utraty korzyści wynikających z wykorzystania nieefektywności organizacji i czerpanych przez zaangażowane w taki proceder podmioty.

Leading organizational change / developing a change strategy

Panel poświęcony został analizie typowych problemów, z którymi borykają się organizacje podejmujące wysiłki na rzecz wprowadzenia istotnych zmian w zakresie modelu czy też sposobu ich funkcjonowania (implementacji nowej strategii lub strategii naprawczej). Wprowadzono model zarządzania zmianą, którego wdrożenie pozwoliło na udane przeprowadzenie skomplikowanych transformacji organizacyjnych, tzw. *model Kottera*. Wśród najważniejszych elementów strategii na rzecz transformacji wskazano potrzebę wykreowania wśród pracowników organizacji poczucia konieczności, a nawet nieuchronności zmian oraz zasadniczą rolę lidera, który inspiruje pozostałe osoby, objaśniając im powody, cele oraz główne założenia przeprowadzanej transformacji.

Panel ten został poprowadzony przez prof. Massima Maoreta na podstawie studium przypadku zatytułowanego *Cynthia Carroll at Anglo American*[8]. Przedmiotem studium był przypadek korporacji Anglo American PLC, globalnej firmy wydobywczej z siedzibą w Londynie, która w 2007 roku stanęła w obliczu kryzysu wskutek wciąż rosnącej liczby śmiertelnych wypadków górników pracujących w należących do niej kopalniach. Z tym poważnym problemem, średnio 46 zgonami rocznie w latach 2002–2006, nie zmagały się wyłącznie kopalnie należące do Anglo American, ale całej branży wydobywczej. Nowo zatrudniona dyrektor generalna Anglo American, Cynthia Carroll, nie miała wątpliwości, że wbrew powszechnie panującej w branży opinii dotyczącej nieuchronności incydentów bezpieczeństwa, zredukowanie liczby obrażeń i zgonów wśród pracowników powinno być najwyższym priorytetem zarządu. Szczególny charakter omawianemu problemowi nadał fakt, że Anglo American jest korporacją, która w przeszłości czerpała korzyści z polityki segregacji rasowej (apartheidu), a większość jej pracowników zatrudnionych w tym czasie na stanowiskach niekierowniczych była czarnoskóra.

W ramach dyskusji na gruncie tego studium przypadku uczestnicy seminariów wskazywali na następujące problemy:

1. Istnieje samoistny konflikt interesu między dążeniem do osiągnięcia jak najlepszego wyniku finansowego przedsiębiorstwa a nieuchronnością poniesienia kosztów na rzecz zapewnienia bezpieczeństwa pracowników.
2. Problem, który napotkała organizacja, nie jest odosobniony – w porównywalnym stopniu dotyczył on każdej firmy przynależącej do sektora.
3. Wieloletnia tradycja firmy i sektora, do którego firma przynależy, może być źródłem silnego oporu zespołu pracowniczego względem wprowadzania jakichkolwiek zmian.
4. Pomimo długoletniego istnienia programów na rzecz zwiększania bezpieczeństwa pracowników w kopalniach, dokonujący się w tej dziedzinie postęp nie był wystarczający. Decydenci nie byli przy tym dostatecznie zdeterminowani, aby za wszelką cenę osiągnąć zakładane, pożądane miary efektywności działań podejmowanych na rzecz bezpieczeństwa pracowników.

[8] G. Mukunda, L. Mazzanti, A. Sesia, *Cynthia Carroll at Anglo American (A)*…, op. cit.

Uczestnicy zgodnie stwierdzili, że do przedstawionego w studium przypadku problemu bezpieczeństwa pracowników można podejść na trzy sposoby, a mianowicie:

1. Zaakceptować dotychczasowy stan rzeczy, nie podejmując żadnych dodatkowych działań na rzecz bezpieczeństwa pracowników.
2. Podjąć działania zmierzające do zapewnienia pracownikom dodatkowego zabezpieczenia przy jednoczesnym zachowaniu ciągłości operacyjnej organizacji (ang. *business continuity)*.
3. Zawiesić działalność operacyjną do czasu znalezienia przyczyn złego stanu bezpieczeństwa pracowników i wdrożenia koniecznych zmian.

Należy podkreślić, iż w trakcie seminarium dla sektora energetycznego uczestnicy zwrócili przede wszystkim uwagę na wysokie koszty zawieszenia operacji takiego przedsiębiorstwa jak kopalnia. Zgodnie z obserwacją uczestników podobna decyzja musiałaby skutkować koniecznością ewakuacji całego oprzyrządowania z wyrobiska, a przyszłe wznowienie prac wymagałoby ponownego przeprowadzenia kosztownych badań geologicznych w związku z dynamicznie kształtującą się w czasie stabilnością wyrobiska. Uczestnicy seminarium dla sektora finansowego doszli do wniosku, iż zawieszenie działalności operacyjnej mogłoby skutkować zaburzeniem równowagi rynkowej przedsiębiorstwa i utratą jego przewagi konkurencyjnej nad innymi przedsiębiorstwami.

Na podstawie analizy studium przypadku opracowano następujące wnioski:

1. Zmiana kultury organizacji może w pewnych warunkach wymagać zmiany kultury całego sektora.
2. Członków koalicji na rzecz budowania zmiany należy poszukiwać także wśród menedżerów/kierowników średniego szczebla, ponieważ to oni mają realny wpływ na kształtowanie kultury organizacji wśród podległych im pracowników.
3. Często dzieje się tak, że to pracownicy niższego szczebla posiadają kluczowe informacje, które mogą pomóc właściwie ukierunkować pracę zarządu.

4. Działalność każdej organizacji musi zawsze opierać się na poszanowaniu praw człowieka. W rozważanym przypadku doszło do naruszenia najwyższego z praw człowieka – tj. prawa do życia[9].

Getting things done: power and networks / Visualizing and understanding your network / Mastering organizational networks / Leveraging informal networks to implement change

Przeprowadzone w ramach niniejszego panelu prace poświęcono identyfikacji wpływu nieformalnych sieci funkcjonujących w ramach organizacji na działalność operacyjną tej organizacji. W szczególności skupiono się na wykorzystaniu sieci nieformalnych jako narzędzia wprowadzania zmian na rzecz przeciwdziałania przestępczości w organizacjach, na czym w bezpośredni sposób skupia się również etap opracowany w ramach *modelu Kottera*, tj. budowanie koalicji przewodzącej wprowadzaniu zmian.

W pierwszej, prowadzonej przez uznanego specjalistę ds. sieci nieformalnych prof. Massima Maoreta części, wprowadzono pojęcie sieci nieformalnej, zastrzegając że w procesie wprowadzania zmian i zarządzania organizacją sieć ta może stanowić zarówno barierę, jak i ułatwienie. Treści zaprezentowane przez zaproszonego eksperta objęły wykorzystanie dwóch typów sieci nieformalnych – sieci zaufania oraz sieci eksperckiej – jako narzędzi do wywierania wpływu na rzecz wprowadzania zmian. Mają one na celu przeciwdziałanie przestępczości oraz mechanizmom powstawania powiązań opartych na tendencji jednostki do preferowania osób wykazujących cechy podobne (ang. *homophily*)[10]. Przedstawiono ponadto problematykę postrzegania sieci powiązań jako ważnego czynnika wpływającego na zdolność operacyjną poszczególnych pracowników i, w konsekwencji, całej organizacji. Wprowadzono również klasyfikacje istniejących sieci z uwagi na ich system powiązań (sieci zamknięte i otwarte). Elementem końcowym wprowadzenia tematyki sieci nieformalnych było ćwiczenie angażujące uczestników w samodzielną analizę własnej sieci powiązań nieformalnych.

---

[9] *A/RES/3/217 A – Universal Declaration of Human Rights – UN Documents: Gathering a Body of Global Agreements*, b.d., http://www.un-documents.net/a3r217a.htm (dostęp: 9.02.2019).

[10] M. McPherson, L. Smith-Lovin, J.M. Cook, *Birds of a Feather: Homophily in Social Networks*, „Annual Review of Sociology", 2001, t.27, nr 1, s. 415–444.

W ramach drugiej części panelu rola sieci nieformalnych została przedstawiona za pomocą wybranego studium przypadku (zob. tabela 1). Studium przypadku *Jerry Sanders*[11] dotyczy historii tytułowego bohatera: odnoszącego sukcesy biznesmena zmagającego się aktualnie z kwestią dalszego rozwoju organizacji *San Francisco Science*, której jest współzałożycielem. Wybrana historia zawiera opis rozwoju kariery zawodowej oraz kompetencji tytułowego bohatera posiadającego bardzo wszechstronne doświadczenie, począwszy od służby w armii izraelskiej, poprzez pracę jako prawnik, aż do objęcia stanowiska prezesa własnej firmy specjalizującej się w produkcji innowacyjnego sprzętu medycznego. Każdy etap kariery Jerry'ego Sandersa jest związany z tworzeniem nowych połączeń w ramach swoich sieci powiązań. Skutkuje to budową rozległej, otwartej sieci powiązań nieformalnych, która leży u podstaw założenia *San Francisco Science*, organizacji będącej platformą pozwalającą na łączenie kompetencji świata nauki i biznesu. W ramach niniejszego panelu skupiono się na sieci utworzonej przez Jerry'ego Sandersa jako przykładzie obrazującym rolę powiązań nieformalnych w karierze zawodowej oraz wdrażaniu zmian.

Na podstawie niniejszego panelu uczestnicy sformułowali następujące wnioski:

- analiza sieci nieformalnych w organizacji jest kluczowym elementem wprowadzania nowych rozwiązań i budowania koalicji na rzecz zmian;
- sieci nieformalne mogą być skutecznym narzędziem zarządzania organizacją;
- sieci zamknięte poprzez istniejące współzależności między poszczególnymi członkami sprzyjają powstawaniu nadużyć i nieprawidłowości;
- budowanie sieci powiązań stanowi istotny element rozwoju personalnego i kompetencji jednostki;
- analiza sieci nieformalnych jest ponadto użyteczna w kontekście identyfikacji grup przestępczych i osób charakteryzujących się wyższą skłonnością do popełniania nadużyć;
- znajomość nieformalnej sieci powiązań w organizacji determinuje zdolność poszczególnych pracowników (a w konsekwencji całej organizacji) do realizacji zadań operacyjnych, przy czym relacje przyjaźni

[11] M.D. Burton, K. Lawrence, *Jerry Sanders*…, op. cit.

rzutują w decydujący sposób na dobór współpracowników do realizacji powierzonych zadań,
- sieci powiązań nie są stabilne, lecz zmieniają się w czasie, w związku z czym analiza sieci jest procesem ciągłym i wymagającym stałego monitorowania.

Ponadto uczestnicy seminarium przeznaczonego dla sektora energetycznego zwrócili uwagę na duże znaczenie struktury hierarchicznej w organizacji, gdzie proces podejmowania istotnych decyzji opiera się na modelu kaskadowym. Pomimo, iż uczestnicy pozostałych trzech seminariów sektorowych nie stwierdzili występowania podobnych uwarunkowań w rozważanym obszarze, wszyscy zgodnie stwierdzili, że struktura formalna organizacji stanowi istotną barierę w procesie wdrażania zmian. Zgodnie z opinią zaproszonego eksperta odpowiednie zarządzanie siecią powiązań nieformalnych stanowi metodę zwiększenia sprawności procesu decyzyjnego, przy czym dzieje się tak nawet w organizacjach charakteryzujących się strukturą pionową. Ponadto właściwe funkcjonowanie struktur nieformalnych w organizacjach, w tym zapewnienie odpowiedniej edukacji i świadome zarządzanie siecią relacji międzyludzkich, pozwala na promowanie postaw praworządności, co z kolei zmniejsza ryzyko przestępstw o charakterze wewnętrznym.

Uczestnicy seminarium dla obszaru zarządzania ludźmi zwrócili też uwagę na fakt, iż nieformalne relacje pracowników organizacji mogą również stanowić barierę podczas procesu wdrażania zmian. Niekiedy emocje i osobiste uprzedzenia mogą prowadzić do nieetycznych, a nawet sprzecznych z prawem zachowań, których celem jest przeciwdziałanie wprowadzanym zmianom. Dlatego też istotnym elementem budowania koalicji jest analiza struktury organizacji pod kątem istniejących sieci nieformalnych w celu ich identyfikacji i wykorzystania jako narzędzia ułatwiające proces wdrażania zmian.

The challenges of future cities / Leadership in future cities

Panel poświęcono koncepcji *inteligentnych miast* (ang. *smart cities*) jako przykładowi wdrażania rozwiązań z zakresu przeciwdziałania przestępczości. W ramach części wprowadzającej, doktor Lucien Randazzese z SRI International zaznajomił uczestników z tematyką rozwoju aglomeracji dzięki wykorzystaniu nowoczesnych technologii opartych w przeważającej mierze na paradygmacie analizy wielkiej ilości różnorodnych danych (*Big Data*)

i wykorzystaniu sztucznej inteligencji. Dodatkowo, na przykładzie projektów w obszarze inteligentnych miast przedstawiono problematykę wdrażania szeroko zakrojonych działań na rzecz przeciwdziałania przestępczości i wymaganych czynników inicjujących konieczność wprowadzenia zmian. W ramach panelu poruszono również kwestie związane z wdrażaniem rozwiązań w kontekście wyzwań natury regulacyjnej, organizacyjnej i etycznej, z którymi muszą liczyć się decydenci zaangażowani w obszarze wdrożeń nowych technologii, co omówiono na przykładzie rozwiązań wdrażanych obecnie przez SRI International. Część dyskusji poświęcono koncepcji inteligentnych miast jako potencjalnemu narzędziu służącemu przeciwdziałaniu przestępczości.

Na podstawie niniejszego panelu uczestnicy sformułowali następujące wnioski:

- szeroko zakrojone działania wymagają szerokiego zaangażowania i poparcia wszystkich osób, których dotyczy wdrażane rozwiązanie;
- wdrażanie rozwiązań opartych na innowacyjnych technologiach wymaga uwzględnienia w wizji strategicznej kwestii etycznych i regulacyjnych, w tym problemów związanych z odpowiedzialnością za decyzje podejmowane wskutek działań sztucznej inteligencji;
- mniejsze inicjatywy mogą być punktem wyjścia do przeprowadzenia większych zmian. Przykładem mogą być lokalne inicjatywy, które niewielkimi, za to mierzalnymi wynikami zachęcają do wprowadzania projektów o większym zasięgu;
- lokalne inicjatywy mogą ponadto być elementem, który posłuży do stworzenia koalicji na rzecz zmian poprzez wstępną identyfikację osób proaktywnych i zaangażowanych w działania społeczne;
- inteligentne miasta, poprzez przeciwdziałanie nierównościom społecznym i promowanie postaw praworządności, mogą przyczynić się do redukcji liczby popełnianych przestępstw;
- zaletą koncepcji inteligentnych miast jest wysoki poziom zintegrowania baz danych dotyczących przestępstw, co może przyczynić się do usprawnienia działań zapobiegawczych w rozważanym obszarze;
- istniejąca i wciąż rozwijana infrastruktura komunikacyjno-informacyjna aglomeracji miejskich pozwala na wdrożenie skutecznych rozwiązań na rzecz przeciwdziałania przestępczości;

- podczas wdrażania rozwiązań w sferze publicznej, jedną z największych przeszkód stanowi brak odpowiedniego poziomu zaufania do administracji publicznej.

Managing people in service operations: Shouldice Hospital case

W ramach panelu omówiono przypadek udanego wdrożenia zasad *Lean Management*. Wykazano jednak, że zbiór zasad *Lean* to tylko jeden z wielu z elementów procesu budowania trwałego sukcesu organizacji opartego na metodologii *Be Lean – Be a Team – Be Ready*. Prace w ramach panelu posłużyły udowodnieniu tezy, że przyszła konkurencyjność i efektywność organizacji wiąże się z jej bieżącą strukturą operacyjną, w tym z jej zdolnością adaptacji do zmian zachodzących w świecie.

Panel ten poprowadził prof. Adrian Done na podstawie studium przypadku *Shouldice Hospital Limited*[12], którego przedmiotem było omówienie sprawdzonego modelu biznesowego zorientowanego na dostarczanie usługi (ang. *service delivery system*) na przykładzie dobrze prosperującej kanadyjskiej kliniki o wieloletniej tradycji, wyspecjalizowanej w leczeniu przepuklin brzusznych. Wieloletni sukces przedsiębiorstwa umożliwiły wdrożenie i ciągłe udoskonalanie metody leczenia opracowanej przez dr. Edwarda Earle'a Shouldice'a[13] – twórcę kliniki *Shouldice*.

Wymieniono następujące filary modelu zarządzania wdrożonego w organizacji:

1. Kultura organizacji – rozumiana tutaj w węższym znaczeniu, opisywanym terminem *kultury służby* (ang. *culture of service*). Organizacja dokonała identyfikacji elementów łańcucha wartości, które pozwoliły jej na uzyskanie rynkowej przewagi konkurencyjnej, po czym wdrożyła narzędzia podporządkowane ochronie tych elementów w celu świadczenia usługi na najwyższym poziomie (za poziom referencyjny przyjmując ofertę innych klinik działających na rynku). Wśród zastosowanych narzędzi uczestnicy wymienili:

[12] J.L. Heskett, *Shouldice Hospital Limited*…, op. cit.

[13] *About Shouldice Hernia Clinic | Hernia Repair and Treatment Hospital Canada*, b.d., https://www.shouldice.com/about/

   a. program szkoleń i zestaw procedur dla chirurgów wykonujących zabiegi według opracowanej i udoskonalanej techniki leczenia,
   b. zestaw norm zmierzających do wypracowania dobrych nawyków postępowania wśród pracowników wszystkich szczebli struktury organizacyjnej, oraz
   c. wypracowanie wizji strategicznej i jej realizacja za pośrednictwem charyzmatycznego lidera.
2. Zaangażowanie pracowników – przemyślany zestaw działań, które umożliwiły pracownikom realizację poszczególnych zadań przy jednoczesnym zapewnieniu im możliwości samorealizacji.
3. Zadowolenie klienta – wszystkie działania organizacji w przestrzeni procesów operacyjnych podejmowano z myślą o dobru i satysfakcji pacjentów (klientów).
4. Jakość obsługi – organizacja dokonywała systematycznego pomiaru efektywności prowadzonych działań i satysfakcji klientów.
5. Wysoka specjalizacja usług – w szpitalu wykonywano tylko jeden rodzaj operacji.

Uczestnicy dokonali krytycznej oceny wyżej nakreślonego modelu biznesowego. W pozornie doskonałym modelu, niemal każdy z uczestników odnalazł zasadniczą wadę: brak zdolności do wdrażania innowacji.

Na podstawie analizy studium przypadku wywnioskowano, że organizacja dążąca do osiągnięcia doskonałości w realizacji wypracowanych dotychczas procesów operacyjnych może ograniczyć swoją zdolność do adaptacji innowacji, czego skutki wprawdzie nie muszą być widoczne natychmiast, ale z czasem prowadzą jednak do spadku konkurencyjności organizacji i jej roli społecznej. Z tego powodu znalezienie bezpośredniej przyczyny spadku efektywności organizacji może być trudne a nawet niemożliwe, stając się źródłem frustracji dla zarządu i pracowników organizacji, którzy pomimo usilnych starań, aby właściwie realizować postawione zadania, nie zauważają pozytywnych skutków swojej pracy. Dalsze losy kliniki *Shouldice* potwierdziły obawy uczestników: odsetek operacji przepuklin wykonywanych za pomocą

techniki laparoskopowej zdominował rynek tego rodzaju usług[14], a sama klinika odnotowała znaczny spadek udziału w rynku.

City of Atlanta Police / US Department of Homeland Security – implementing intelligence-led policing through advanced technology

Celem panelu było przybliżenie uczestnikom seminariów bezprecedensowego procesu wdrożenia najnowocześniejszych rozwiązań technologicznych, organizacyjnych i prawnych na rzecz zwalczania i ograniczania przestępczości w stolicy amerykańskiego stanu Georgia, Atlancie. Przedstawiony proces wdrażania został wybrany z uwagi na swoją skalę i złożoność, jak również kontekst przeciwdziałania przestępczości. Panel ten poprowadziła Silvia King, członek komitetu wdrożeniowego projektu, dzięki czemu uczestnicy mieli możliwość poznania niuansów związanych z metodyką opartą na *modelu Kottera*. Reformę polityki bezpieczeństwa publicznego oparto w Atlancie na koncepcji bliskiej współpracy Policji i członków lokalnej społeczności (ang. *community policing*) przy wykorzystaniu zaawansowanych narzędzi rozpoznawania. Posłużono się tezą, zgodnie z którą bezpieczeństwo publiczne jest ważnym czynnikiem rozwoju ekonomicznego. Wykazano, że źródłem sukcesu podjętych działań było uzyskanie szerokiego konsensusu opartego na skutecznej komunikacji społecznej dotyczącej zakresu i potencjalnych implikacji planowanych działań.

Na podstawie przeprowadzonej dyskusji sformułowano następujące wnioski:

- przejrzyste wyjaśnienie planu wdrażania i zakomunikowanie wizji strategicznej ma kluczowe znaczenie dla osiągnięcia ostatecznego sukcesu, zwłaszcza jeśli mówimy o dużych przedsięwzięciach;
- budowanie koalicji na rzecz wprowadzenia zmian w organizacji powinno angażować pracowników wszystkich szczebli;
- dla zachowania ciągłości wdrożonej zmiany konieczne jest stworzenie odpowiedniego organu zarządczego, odpowiedzialnego za przyszłe funkcjonowanie i dalszy rozwój wprowadzonych zmian.

[14] P.B. Poulsen i in., *Diffusion of Laparoscopic Technologies in Denmark*, „Health Policy", 1998, t.45, nr 2, s. 149–167.

2.3. Faza podsumowania

2.3.1. Ocena prelegentów, treści wystąpień i aspektów organizacyjnych seminariów

W niniejszym podrozdziale przedstawiono ocenę zakresu merytorycznego seminariów i aspektów organizacyjnych. Zaprezentowane statystyki ocen prelegentów i seminariów sporządzono na podstawie anonimowych kwestionariuszy ankietowych wypełnionych przez uczestników.

W celu przeprowadzenia kompleksowej merytorycznej i organizacyjnej oceny seminariów wyodrębniono kryteria, które następnie przedstawiono odpowiednio w poniższych dwu tabelach (zob. tabela 2 i tabela 3).

Tabela 2. Kryteria oceny części merytorycznej seminariów

Kryterium nr 1	Jasność przekazu i zaangażowanie prowadzącego
Kryterium nr 2	Wybór metodyki przekazu
Kryterium nr 3	Adekwatność materiałów
Kryterium nr 4	Efektywne rozwiązywanie problemów i wyjaśnianie wątpliwości
Kryterium nr 5	Poprawa stanu wiedzy z danego zakresu

Tabela 3. Kryteria oceny części organizacyjnej warsztatów

Kryterium nr 1	Standard obsługi warsztatów
Kryterium nr 2	Stan sali wykładowej i pomieszczeń do pracy grupowej
Kryterium nr 3	Możliwość nawiązania współpracy i nowych kontaktów
Kryterium nr 4	Jakość przerw kawowych
Kryterium nr 5	Jakość obiadów
Kryterium nr 6	Witryna internetowa projektu

Uczestnicy ocenili aspekty organizacyjne i merytoryczne seminariów według kryteriów zamieszczonych w powyższych tabelach w skali od 1 do 5, co podsumowano w formie diagramów satysfakcji uczestników[15] przedstawionych na poniższych ilustracjach (zob. rysunek 2 do rysunek 9).

[15] Diagramy opracowano na podstawie ankiet ewaluacyjnych. Oceny każdego sektora i aspektu (organizacyjnego lub merytorycznego) seminarium zsumowano według zadanej skali, tj. każdej ocenie (od 1 do 5) przyporządkowano liczbę ocen wystawionych. Dla większej przejrzystości przeskalowano liczbę wystąpień ocen do skali 10-stopniowej. Udział zadowolonych

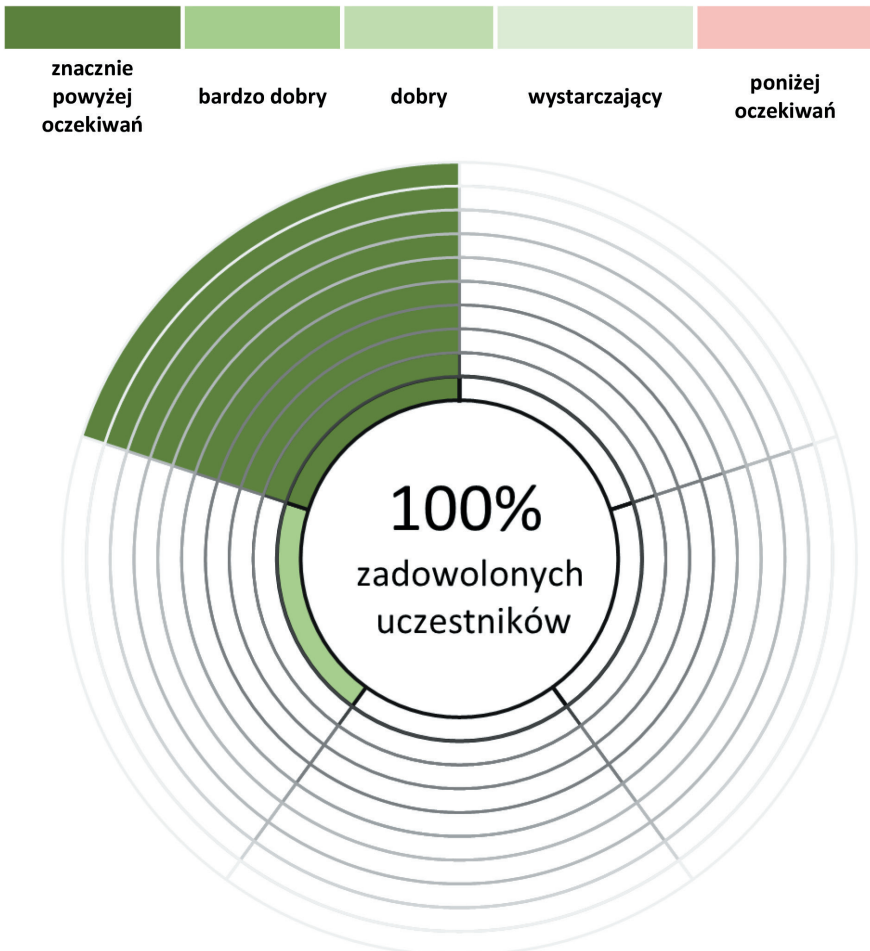
Sektor finansowy

Rysunek 2. Ocena aspektów merytorycznych części seminariów poświęconej sektorowi finansowemu

Źródło: opracowanie własne

uczestników obliczono na podstawie procentowego udziału następujących ocen w całkowitej liczbie wystawionych ocen: wystarczający (2), dobry (3), bardzo dobry (4) i znacznie powyżej oczekiwań (5).

Rysunek 3. Ocena aspektów organizacyjnych seminariów poświęconych sektorowi finansowemu

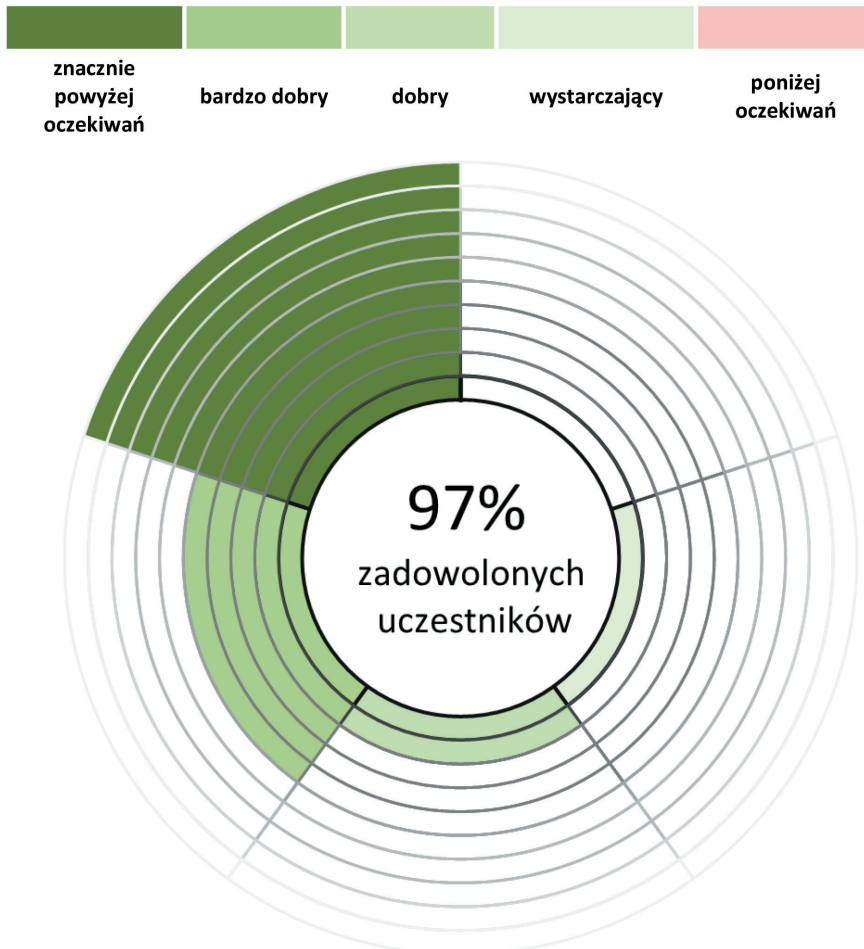


Źródło: opracowanie własne

Uczestnicy modułu przeznaczonego dla przedstawicieli sektora finansowego przyznali najwyższe oceny prelekcji nt. metodyki wdrażania zmian w organizacjach i jej praktycznego zastosowania w kontekście rozwiązań na rzecz przeciwdziałania przestępczości przedstawionej przez profesora Massima Maoreta z IESE Business School.

Sektor ubezpieczeń

Rysunek 4. Ocena aspektów merytorycznych seminariów poświęconych sektorowi ubezpieczeń

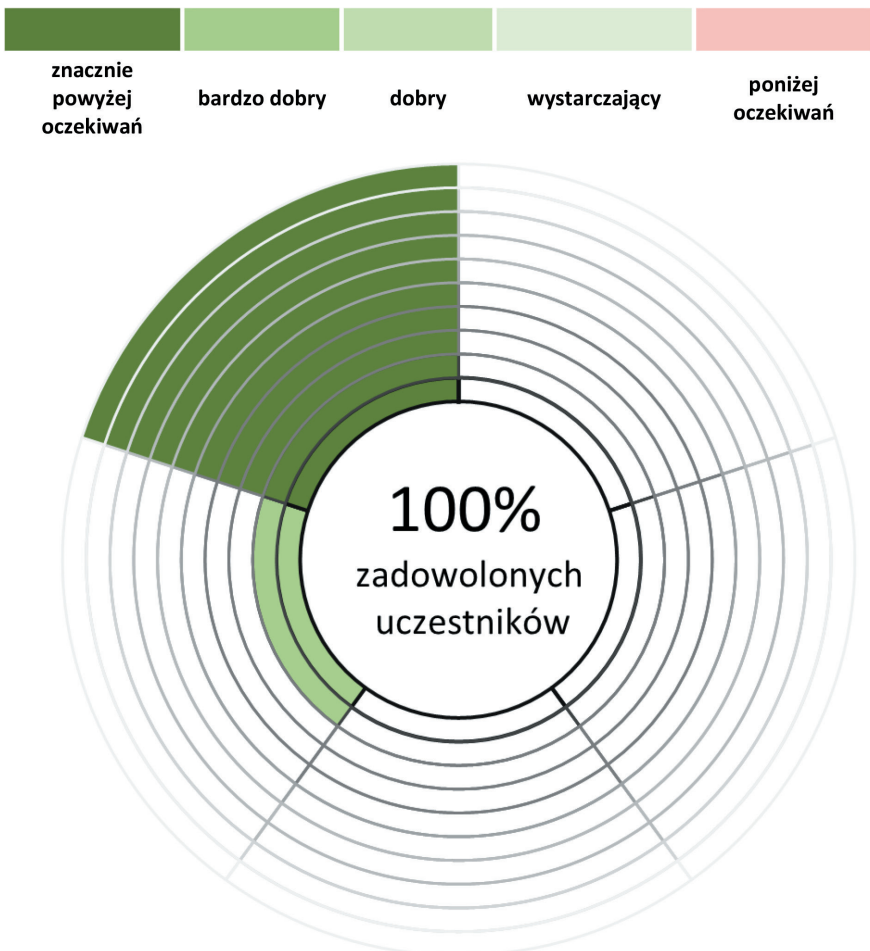


Źródło: opracowanie własne

Wśród reprezentantów sektora ubezpieczeń największe zainteresowanie wzbudziły warsztaty prowadzone przez profesora A. Done'a, poświęcone metodom zarządzania operacyjnego w organizacji w kontekście zwiększania efektywności przeciwdziałania przestępczości. Szczególne uznanie zdobyła

symulacja obrazująca poprzez aktywne zaangażowanie uczestników korzyści wynikające z wdrażania metod zarządzania operacyjnego.

Rysunek 5. Ocena aspektów organizacyjnych seminariów poświęconych sektorowi ubezpieczeń



Źródło: opracowanie własne

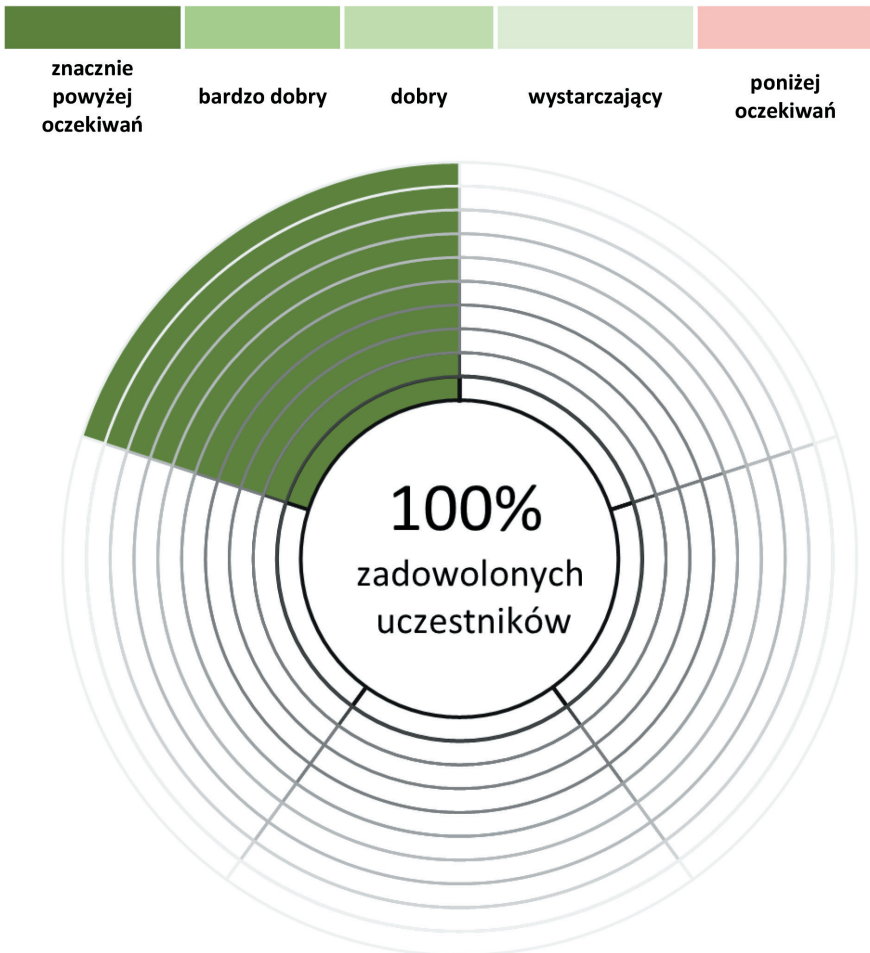
Sektor energetyki

Rysunek 6. Ocena aspektów merytorycznych seminariów poświęconych sektorowi energetyki

Źródło: opracowanie własne

Uczestnicy modułu przeznaczonego dla sektora energetyki wysoko ocenili część warsztatów prowadzonych przez Adriana Done'a, który przedstawił praktyczne aspekty wdrażania metodyki zarządzania operacyjnego dla potrzeb przeciwdziałania przestępczości i zwiększania efektywności operacyjnej w organizacjach aktywnych w sektorze energetyki.

Rysunek 7. Ocena aspektów organizacyjnych seminariów poświęconych sektorowi energetyki



Źródło: opracowanie własne

Jednak najwyższe oceny otrzymał ponownie profesor Massimo Maoret, który wprowadził uczestników w tematykę metodyki wdrażania zmian i identyfikacji powiązań formalnych i nieformalnych w kontekście rozwiązań na rzecz przeciwdziałania przestępstwom.

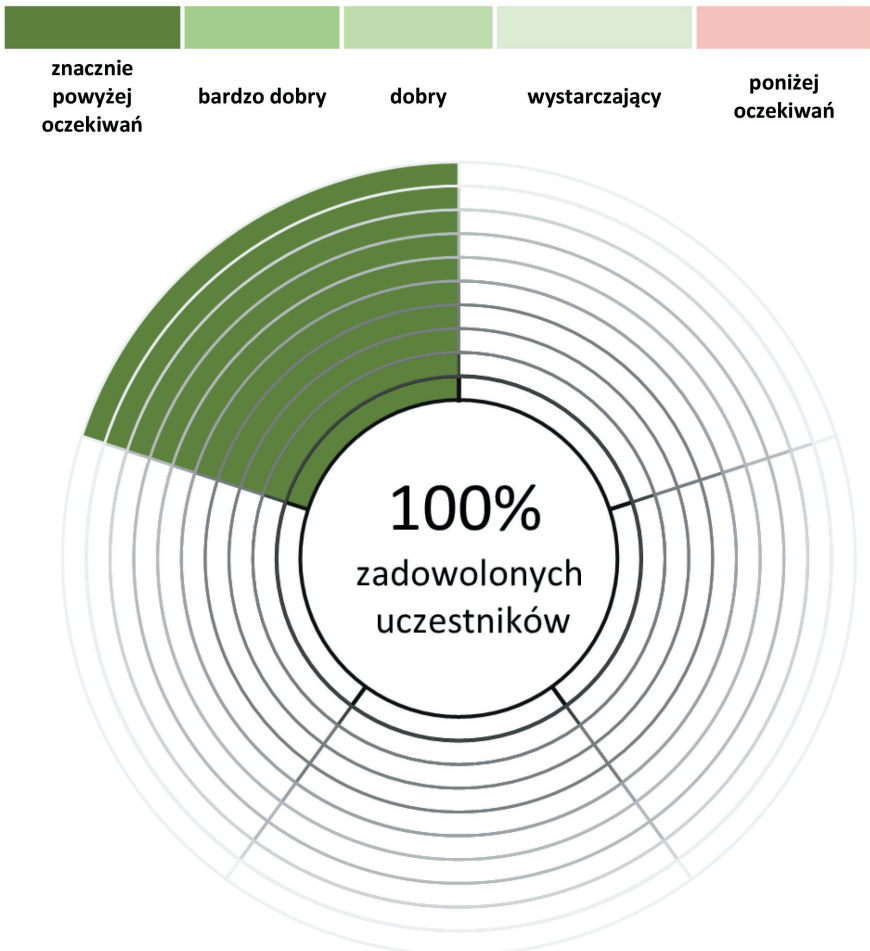
Zarządzanie ludźmi w organizacjach

Rysunek 8. Ocena aspektów merytorycznych seminariów poświęconych obszarowi zarządzania ludźmi

Źródło: opracowanie własne

Uczestnicy modułu dedykowanego obszarowi zarządzania ludźmi w organizacjach najwyżej ocenili wystąpienie profesora Massima Maoreta, który przedstawił tematykę sieci formalnych i nieformalnych w kontekście wprowadzania zmian w organizacjach oraz tworzenia i identyfikowania powiązań przestępczych.

Rysunek 9. Ocena aspektów organizacyjnych seminariów poświęconych obszarowi zarządzania ludźmi



Źródło: opracowanie własne

Uczestnicy ocenili bardzo wysoko aspekty organizacyjne. W szczególności uczestnicy seminarium dla obszaru zarządzania ludźmi podkreślali praktyczność zaprezentowanych treści i wysoką spójność tematyczną.

2.3.2. Analiza statystyczna w zakresie wdrażania metod zapobiegania przestępczości w Polsce

Jednym z elementów fazy podsumowania niniejszego etapu projektu badawczego „Prawo, gospodarka i technologie na rzecz zapobiegania przyczynom przestępczości" była analiza statystyczna obejmująca odpowiedzi uczestników nt. wdrażania w polskich przedsiębiorstwach metod zapobiegania przestępczości stosowanych za granicą. Analizę przeprowadzono zgodnie z metodyką analogiczną do tej, którą zastosowano we wcześniejszych etapach projektu. Pierwsza część badania opierała się na testach parametrycznych i miała na celu zidentyfikowanie czynników wpływających na opinie uczestników dotyczące rozważanego zjawiska. Druga część skupiła się na zbadaniu za pomocą testów nieparametrycznych korelacji pomiędzy odpowiedziami udzielonymi przez uczestników na poszczególne pytania, co z kolei zmierzało do stworzenia zależności obrazujących skłonność do wdrażania innowacyjnych metod zapobiegania przestępczości.

W ramach pierwszej części analizy przeprowadzono szereg symulacji pozwalających na oszacowanie wpływu poszczególnych parametrów na kształtowanie opinii uczestników. W tym celu wykorzystano metodę najmniejszych kwadratów stanowiącą najefektywniejszy estymator w klasie estymatorów liniowych oraz test parametryczny t-Studenta. Jako błąd istotności pierwszego rzędu przyjęto wartość typową dla testów statystycznych, tj. α = 5 procent. Hipotezę zerową, dla której odrzucenia wartość *pi* nie powinna przekraczać 0,05, sformułowano jako brak wpływu parametru na udzieloną odpowiedź.

Tabela 4. Test istotności parametrów dla pytania nr 1 (liczba obserwacji n = 39)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,823224	0,133225	6,179	<0,0001
Typ organizacji	0,579081	0,295528	1,959	0,0581
Wielkość organizacji	0,234182	0,168310	1,391	0,1729
Reprezentowany sektor	0,0826762	0,0911708	0,9068	0,3707
Współczynnik korelacji R^2	0,967196			

Opinie uczestników dotyczące skłonności do wdrażania innowacyjnych rozwiązań z zakresu przeciwdziałania przestępczości (zob. pytanie nr 1 z załącznika B) były silnie uzależnione od doświadczenia zawodowego uczestników. W przypadku pozostałych parametrów uzyskane dane nie dały podstawy do odrzucenia hipotezy zerowej. Biorąc pod uwagę powyższe obserwacje, można wnioskować, iż głównym czynnikiem wpływającym na opinie uczestników jest staż pracy. Ponadto, z uwagi na niską wartość współczynnika dla reprezentowanego sektora, można wykluczyć znaczenie ww. parametru w obrębie rozważanego modelu.

Tabela 5. Test istotności parametrów dla pytania nr 2 (liczba obserwacji n = 38)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,627522	0,162748	3,856	0,0005
Typ organizacji	0,329559	0,304289	1,083	0,2864
Wielkość organizacji	0,374157	0,155485	2,406	0,0217
Reprezentowany sektor	0,195774	0,142676	1,372	0,1790
Współczynnik korelacji R^2	0,960614			

W przypadku pytania dotyczącego adekwatności zaprezentowanych innowacyjnych rozwiązań w kontekście zwiększenia wykrywalności przestępstw największy wpływ na opinie uczestników, z uwagi na wysoką wartość współczynnika, miało ich doświadczenie zawodowe. Ponadto wielkość reprezentowanej instytucji również pełniła istotną rolę w rozważanym modelu, co może świadczyć o wysokim poziomie świadomości w zakresie zagrożeń skorelowanym z wielkością organizacji.

Tabela 6. Test istotności parametrów dla pytania nr 3 (liczba obserwacji n = 39)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,853017	0,196566	4,340	0,0001
Typ organizacji	0,332541	0,365960	0,9087	0,3697
Wielkość organizacji	0,211833	0,188002	1,127	0,2675
Reprezentowany sektor	0,179232	0,172571	1,039	0,3061
Współczynnik korelacji R^2	0,947131			

Odpowiedzi na pytanie dotyczące potencjalnego zwiększenia efektywności poprzez wdrożenia zaproponowanych rozwiązań są ściśle związane z doświadczeniem zawodowym ankietowanego. Z uwagi na wysoką wartość współczynnika w przypadku omawianego parametru można zauważyć, że długi staż pracy jest połączony z przekonaniem o wysokiej skuteczności zaproponowanych rozwiązań. W przypadku pozostałych parametrów uzyskane dane nie pozwoliły na odrzucenie hipotezy zerowej.

Zdanie uczestników na temat obowiązywania regulacji prawnych pozwalających na wprowadzenie innowacyjnych rozwiązań z zakresu przeciwdziałania przestępczości w polskich przedsiębiorstwach zależy od dwóch omawianych parametrów, tj. od wielkości organizacji i doświadczenia zawodowego (zob. tabela 7). Powyższa obserwacja może wskazywać na zróżnicowanie uwarunkowań prawnych w organizacjach o różnej wielkości (najwyższy poziom istotności). Z uwagi na brak podstaw do odrzucenia hipotezy zerowej, w przypadku typu organizacji i reprezentowanego sektora nie można jednoznacznie określić poziomu ich istotności.

Tabela 7. Test istotności parametrów dla pytania nr 4 (liczba obserwacji n = 39)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,410572	0,189120	2,171	0,0368
Typ organizacji	−0,0544640	0,352097	−0,1547	0,8780
Wielkość organizacji	0,641072	0,180881	3,544	0,0011
Reprezentowany sektor	0,226956	0,166034	1,367	0,1804
Współczynnik korelacji R^2	0,936010			

Głównym czynnikiem wpływającym na opinie uczestników dotyczące potrzeby zmiany obowiązujących regulacji prawnych na rzecz ułatwienia wdrażania innowacyjnych rozwiązań z zakresu przeciwdziałania przestępczości było doświadczenie zawodowe (zob. tabela 8). Ponadto można zauważyć, że dłuższy staż pracy jest dodatnio skorelowany ze zwiększoną skłonnością do zmian regulacyjnych.

Tabela 8. Test istotności parametrów dla pytania nr 5 (liczba obserwacji n = 39)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,635910	0,247125	2,573	0,0145
Typ organizacji	0,366925	0,460090	0,7975	0,4305
Wielkość organizacji	0,352473	0,236359	1,491	0,1449
Reprezentowany sektor	0,207376	0,216959	0,9558	0,3457
Współczynnik korelacji R^2	0,915248			

Opinie na temat uwarunkowań kulturowo-społecznych sprzyjających wdrażaniu innowacyjnych rozwiązań z obszaru przeciwdziałania przestępczości cechuje wysoki poziom istotności doświadczenia zawodowego oraz wielkości organizacji. Powyższe dane sugerują, że poziom świadomości w zakresie rozważanego zjawiska wykazuje silne zróżnicowanie z uwagi na charakter działalności, osobiste doświadczenie, jak również reprezentowaną instytucję. Co więcej, pomimo braku podstaw do odrzucenia hipotezy zerowej dla reprezentowanego sektora i typu organizacji, można założyć brak istotności w ramach rozważanego modelu.

Tabela 9. Test istotności parametrów dla pytania nr 6 (liczba obserwacji n = 39)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,588345	0,182920	3,216	0,0029
Typ organizacji	0,144208	0,344175	0,4190	0,6779
Wielkość organizacji	0,336289	0,175339	1,918	0,0638
Reprezentowany sektor	0,139742	0,156221	0,8945	0,3775
Współczynnik korelacji R^2	0,933993			

Druga część przeprowadzonej analizy statystycznej była skoncentrowana na identyfikacji korelacji istniejących pomiędzy odpowiedziami udzielonymi przez uczestników na poszczególne pytania. W tym celu odpowiedzi zostały poddane nieparametrycznemu testowi polegającemu na wyznaczeniu tzw. współczynnika *rho Spearmana*, który posłużył do wyznaczenia wartości *pi* stanowiącej o prawidłowości hipotezy zerowej. Z uwagi na typowość rozważanego problemu, założono poziom błędu istotności na poziomie $\alpha = 5$ procent.

Wyniki testu zostały umieszczone w powyższej tabeli (zob. tabela 10). Wartości zaznaczone pogrubioną czcionką stanowią podstawę do odrzucenia hipotezy zerowej, co stanowi o występowaniu korelacji między udzielonymi odpowiedziami.

Tabela 10. Wyniki analizy korelacyjnej dla odpowiedzi udzielonych na poszczególne pytania

	nr 1	nr 2	nr 3	nr 4	nr 5	nr 6
nr 1		**0,0004**	**0,0014**	0,2702	0,1020	0,9862
nr 2	**0,0004**		**0,0015**	0,0798	0,4116	0,6445
nr 3	**0,0014**	**0,0015**		0,1835	**0,0183**	0,3934
nr 4	0,2702	0,0798	0,1835		0,5285	0,4776
nr 5	0,1020	0,4116	**0,0183**	0,5285		0,7468
nr 6	0,9862	0,6445	0,3934	0,4776	0,7468	

2.3.3. Analiza wyników wypracowanych z grupą fokusową w kontekście wdrażania metod i instrumentów zapobiegania przestępczości

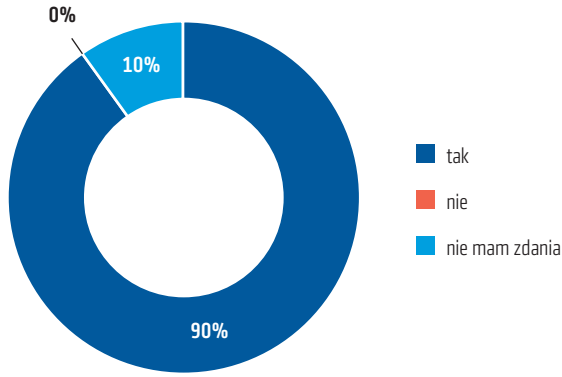
W ramach seminariów przeprowadzono analizę bazującą na dyskusjach grup fokusowych reprezentujących wybrane sektory polskiej gospodarki. Celem tego etapu projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" było wprowadzanie w organizacjach zmian zapobiegających przestępstwom i promującym postawy praworządności. Z tego względu badanie przeprowadzone na podstawie dyskusji zaproszonych uczestników miało na celu zidentyfikowanie istotnych czynników przyczyniających się do osiągnięcia sukcesu we wdrażaniu metod i instrumentów zapobiegania przestępczości w polskich organizacjach. W ramach zaproszonych grup fokusowych złożonych z członków wyższej kadry kierowniczej przedsiębiorstw prywatnych i państwowych oraz agencji rządowych przeprowadzono szereg dyskusji plenarnych i grupowych moderowanych przez wybitnych profesorów (załącznik A – Informacje uzupełniające dotyczące prelegentów), które pozwoliły na optymalne wykorzystanie potencjału intelektualnego wszystkich uczestników. Głównym założeniem dyskusji była rekonstrukcja czynników sprzyjających skutecznemu wdrażaniu

innowacyjnych rozwiązań dedykowanych zapobieganiu przestępczości. Pierwszym etapem wybranej metody były warsztaty naukowe prowadzone przez zaproszonych ekspertów, poświęcone najbardziej uznanym na świecie rozwiązaniom w kontekście wdrażania innowacyjnych metod i instrumentów. Kolejny etap obejmował dyskusje plenarne i grupowe, których zadaniem było opracowanie na podstawie opinii ekspertów będących uczestnikami seminariów mechanizmów pozwalających na dostosowanie światowych standardów wdrażania rozwiązań do warunków polskich. W ramach etapu podsumowania przeprowadzano badanie ilościowe z zastosowaniem kwestionariuszy ankietowych (zob. załącznik B), co miało na celu weryfikację zbiorowej opinii uczestników w zakresie przedstawionych propozycji wdrożeniowych i wniosków dotyczących czynników sprzyjających wdrażaniu nowych rozwiązań na rzecz przeciwdziałania przestępczości.

W ramach fazy wstępnej wywiadu skoncentrowano się na zbadaniu opinii uczestników dotyczącej możliwości wdrożenia przedstawionych rozwiązań w reprezentowanych organizacjach w kontekście całokształtu działalności operacyjnej, bez doprecyzowania ich zastosowania pod kątem przeciwdziałania przestępczości (zob. rysunek 10).

Szczególnym zainteresowaniem uczestników cieszyły się zagadnienia dotyczące tworzenia scenariuszy dla strategii wprowadzania zmian, które zaprezentował prof. Massimo Maoret. Dalsza część dyskusji była nakierowana na możliwość użycia ww. metodyki wdrożeniowej w kontekście zmian skutkujących podwyższeniem wykrywalności przestępstw. Podobną dyskusję przeprowadzono nt. innowacyjnych rozwiązań w obszarze bezpieczeństwa miast przyszłości zaprezentowanych przez Luciena Randazzesego. Jak wykazało badanie ankietowe, 76 proc. uczestników stwierdziło, iż wdrożenie zaprezentowanych rozwiązań pozwoli na zwiększenie wykrywalności przestępstw w Polsce, jak również podniesienie ogólnej skuteczności funkcjonowania przedsiębiorstwa.

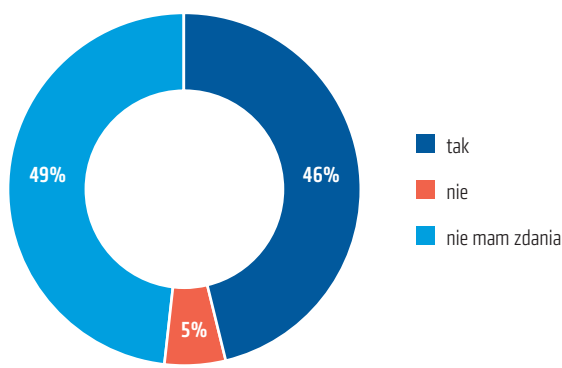
Rysunek 10. Opinia uczestników na temat prawdopodobieństwa wdrożenia zaproponowanych rozwiązań w reprezentowanych organizacjach



Źródło: opracowanie własne

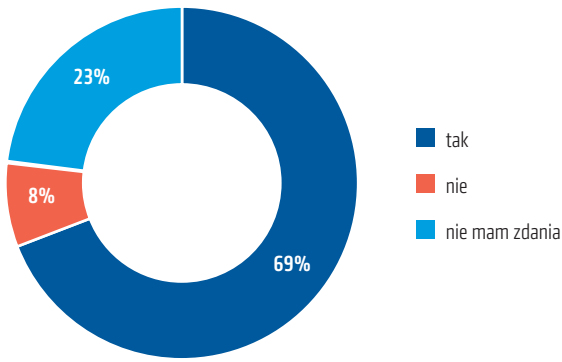
Kolejnym omówionym zagadnieniem były obowiązujące regulacje prawne w kontekście możliwości wprowadzania innowacyjnych rozwiązań z zakresu przeciwdziałania przestępczości. Niemal połowa zaproszonych uczestników stwierdziła, iż obecne regulacje prawne nie sprzyjają wdrażaniu tego typu rozwiązań (zob. rysunek 11). Dyskusja dotyczyła ograniczeń, które RODO wprowadziło do przetwarzania danych osobowych w kontekście predykcji behawiorystycznej, a także aspektów związanych z odpowiedzialnością za decyzje podjęte przez narzędzia wykorzystujące sztuczną inteligencję.

Rysunek 11. Rozkład procentowy dot. odpowiedzi na pytanie „Czy uważa Pan/Pani, że istniejące regulacje prawne w Polsce pozwalają na wdrażanie innowacji zmierzających do zwalczania przestępczości prezentowanych na seminarium?"



Źródło: opracowanie własne

Rysunek 12. Rozkład procentowy dot. odpowiedzi na pytanie „Czy uważa Pan/Pani, że regulacje prawne dotyczące wprowadzania innowacyjnych rozwiązań z zakresu zwalczania przestępczości w Polsce powinny ulec zmianie?"



Źródło: opracowanie własne

W związku ze stwierdzonymi ograniczeniami, 69 proc. uczestników zasygnalizowało potrzebę zmiany obecnie obowiązujących regulacji prawnych na rzecz ułatwienia wdrażania i funkcjonowania innowacyjnych rozwiązań z zakresu przeciwdziałania i zwalczania przestępczości (zob. rysunek 12). Warto jednak podkreślić, że obecnie prowadzone przez Rząd Rzeczypospolitej Polskiej działania na rzecz przeciwdziałania przestępczości uwzględniają postulaty uczestników, m.in. krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 jako jeden z celów strategicznych obejmują zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym[16]. Niska świadomość w zakresie rządowych działań z zakresu cyberbezpieczeństwa jest na świecie zjawiskiem powszechnym, charakterystycznym nie tylko dla Polski. Można przytoczyć przykład badania przeprowadzonego na zlecenie brytyjskiego rządu[17], na którego podstawie

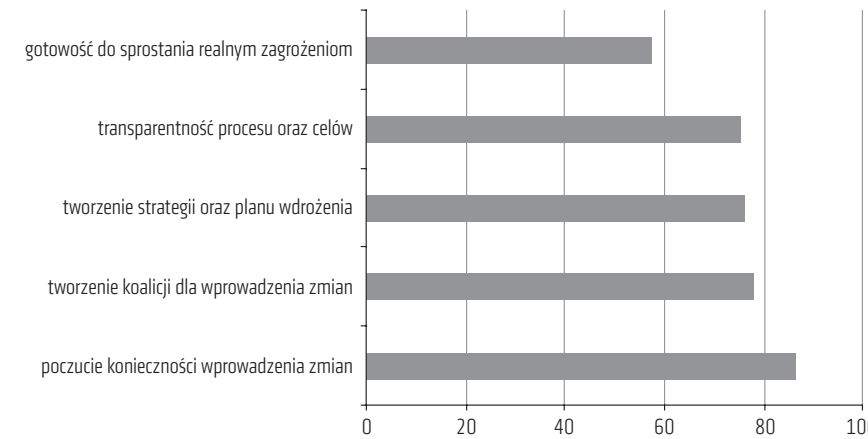
[16] *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Ministerstwo Cyfryzacji, Warszawa 2017, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/obbc7a32-64df-b45e-b08c-dac59415f109

[17] *Cyber Security Breaches Survey 2018*, Department for Digital, Culture, Media and Sport, London 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

stwierdzono, iż jedynie 29 proc. respondentów[18] ma świadomość istnienia rządowych programów przeciwdziałania przestępczości, zaś jedynie 14 proc. zna rządowe zalecenia w rozważanym obszarze.

Opierając się o powyższe dane, uczestnicy seminariów zarekomendowali stworzenie inicjatyw mających na celu realizację bezpośredniej współpracy publiczno-prywatnej w zakresie wdrażania metod przeciwdziałania przestępczości, obejmującej zarówno wsparcie przy wprowadzaniu tego typu rozwiązań, jak również promującej postawę proaktywną. Zgodnie z przeprowadzoną dyskusją inicjatywy tego typu, wpisujące się w tworzenie koalicji dla wprowadzania zmian, stanowią bardzo istotny czynnik skutecznego wdrażania nowych rozwiązań. Uczestnicy zidentyfikowali również inne uwarunkowania sprzyjające wprowadzaniu zmian, co zilustrowano na poniższym wykresie (zob. rysunek 13).

Rysunek 13. Opinia uczestników w zakresie najważniejszych czynników sprzyjających wdrażaniu nowych rozwiązań w zakresie bezpieczeństwa



Źródło: opracowanie własne

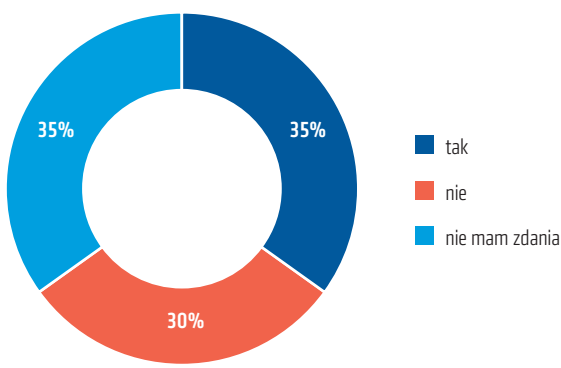
Uczestnicy seminariów wskazali na „poczucie konieczności wprowadzenia zmian" jako na najważniejszy czynnik sukcesu wdrożonych zmian. Jest to szczególnie ważne w perspektywie wprowadzania szeroko zakrojonych zmian zmierzających do poprawy bezpieczeństwa. Zgodnie z opinią uczestników

[18] Badanie przeprowadzono z udziałem 1519 przedsiębiorstw prowadzących działalność w Wielkiej Brytanii.

obecne uwarunkowania społeczno-kulturowe w Polsce nie sprzyjają wdrażaniu rozwiązań z zakresu zwalczaniu przestępczości (zob. rysunek 14), co może być spowodowane niską świadomością społeczną w obszarze potencjalnych zagrożeń związanych z działalnością przestępczą, w związku z czym jedna z rekomendacji wysuniętych w ramach tego etapu projektu naukowego dotyczy stworzenia krajowych inicjatyw zmierzających do upowszechnienia wiedzy dot. zagrożeń związanych z działalnością przestępczą i jej wpływu na polską gospodarkę.

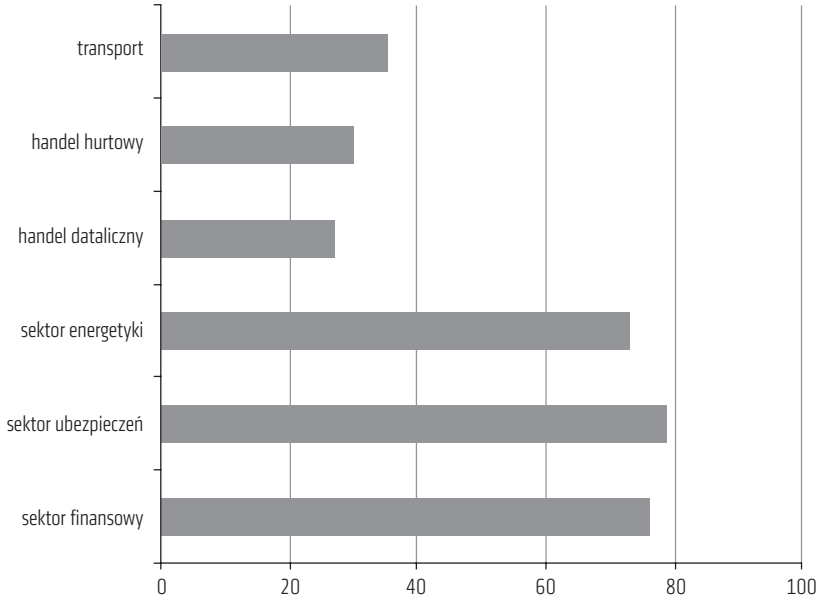
W celu zidentyfikowania sektorów charakteryzujących się największą potrzebą wdrażania innowacyjnych rozwiązań z zakresu przeciwdziałania przestępczości, moderatorzy dyskusji poprosili uczestników o wyrażenie opinii na temat omawianego obszaru. Uczestnicy wskazali sektor ubezpieczeń jako wykazujący szczególną potrzebę wdrażania rozwiązań z zakresu zapobiegania przestępczości. W szczególności przedstawiciele sektora wyrazili duże zainteresowanie zwiększeniem wykrywalności działalności przestępczej poprzez wdrożenie zarządzania operacyjnego na potrzeby działalności operacyjnej reprezentowanych organizacji. Ponadto wskazali na potrzebę stworzenia kolektywnej bazy danych zrzeszającej informacje z zakresu wyłudzeń i oszustw pochodzące zarówno od organizacji działających w sektorze ubezpieczeń, jak i formacji stojących na straży bezpieczeństwa publicznego, w tym policji, ABW i CBA.

Rysunek 14. Rozkład procentowy dot. odpowiedzi na pytanie „Czy uważa Pan/Pani, że uwarunkowania kulturowo-społeczne w Polsce sprzyjają wprowadzaniu innowacyjnych rozwiązań z zakresu zwalczania przestępczości?”



Źródło: opracowanie własne

Rysunek 15. Opinia uczestników dot. sektorów charakteryzujących się szczególną potrzebą wdrażania rozwiązań z zakresu zapobiegania przestępczości



Źródło: opracowanie własne

3. Wnioski seminaryjne i zalecenia w zakresie wdrażania metod i instrumentów zapobiegania przestępczości

W niniejszym rozdziale przedstawiono wyniki prac zespołu badawczego złożonego z uczestników seminariów oraz zaproszonych wybitnych ekspertów z uznanych ośrodków naukowych na całym świecie. Przeprowadzone dyskusje skoncentrowały się na problematyce skutecznego wdrażania rozwiązań z zakresu przeciwdziałania przestępczości w Polsce. W ramach prac przygotowawczych zaproszeni eksperci wskazali odpowiednie kroki pozwalające na wprowadzenie gruntownych zmian w organizacjach. Dlatego sformułowane podczas dyskusji wnioski i rekomendacje w sposób bezpośredni wpisują się w poszczególne etapy zaproponowanej metodyki, które uczestnicy seminariów uznali za kluczowe w kontekście przeciwdziałania przestępczości w Polsce.

3.1. Poczucie potrzeby wprowadzania zmian – skala przestępczości w Polsce

Niniejszy podrozdział zawiera podsumowanie prac, których przedmiotem jest ocena skali przestępczości w Polsce, co zgodnie z zaleceniami uczestników ma na celu uświadomienie potrzeby wprowadzenia zmian na rzecz przeciwdziałania przestępczości. Prace te nawiązują bezpośrednio do pierwszego etapu zaproponowanej metodyki wprowadzania zmian bazującej na *modelu Kottera*. Zespół ekspertów oraz uczestnicy seminariów dokonali razem analizy zjawiska, wykorzystując oficjalne statystyki przestępczości opublikowane przez Centrum Badania Opinii Społecznej, Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Sprawiedliwości oraz instytut NASK. Biorąc pod uwagę istniejące niedoskonałości w systemach

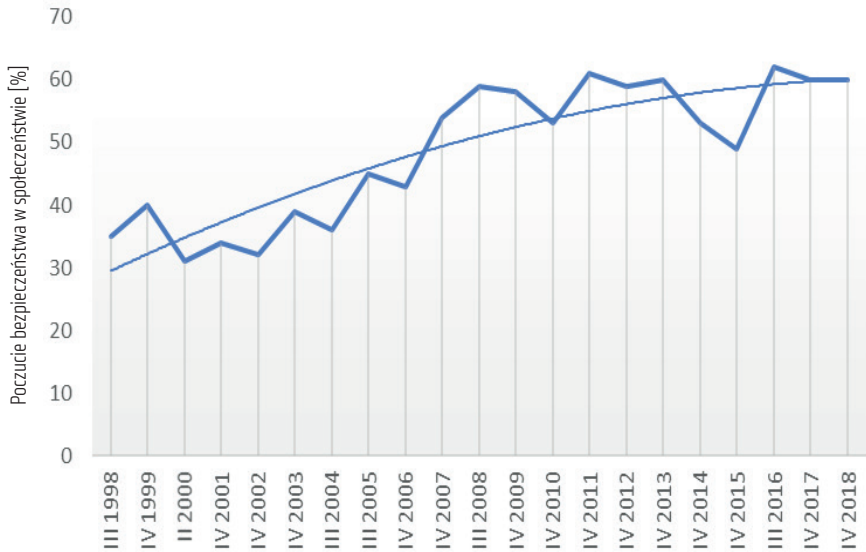
gromadzenia danych i ogólne braki w zakresie statystyk przestępczości, zespół ekspertów zwrócił uwagę na luki w wiedzy i metodach pomiarów zjawiska przestępczości w Polsce, których występowanie sprawia, że przeprowadzone analizy obarczone są czynnikiem niekompletności obrazu zjawiska. Wobec takiego założenia zespół ekspertów dostrzega konieczność przeprowadzenia pogłębionych badań nad przestępczością w Polsce przy szczególnym uwzględnieniu tych obszarów, których nie brano dotychczas pod uwagę lub nie opisano w wystarczającym stopniu. Niemniej, powstałe przy udziale ekspertów opracowanie spełnia rolę czynnika stymulującego do podjęcia działań zaradczych w ramach szeroko zakrojonych inicjatyw stanowiących podstawę dalszych badań i analiz w rozważanym obszarze.

Uczestnicy seminariów zauważyli, że według badań CBOS[19] z 2017 r. mniej niż 50 proc. Polaków żywiło obawy, że mogłoby paść ofiarą przestępstwa lub że mogłoby to spotkać ich bliskich. Warto podkreślić fakt, iż omawiana sytuacja pozostawała stabilna w ostatnich latach (zob. rysunek 16). Obserwowalną tendencję wzrostową spowodował spadek liczby przestępstw kryminalnych[20] bezpośrednio dotykających obywateli.

[19] M. Bożewicz, *Poczucie bezpieczeństwa i zagrożenia przestępczością*, Centrum Badania Opinii Społecznej (CBOS) 11.05.2018, https://www.cbos.pl/SPISKOM.POL/2018/K_061_18.PDF

[20] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku*, Ministerstwo Spraw Wewnętrznych i Administracji 2016, https://bip.mswia.gov.pl/download/4/31673/RaportostaniebezpieczenstwawPolscew2016roku.pdf.

Rysunek 16. Poczucie bezpieczeństwa w polskim społeczeństwie – ostatnie 20 lat [21]



Źródło: opracowanie własne na podstawie danych CBOS[22]

Zgodnie z danymi z rysunku 12, w ostatnich dwudziestu latach poczucie bezpieczeństwa wśród obywateli Polski wzrosło aż o 20 procent. Powodem tak dużego wzrostu jest m.in. wzrost wykrywalności przestępstw, większa przejrzystość przepisów, dostosowanie przepisów do standardów międzynarodowych, rozwój technik śledczych, zmiana w polityce administracji państwowej w zakresie informowania o skali i charakterze wykrywanej w Polsce przestępczości, czego dowód stanowią opublikowane statystyki policyjne. W związku z tym uczestnicy stwierdzili, że w Polsce aktualnie brakuje powszechnego zrozumienia wynikającej z braku poczucia bezpieczeństwa konieczności wprowadzenia zmian. Ta konieczność jest z jednej strony pozytywnym wskaźnikiem, jednak z drugiej strony świadczy o braku warunków sprzyjających wprowadzeniu szeroko zakrojonych działań na rzecz przeciwdziałania przestępczości.

[21] Na podstawie odpowiedzi respondentów „Nie obawiam się" na pytanie „Czy obawia się Pan(i) tego, że może stać się ofiarą przestępstwa?".

[22] M. Bożewicz, *Poczucie bezpieczeństwa i zagrożenia przestępczością*…, op. cit.

Przedmiotem kolejnego etapu analizy były przestępstwa o charakterze gospodarczym, których celem było zweryfikowanie poczucia potrzeby wprowadzenia zmian w poszczególnych sektorach polskiej gospodarki. Według dostępnych danych policja odnotowuje zwiększoną liczbę przestępstw o charakterze gospodarczym[23, 24] (zob. tabela 11). Z analizy danych dot. lat 2011–2017 wynika, że – pomimo utrzymującego się podobnego poziomu wykrywalności przestępstw – w kategorii przestępstw gospodarczych nastąpił wzrost o 25 procent. Warto podkreślić, iż trend wzrostowy występuje pomimo wysokiego i stabilnego współczynnika wykrywalności przestępstw w tym sektorze[25] (zob. rysunek 17).

Tabela 11. Przestępstwa o charakterze gospodarczym w latach 2011–2017[26]

	2011	2012	2013	2014	2015	2016	2017
Liczba przestępstw stwierdzonych	151655	141483	159624	161135	167741	150386	189871
Wykrywalność [%]	–	–	88,9	87,1	84,4	82,5	87,6

Źródło: Bank Danych Lokalnych, https://bdl.stat.gov.pl/ (dostęp: 29.09.2018).

Uczestnicy zauważyli, że wzrost przestępstw gospodarczych znajduje odzwierciedlenie w dynamice liczby naruszeń prawa w poszczególnych sektorach. W sektorze ubezpieczeniowym, oprócz wzrostu przestępstw, zmieniła się ponadto ich struktura. W trakcie dyskusji seminaryjnych uczestnicy jako główny problem dotykający sektor ubezpieczeń wskazali oszustwa ubezpieczeniowe. Potwierdzają to analizowane statystyki policyjne, gdzie w latach 2011–2017 zaobserwowano znaczny udział procentowy przestępstw związanych z oszustwami ubezpieczeniowymi i wyłudzeniami odszkodowań (zob. tabela 12 i rysunek 18). Warto zauważyć, że odsetek ww. przestępstw utrzymuje się (z wyjątkiem roku 2015), zaś odsetek przestępstw w cyberprzestrzeni (pozycja „oszustwo ubezpieczeniowe komputerowe") wydaje się

[23] Zdarzenie, które w wyniku zakończenia postępowania przygotowawczego policja i prokuratura potwierdziły jako przestępstwo.

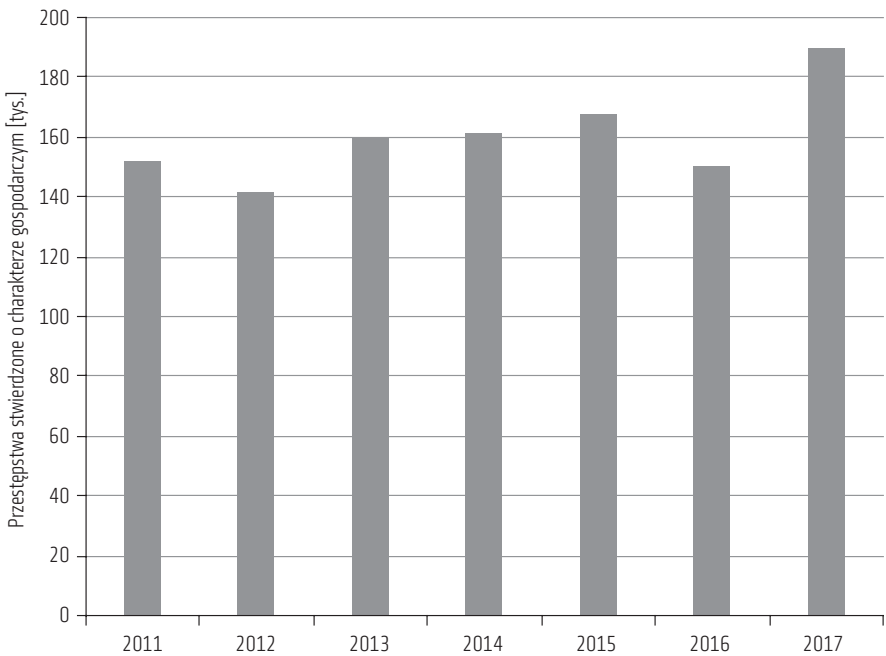
[24] M. Adamczyk, *Przestępstwa stwierdzone a postępowania wszczęte i ich wykrywalność w Polsce w latach 2000–2012*, „Security, Economy & Law", b.d., nr 1/2016, s. 18–36.

[25] M. Bożewicz, *Poczucie bezpieczeństwa i zagrożenia przestępczością*…, op. cit.

[26] Bank Danych Lokalnych, https://bdl.stat.gov.pl/ (dostęp: 29.09.2018).

mieć marginalne znaczenie. Jednak w opinii zaproszonych ekspertów w najbliższych latach przestępstwa w cyberprzestrzeni będą wykazywać wyraźną dynamikę wzrostową. Uczestnicy seminarium przeznaczonego dla sektora ubezpieczeń zgodnie stwierdzili, że oszustwa ubezpieczeniowe stanowią istotne zagrożenie dla działalności organizacji, co z kolei przekłada się na silne poczucie konieczności wprowadzenia zmian w tym zakresie. Ponadto pomimo odnotowania znacznie mniejszej dotkliwości cyberprzestępstw ochrona przed tego typu zagrożeniami jest priorytetem dla wielu organizacji aktywnych w sektorze ubezpieczeń.

Rysunek 17. Liczba przestępstw o charakterze gospodarczym stwierdzonych przez policję w latach 2011–2017



Źródło: opracowanie własne na podstawie danych MSWiA[27], [28]

[27] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku*…, op. cit.

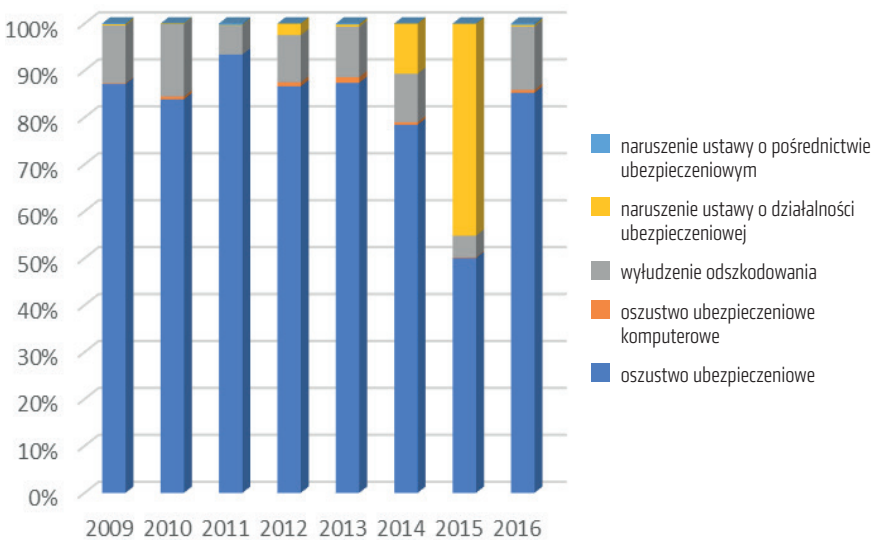
[28] *Raport o stanie bezpieczeństwa w Polsce w 2015 roku*, Ministerstwo Spraw Wewnętrznych i Administracji 2015, https://bip.mswia.gov.pl/download/4/29642/file.file

Tabela 12. Przestępstwa stwierdzone w sektorze ubezpieczeń wg kategorii (2009–2016)

	2009	2010	2011	2012	2013	2014	2015	2016
Oszustwo ubezpieczeniowe[29]	669	669	821	803	919	1224	1124	797
Oszustwo ubezpieczeniowe komputerowe[30]	1	5	0	8	13	9	3	6
Wyłudzenie odszkodowania[31]	95	123	54	93	113	161	104	126
Naruszenie ustawy o działalności ubezpieczeniowej[32]	2	1	1	23	5	167	1014	3
Naruszenie ustawy o pośrednictwie ubezpieczeniowym[33]	1	0	3	0	2	0	1	3

Źródło: opracowanie własne na podstawie danych MSWiA[34]

Rysunek 18. Rozkład procentowy przestępstw ubezpieczeniowych wg kategorii (2009–2016)



Źródło: opracowanie własne na podstawie danych MSWiA[35]

[29] Art. 286 § 1 i 3 k.k.
[30] Art. 287 § 1–2 k.k.
[31] Art. 298 § 1 k.k.
[32] Art. 225–232 ustawy o działalności ubezpieczeniowej i art. 430–440 ustawy o działalności ubezpieczeniowej i reasekuracyjnej
[33] Art. 47–48 ustawy o pośrednictwie ubezpieczeniowym
[34] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku*..., op. cit.
[35] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku*..., op. cit.

Tabela 13. Przestępstwa stwierdzone w sektorze finansowym wg kategorii (2009–2016)

	2009	2010	2011	2012	2013	2014	2015	2016
Wyłudzenie kredytu[36]	11105	1155	9061	7701	6423	7720	5971	4632
Niepowiadomienie właściwego podmiotu o sytuacji mogącej mieć wpływ na wstrzymanie lub ograniczenie udzielonego wsparcia finansowego[37]	61	73	40	29	46	46	15	11
Prowadzenie działalności bankowej bez zezwolenia[38]	14	12	10	13	20	12	26	17
Lichwa[39]	6	57	13	15	21	170	158	40
E-bankowość, phishing[40]	0	0	0	0	0	527	1027	1615

Źródło: opracowanie własne na podstawie danych MSWiA[41]

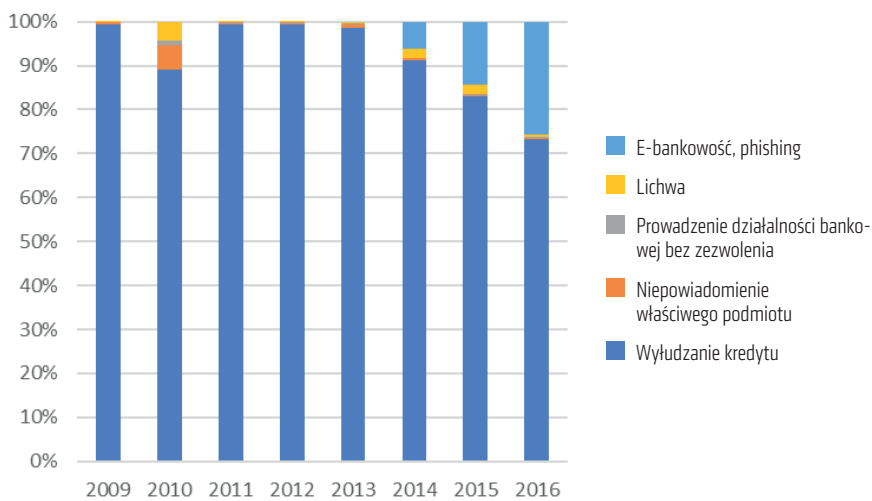
Uczestnicy seminariów podkreślili, że konieczność zmian łatwo dostrzec w zakresie przeciwdziałania oszustwom kredytowym. Statystyki policyjne dotyczące przestępstw w sektorze finansowym jednoznacznie wskazują na dominujący udział procentowy wyłudzania kredytów w ogólnej liczbie stwierdzonych incydentów (zob. tabela 13). Jednakże w ostatniej dekadzie nastąpił istotny wzrost odsetka cyberprzestępstw w ogólnej liczbie stwierdzonych incydentów wynikających z naruszeń art. 287 § 1 i 2 kodeksu karnego (zob. rysunek 19). Szczególnie niepokoi widoczna w kategorii „e-bankowość, phishing" tendencja wzrostowa, a w szczególności, zaobserwowany w ciągu dwóch lat, wzrost liczby przestępstw o 313 procent.

Zgodnie z tym, co mówią uczestnicy, oficjalne statystyki policji nie obejmują jednak trudnego do oszacowania odsetka przestępstw o charakterze wewnętrznym, tj. popełnianych przez pracowników sektora finansowego lub przy ich współudziale. Jak dowodzą dane pochodzące bezpośrednio od banków[42], znaczące straty generują oszustwa wewnętrzne i zewnętrzne,

[36] Art. 297 § 1 k.k.
[37] Art. 297 § 2 k.k.
[38] Art. 171 ustawy z 29 sierpnia 1997 r. Prawo bankowe
[39] Art. 304 k.k.
[40] Art. 287 § 1 i 2 k.k., pozycja wprowadzona dnia 13.01.2014 r.
[41] Ibid.
[42] Ibid.

uznawane za część ryzyka operacyjnego (zob. rysunek 20). Szczególnie wyraźnie widać to w ujęciu prezentującym straty wynikające z oszustw dla przedstawicieli sektora bankowego, gdzie zaobserwowano łączne straty za rok 2017 na poziomie 150 mln zł (zob. rysunek 21). Na uwagę zasługuje odmienna skala zjawiska w poszczególnych bankach. Zróżnicowanie wartości oszustw wynika raczej ze struktury rynkowej udziałów poszczególnych banków w sektorze. Udział procentowy oszustw bankowych w poszczególnych bankach pozostaje na porównywalnym poziomie. Z uwagi na istotny udział przestępstw wewnętrznych w ogólnej liczbie odnotowanych oszustw, uczestnicy stwierdzili, iż wizja strategiczna tworzona w ramach wdrażania rozwiązań na rzecz przeciwdziałania tego rodzaju przestępstwom, powinna obejmować aspekty związane z kapitałem ludzkim, w tym wprowadzenie stosownej kultury zgodności.

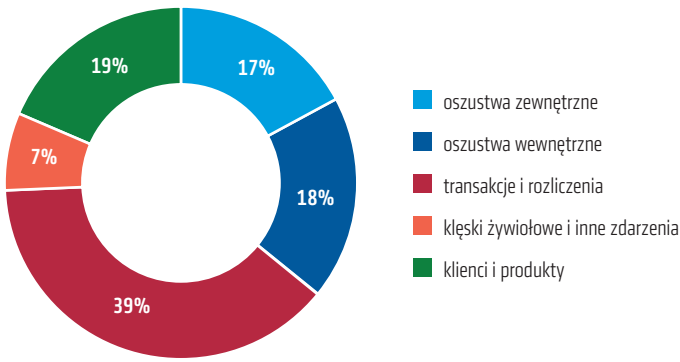
Rysunek 19. Udział przestępstw w sektorze finansowym wg kategorii w latach 2009–2016



Źródło: opracowanie własne na podstawie danych MSWiA[43]

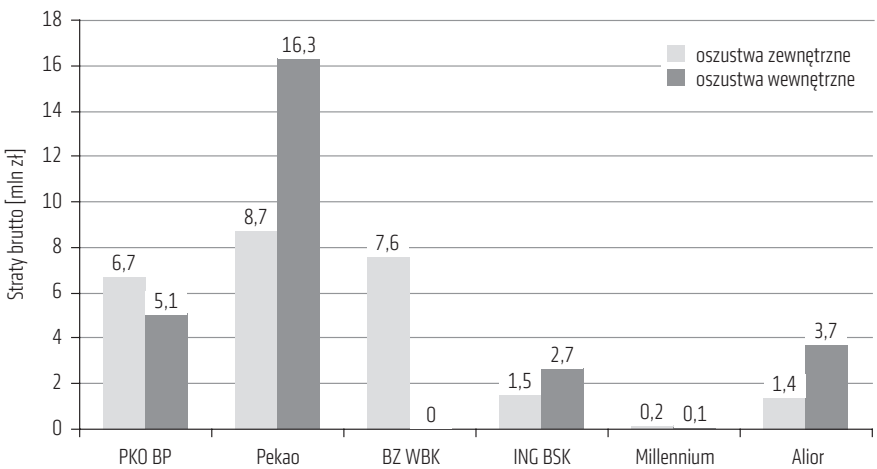
[43] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku*…, op. cit.

Rysunek 20. Udział procentowy strat wg kategorii w polskim sektorze bankowym w roku 2017



Źródło: opracowanie własne na podstawie publikacji w prasie branżowej[44]

Rysunek 21. Straty (w mln zł) wynikające z oszustw popełnionych względem wybranych banków (dane za rok 2017)



Źródło: opracowanie własne na podstawie publikacji w prasie branżowej [45]

Statystyki policyjne wskazują tutaj na stosunkowo niewielką skalę zjawiska (zob. tabela 14). Ponadto, ze względu na spadek liczby przestępstw w roku

[44] M. Rudke, *Banki: ile tracą na oszustwach pracowników i wyłudzeniach?*, 26.06.2018, https://www.parkiet.com/Parkiet-PLUS/306269958-Banki-ile-traca-na-oszustwach-pracownikow-i-wyludzeniach.html

[45] Ibid.

2016, nie można wykazać jednoznacznej tendencji wzrostowej (zob. rysunek 22). Jednak według Sylvii King i Luciena Randazzese'a światowe trendy wykazują na zdecydowany wzrost liczby popełnionych cyberprzestępstw, co zdaje się przeczyć wiarygodności statystyk policyjnych w tym zakresie. Eksperci podkreślali również, iż częstym czynnikiem umożliwiającym cyberatak jest niska świadomość personelu organizacji w zakresie cyberbezpieczeństwa, dlatego wdrażane aktualnie na świecie rozwiązania przeciwdziałające cyberprzestępstwom obejmują szeroko zakrojone programy szkoleniowe w zakresie cyberbezpieczeństwa.

Tabela 14. Wybrane przestępstwa odnotowane w cyberprzestrzeni (2010–2016)

	2010	2011	2012	2013	2014	2015	2016
Atak na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych[46]	0	5	5	9	7	4	6
Atak na system komputerowy lub sieć teleinformatyczną[47]	18	30	30	34	52	111	40

Źródło: opracowanie własne na podstawie danych MSWiA[48]

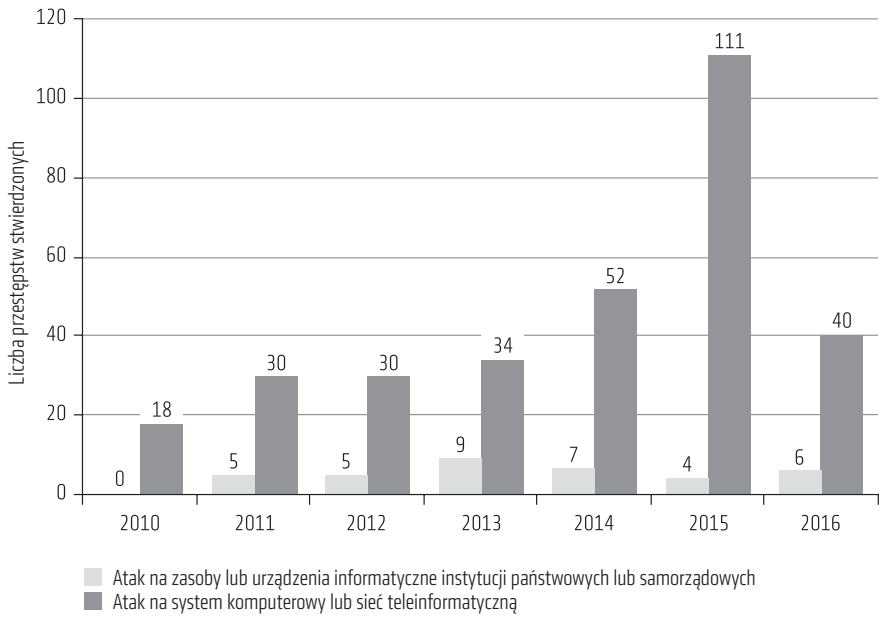
W trakcie dyskusji uczestnicy zwrócili uwagę na duży wzrost liczby cyberprzestępstw w sektorze bankowym w przeciągu ostatnich lat wynikający z dysproporcji istniejących zabezpieczeń w stosunku do kompetencji cyberprzestępców. W celu weryfikacji skali przestępstw tego typu odnotowanych na poziomie krajowym, przeprowadzono stosowaną estymację zjawiska bazując na dostępnych statystykach.

W celu weryfikacji wiarygodności statystyk policyjnych podczas oceniania skali zjawiska cyberprzestępczości w Polsce skorzystano z danych pochodzących od Rządowego Zespołu Reagowania na Incydenty Komputerowe – instytucji powołanej do badania zdarzeń mających miejsce w rozważanym obszarze. Statystyki dotyczące liczby zarejestrowanych incydentów różnią się znacznie od przestępstw odnotowanych przez policję (porównaj: rysunek 22 i rysunek 23). Uczestnicy dyskusji wskazywali również na potrzebę wskazania

[46] Art. 269 §1–2 k.k.
[47] Art. 269a k.k.
[48] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku*…, op. cit.

celów ataków cybernetycznych w kontekście ochrony krajowej infrastruktury krytycznej. Ponadto uczestnicy seminarium przeznaczonego dla sektora energetyki stwierdzili, że tego typu ataki stanowią bardzo poważne zagrożenie dla bezpieczeństwa polskiej gospodarki jako całości; jednakże świadomość w tym obszarze, a zatem jednocześnie poczucie konieczności wprowadzenia zmiany, są wciąż bardzo niskie.

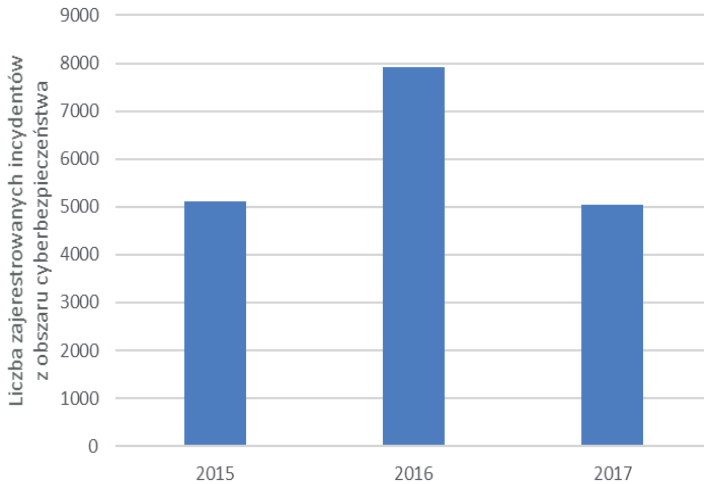
Rysunek 22. Liczba wybranych cyberprzestępstw odnotowanych przez policję w latach 2010–2016



Źródło: opracowanie własne na podstawie danych MSWiA[49]

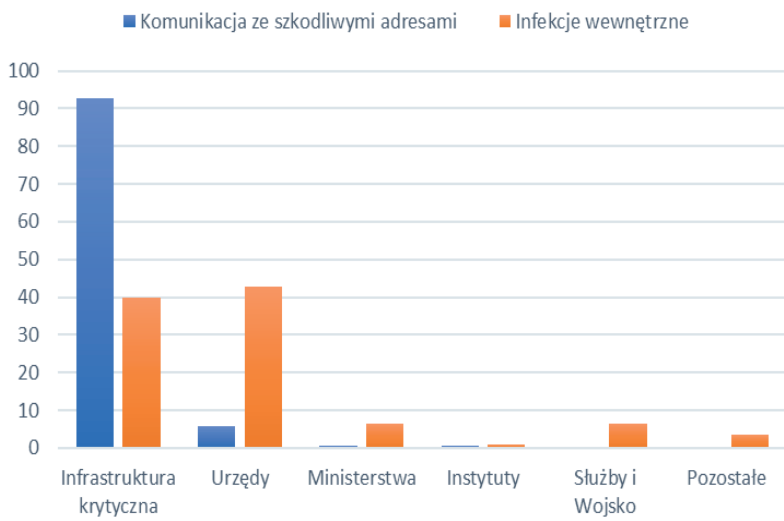
[49] *Raport o stanie bezpieczeństwa w Polsce w 2016 roku…*, op. cit.

Rysunek 23. Liczba incydentów z obszarów bezpieczeństwa zarejestrowanych przez Rządowy Zespół Reagowania na Incydenty Komputerowe



Źródło: opracowanie własne na podstawie danych CERT.GOV.PL[50]

Rysunek 24. Rozkład procentowy skategoryzowanych celów ataku wg kategorii ataku wykrytych przez system ARAKIS



Źródło: opracowanie własne na podstawie danych CERT.GOV.PL[51]

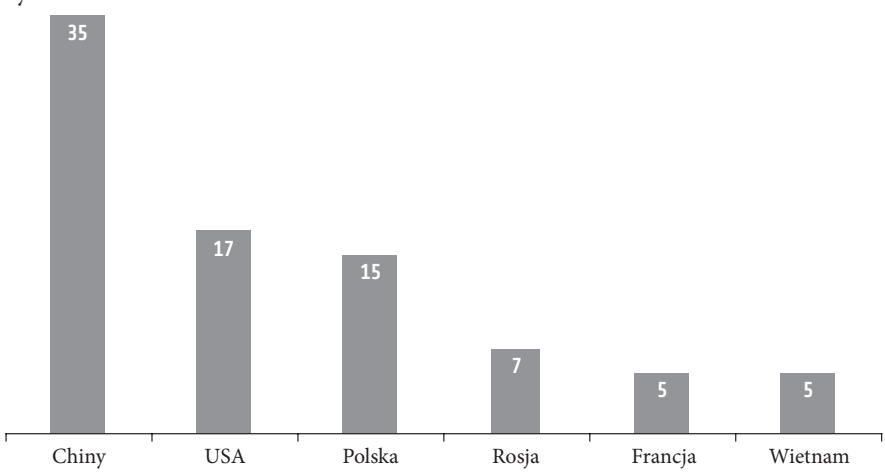
[50] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL 2017, https://csirt.gov.pl/download/3/186/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2017roku.pdf

[51] Ibid.

Dane pochodzące z systemu ARAKIS[52] pozwoliły stwierdzić, iż znaczna część ataków koncentrowała się na obiektach sklasyfikowanych przez system jako „infrastruktura krytyczna" lub „urzędy". Zgodnie z opiniami zaproszonych ekspertów powyższe dane wykazują zgodność z tendencjami międzynarodowymi nie tylko odnośnie do wzrostu liczby popełnianych przestępstw, lecz również doboru celu cyberataków.

System ARAKIS pozwolił również na wykrycie źródeł ataków cybernetycznych. Procentowy udział największych źródeł ataków z podziałem na kraje przedstawiono na poniższym wykresie (zob. rysunek 25). Niemal co trzeci atak pochodzi z Chin. Zjawisko to wydaje się znajdować uzasadnienie w obserwacji uczestników seminariów, popartej również innymi źródłami[53], dot. intensywnego rozwoju chińskiego zaplecza cybernetycznego.

Rysunek 25. Rozkład geograficzny największych źródeł cyberataków wykrytych przez system ARAKIS



Źródło: opracowanie własne na podstawie danych CERT.GOV.PL[54]

Odnotowuje się stosunkowo niewielką liczbę ataków pochodzących od bezpośrednich sąsiadów Polski połączoną z dużym udziałem ataków z terminali

[52] ARAKIS-GOV jest systemem wsparcia ochrony zasobów teleinformatycznych administracji państwowej. Źródło: https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html

[53] G. Austin, *Cyber Policy in China*, John Wiley & Sons, Cambridge, UK, 2014.

[54] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*…, op. cit.

zlokalizowanych wewnątrz kraju. Jednakże uczestnicy seminariów zwrócili uwagę, iż klasyfikacja wykonana przy pomocy system ARAKIS obejmuje położenie geograficzne tylko węzłów, które wykorzystano do ataku. Wobec tego wskaźnik ten może nie uwzględniać prawdziwego źródła niektórych incydentów, co chociażby ma miejsce w przypadku ataku wykorzystującego sieć typu *botnet*[55]. Jako taki wskaźnik ten może być nie w pełni miarodajny. Uczestnicy i zaproszeni eksperci stwierdzili, że ogólna poprawa cyberbezpieczeństwa wymaga zbudowania szeroko zakrojonej koalicji zaangażowanej we wprowadzanie zmian, ponieważ podniesienie i utrzymanie wysokiego poziomu cyberbezpieczeństwa wymaga kolektywnego wysiłku administracji publicznej, organizacji prywatnych, jak również zwykłych obywateli.

Kolejnym problemem jaki poruszono w ramach seminariów były przestępstwa dotyczące zarządzania ludźmi w organizacjach. W ramach dyskusji stwierdzono, iż możliwe pomyłki w szacowaniu skali tego zjawiska wynikają z chęci ochrony reputacji organizacji, w której doszło do wystąpienia nieprawidłowości. Dotyczy to zarówno przestępstw, których ofiarą jest sama instytucja, jak też przestępstw w jej strukturze – np. wobec pracowników. Takie działania mogą być związane z przeciwdziałaniem skutkom wycieków, których źródłem są tzw. *demaskatorzy* (nazywani także *sygnalistami*, ang. *whistleblowers*), co z kolei często skutkuje zawieraniem ugód z poszkodowanymi pracownikami. Pomimo tego, że takie postępowanie może wpływać na wiarygodność oficjalnych statystyk, w celu dokonania oceny postrzegania konieczności wprowadzenia zmian przez organy publiczne, podjęto próbę oszacowania skali przestępczości dotykającej rozważanego obszaru w drodze analizy danych pochodzących z bazy Ministerstwa Sprawiedliwości[56].

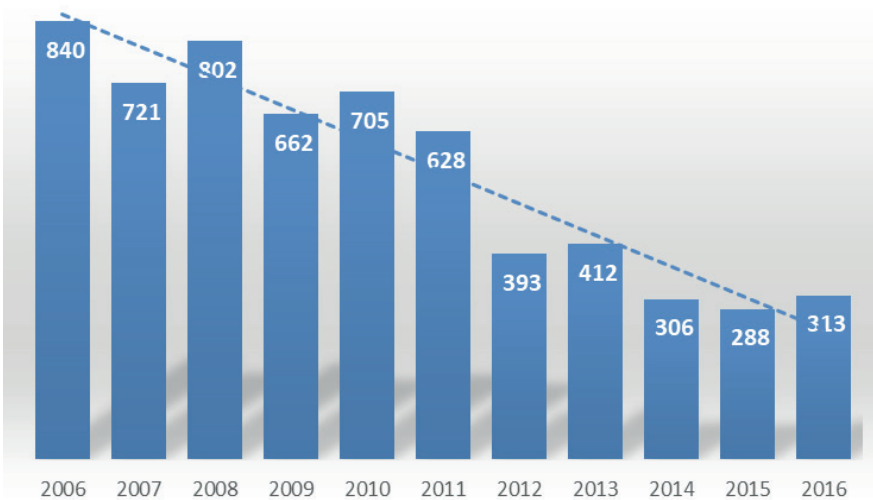
Dane przywołane podczas seminariów wskazują na występowanie w ostatnich latach tendencji spadkowej, co zilustrowano poprzez mniejszą liczbę osób skazanych oraz wskaźnik dyskryminacji w zatrudnieniu. Warto jednak podkreślić, że zaobserwowany trend jest oparty wyłącznie na oficjalnych statystykach, które nie uwzględniają trudnej do oszacowania skali niezgłoszonych

[55] Typ ataku z wykorzystaniem botnetu polega na zarażeniu grupy komputerów szkodliwym oprogramowaniem, umożliwiając wykonywanie ataku za pośrednictwem zarażonych terminali.

[56] Dane Wydziału Statystycznej Informacji Zarządczej w Departamencie Strategii i Funduszy Europejskich Ministerstwa Sprawiedliwości.

naruszeń. Zgodnie z opiniami zaproszonych ekspertów, pozytywny charakter występujących w Polsce tendencji jest mało wiarygodny w kontekście przeciwnych tendencji obserwowanych na całym świecie[57]. Uczestnicy seminarium dedykowanego wdrażaniu rozwiązań w obszarze zarządzania ludźmi również stwierdzili, że skala wynikająca z oficjalnych statystyk nie obrazuje w pełni rozważanego zjawiska. Ponadto w ramach dyskusji stwierdzono, że kluczowym elementem wdrażania rozwiązań w tym obszarze jest powołanie stosownych organów kontroli polityki zgodności.

Rysunek 26. Wyroki skazujące dotyczące przestępstw przeciwko prawom osób wykonujących pracę zarobkową[58]

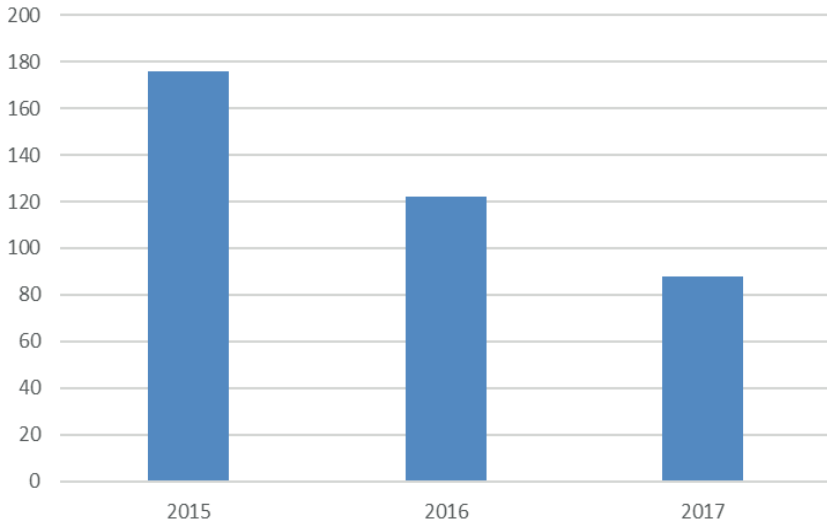


Źródło: opracowanie własne na podstawie danych Ministerstwa Sprawiedliwości

[57] L. Woan Jinq, R. Yazdanifard, *The Alarming Trend of Sexual Harassment Occurrences in the Workplace and What Can Be Done*, „International Journal of Management, Accounting and Economics", 2015, t.2, nr 5.

[58] Uwzględniono naruszenia wynikające z art. 218 §1a k.k., art. 218 §2 k.k., art. 218 §3 k.k., art. 219 k.k., art. 219 §1 k.k., art. 220 §1 k.k., art. 220 §2 k.k., art. 220 §3 k.k. oraz art. 221 k.k.

Rysunek 27. Wskaźnik dyskryminacji w zatrudnieniu w latach 2015–2017[59]



Źródło: opracowanie własne na podstawie danych Ministerstwa Sprawiedliwości

Niniejszy rozdział stanowi podsumowanie części prac badawczych poświęconych ocenie skali przestępczości w Polsce, mających na celu zbadanie poczucia konieczności wprowadzenia zmian na rzecz przeciwdziałania rozważanym zjawiskom. Analizę przeprowadzono na podstawie danych statystycznych, zaś jej podbudowę koncepcyjną wypracowali wspólnie uczestnicy seminariów. Zgodnie z zaleceniami uczestników powyższe opracowanie stanowi wstępną fazę do dalszych badań i inicjatyw, mających na celu pogłębianie wiedzy i podwyższanie poziomu świadomości społecznej w zakresie zagrożeń związanych z działalnością przestępczą, co stanowi pierwszy etap wdrażania odpowiednich szeroko zakrojonych działań zaradczych.

[59] Wskaźnik zdefiniowany jako liczba osób poszkodowanych wskutek dyskryminacji w miejscu pracy.

3.2. Tworzenie strategii zmian – rekomendacje w zakresie metody i instrumentów prewencji w obszarach zwiększonego ryzyka w kontekście trendów międzynarodowych

Poniższy rozdział stanowi podsumowanie dyskusji przeprowadzonych w ramach seminariów mających na celu opracowanie podstaw strategii zmian w zakresie przeciwdziałania przestępczości w Polsce. Zidentyfikowane na pierwszym etapie niniejszego projektu najbardziej dotkliwe dla polskiej gospodarki problemy poddano w tym celu analizie. Wyciągnięte wnioski sformułowano jako rekomendacje zaradcze, które należałoby wprowadzić do strategii i planu wdrożeniowego rozwiązań zapobiegawczych, co adresuje jeden z elementów zaproponowanej metodyki, tj. tworzenie strategii wdrażania.

3.2.1. Społeczna akceptacja przestępczości

Na podstawie sondażu diagnostycznego przeprowadzonego wśród uczestników seminariów można stwierdzić, że społeczna akceptacja przestępczości nie dotyczy jedynie wyłudzeń ubezpieczeniowych, lecz również nadużyć występujących we wszystkich obszarach związanych z finansami, a także działalności przestępczej jako całości. Jednym z wniosków sformułowanych w ramach wrześniowego etapu projektu jest teza, iż społeczna akceptacja przestępstw nie wynika jedynie z braku świadomości negatywnych konsekwencji w większej skali, np. ogólnego podwyższenia stawki składek, lecz również z uwarunkowań kulturowych i indywidualnej sytuacji materialnej[60], [61]. Jednym z kluczowych zaleceń powstałych wskutek przeprowadzonej debaty jest nie tylko zwiększenie świadomości istniejących problemów i ich skutków, lecz także fundamentalna zmiana dotycząca postaw etycznych i wskaźników moralnych. Przedmiotem prac przeprowadzonych w ramach

[60] B. Czepil, *Kulturowe uwarunkowania korupcji w systemie demokratycznym i niedemokratycznym na przykładzie USA i ZSRR*, 2008, http://www.antykorupcja.gov.pl/download/4/8767/Kulturoweuwarunkowaniakorupcjiwsystemiedemokratycznymiedemokratycznymnaprzykla.pdf

[61] A. Lewicka-Strzałecka, *Moralność finansowa Polaków. Raport z badań*, Konferencja Przedsiębiorstw Finansowych w Polsce, Gdańsk-Warszawa 06.2018.

niniejszego etapu projektu było sformułowanie zestawu zaleceń, stanowiących podstawę strategii wdrażania rozwiązań przeciwdziałania zjawisku społecznej akceptacji przestępczości, jak również promowanie postaw praworządności. Dla właściwego zdefiniowania problemu poniższy rozdział zawiera zarys tematyki zjawiska społecznej akceptacji przestępczości i sformułowany przez uczestników zestaw zaleceń.

Postawa nieetyczna a sytuacja materialna

Analiza zawarta w raporcie dotyczącym moralności finansowej Polaków jednoznacznie wykazała istnienie związku pomiędzy podwyższonym poziomem akceptacji nieetycznych zachowań a złą sytuacją materialną danej osoby. Statystyki dowodzą, że ludzie mający problemy ze spłacaniem zadłużenia charakteryzują się równocześnie podwyższoną tendencją do nieetycznych zachowań finansowych[62].

Zapewnienie społeczeństwu właściwej edukacji finansowej to powszechny problem na całym świecie[63], [64], [65]. Można stąd wnioskować, że odpowiednie wykształcenie i świadomość zasad funkcjonowania finansów mają znaczenie nie tylko dla osób zajmujących się finansami zawodowo. Ze względu na wciąż zwiększającą się ofertę rynku finansowego i na coraz większą złożoność oferowanych instrumentów edukacja finansowa wydaje się niezbędna dla zapewnienia stabilności finansowej rodziny. Pogłębiona wiedza nie tylko zmniejsza skłonność konsumentów do popełniania naruszeń, lecz ponadto przyczynia się do lepszego zrozumienia zasad funkcjonowania rynku i wykształcenia właściwych postaw etycznych.

---

[62] Ibid.

[63] E.A. Duke, *The Importance of Financial Education*, zaprezentowano na Jump$tart Coalition Investing in Our Future: Financial Education and Washington Event Washington 2010, https://www.federalreserve.gov/newsevents/speech/files/duke20100408a.pdf

[64] M. Vella, C. Calamatta, *Why is Financial Education Important?*, b.d., Times of Malta wydanie, https://www.timesofmalta.com/articles/view/20180703/business-comment/why-is-financial-education-important.683446

[65] R. Dominski, *The Importance of Financial Literacy for a Secure Future*, 16.10.2017, https://www.washingtonpost.com/sf/brand-connect/wp/2017/10/16/usbank/the-importance-of-financial-literacy-for-a-secure-future/?utm_term=.b5d57e19b61a

Celem niniejszej części prac badawczych było opracowanie rekomendacji wpisujących się w międzynarodowe trendy w rozważanych obszarach gospodarki. Potrzeba zapewnienia odpowiedniego poziomu edukacji finansowej to problem rozpoznany na całym świecie. Jednym z najbardziej uznanych organów zajmującym się kreowaniem strategii dot. problemów społecznego dobrobytu, w tym problemu przestępczości, jest Organizacja Współpracy Gospodarczej i Rozwoju (ang. *OECD*)[66], [67], której rekomendacje wraz z obserwacjami uczestników seminariów posłużyły do opracowania poniższych zaleceń wpisujących się w międzynarodowe tendencje dot. zapobiegania przestępczości. Zgodnie z zaleceniami uczestników seminariów poniższe rekomendacje powinny stanowić element strategii wdrażania rozwiązań zapobiegających przestępczości i budowania koalicji na rzecz wprowadzania zmian poprzez promowanie postaw praworządności.

I. Działania sektora publicznego:
   a. Krajowe kampanie zmierzające do zwiększenia świadomości ryzyka finansowego i metod zabezpieczania się przed ryzykiem poprzez oszczędzanie, ubezpieczenia i edukacje finansową.
   b. Edukacja finansowa powinna zaczynać się na możliwie wczesnym etapie edukacji szkolnej.
   c. Programy edukacji finansowej powinny być powszechnie i nieodpłatnie dostępne na każdym etapie życia.
   d. Powinno się ustanowić lub wyznaczyć odpowiednio wyspecjalizowaną strukturę, która posłużyłaby do promowania edukacji finansowej na poziomie krajowych, regionalnych i lokalnych inicjatyw publicznych i prywatnych.
   e. Promowane strony internetowe powinny zawierać istotne i przyjazne użytkownikom informacje dotyczące finansów. Należy również skupić się na tworzeniu darmowych serwisów informacyjnych

[66] OECD (*Organisation for Economic Co-operation and Development*) jest międzynarodową organizacją zajmującą się promowaniem polityki mającej na celu polepszenie jakości życia oraz sytuacji ekonomicznej na świecie. Źródło: http://www.oecd.org/about/

[67] *Recommendation on Principles and Good Practices for Financial Education and Awareness*, the Convention on the Organisation for Economic Co-operation and Development 07.2005, https://www.oecd.org/daf/fin/financial-education/35108560.pdf

i rozwijaniu systemów ostrzegających przed zjawiskami szkodliwymi dla interesów finansowych konsumentów.

f. Międzynarodowa współpraca w kwestiach edukacji finansowej powinna być promowana z wykorzystaniem OECD jako międzynarodowego forum do wymiany bieżących informacji i doświadczeń na polu edukacji finansowej w poszczególnych krajach.

II. Działania sektora prywatnego w zakresie edukacji finansowej:

a. Warto zachęcać instytucje finansowe do tworzenia precyzyjnych wymagań dotyczących rodzajów informacji przekazywanych klientom odnośnie do oferowanych produktów i usług, w tym miejsca, gdzie takie informacje są dostępne, jak również dostarczania ogólnych, obiektywnych informacji porównawczych dotyczących ponoszonego ryzyka i zwrotu, jaki można uzyskać uzyskać z różnych oferowanych produktów.

b. Instytucje finansowe należy zachęcać do przejrzystego zdefiniowania różnic pomiędzy edukacją finansową, informacjami dotyczącymi stanu finansów danego klienta i „komercyjnym" doradztwem finansowym. Każda porada finansowa udzielana w celu biznesowym powinna być przejrzysta i oznaczona jako informacja handlowa. Jeśli usługi finansowe wiążą się z długoterminowym zobowiązaniem lub mogą potencjalnie wiązać się ze znaczącymi konsekwencjami finansowymi, wówczas należy zachęcać instytucje finansowe, aby upewniły się, że przekazane klientom informacje zostały przez nich przyswojone i zrozumiane.

c. Należy zachęcać instytucje finansowe do informowania klientów w zróżnicowany sposób, dążąc jednocześnie do pełnej przejrzystości przekazu. Warto jednocześnie odejść od stosowania małej czcionki i zawiłej dokumentacji, zamiast tego stosując zasady tzw. prostego języka (ang. *plain language*).

d. W celu jak najlepszego sprostania konsumenckim wymaganiom jakość edukacji zapewnianej przez instytucje finansowe należałoby poddawać regularnej ocenie, co można osiągnąć poprzez współpracę z finansowymi organami non-profit, które to organy mogą mieć lepsze powiązania z konsumentami, w tym w szczególności

z konsumentami pozostającymi w niekorzystnej sytuacji na rynku finansowym.

e. Warto, aby instytucje finansowe szkoliły personel w zakresie edukacji finansowej i procedur dotyczących świadczenia usług takiego doradztwa inwestycyjnego i pożyczkowego, które nie jest powiązane z żadnym z oferowanym produktów.

III. Edukacja finansowa dot. oszczędności emerytalnych

a. Osoby z prywatnym planem emerytalnym powinny otrzymywać odpowiednie informacje finansowe i wiedzę niezbędną do zarządzania swoimi przyszłymi dochodami i oszczędnościami emerytalnymi.

b. W kontekście kariery zawodowej edukacja finansowa i świadomość pracowników powinny być dalej rozwijane i promowane poprzez dodatkowe gratyfikacje finansowe bądź inne formy świadczeń dodatkowych.

IV. Program edukacji finansowej

a. Należy propagować programy edukacji finansowej, które pomagają konsumentom dostrzec wszelkie wady i zalety, jak również ryzyka ponoszone w związku z poszczególnymi rodzajami oferowanych produktów finansowych i usług. Dodatkowo warto popularyzować dalsze badania dotyczące ekonomii behawioralnej.

b. Warto promować rozwój metodologii umożliwiających ocenę już istniejących finansowych programów edukacyjnych. Być może oddelegowane rządowe agendy powinny w oficjalny sposób uznawać i certyfikować programy spełniające istotne kryteria.

c. W celu osiągnięcia większego zainteresowania i nagłośnienia należy wykorzystać wszystkie dostępne kanały medialne do rozpowszechniania przesłania o walorach edukacyjnych.

d. W edukacji finansowej należy promować podejście uwzględniające zróżnicowane pochodzenie konsumentów, jak i inwestorów, poprzez tworzenie programów dopasowanych do potrzeb konkretnych podgrup inwestorów i konsumentów, takich jak np. ludzie młodzi, osoby gorzej wykształcone lub znajdujące się w trudnej sytuacji życiowej.

e. Zaleca się promować programy uwzględniające wykorzystanie kompetentnych i właściwie przygotowanych dydaktyków. Ponadto należy wspierać rozwój programów mających na celu przygotowanie

edukatorów dostarczenie im określonego materiału informacyjnego oraz narzędzi.

Powyższe dotyczące programów edukacji finansowej zalecenia są obecnie wdrażane przez niektóre polskie instytucje. Szczególnie dobrze widać to na przykładzie działalności Narodowego Banku Polskiego, wspierającego projekty, które wpisują się w obszary działalności edukacyjnej banku centralnego[68]. Według danych Związku Banków Polskich, aktualnie w Polsce prowadzi się ok. 100 projektów poświęconych edukacji finansowej[69]. Zgodnie z tym, co mówili uczestnicy seminariów, większość prowadzonych aktualnie programów edukacji finansowej ma charakter regionalny lub lokalny, co z kolei przekłada się na mały zasięg efektów końcowych. Jednym z zaleceń sformułowanych w ramach seminariów było stworzenie inicjatyw na poziomie krajowym o szeroko zakrojonym charakterze, które będą skierowane do grona licznych odbiorców na dowolnym etapie rozwoju zawodowego.

3.2.2. Korupcja

Zjawisko korupcji to problem, który dotyczy wszystkich gałęzi gospodarki. Zgodnie z pracami przeprowadzonymi w ramach wrześniowego etapu seminariów, ma ono szczególnie istotne znaczenie w sektorze energetyki, gdzie narażone jest bezpieczeństwo infrastruktury krytycznej, włączając w to aspekty natury prawnej i strategicznej związane z potencjalnymi naruszeniami, do których dochodzi podczas procesu prywatyzacyjnego lub podczas stosowania szeroko rozumianej procedury przetargowej. Poniższe zalecenia opracowane przez uczestników seminariów w oparciu na wytycznych OECD[70] i dyskusjach przeprowadzonych w ramach trzeciego etapu projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom

[68] Dofinansowanie projektów z zakresu edukacji ekonomicznej, NBP, https://www.nbportal.pl/edukacja-w-nbp/dofinansowanie-nbp

[69] K. Czernek, M. Jurek, P. Marszałek, *Mapa edukacji finansowej VI edycja*, Związek Banków Polskich, Poznań 03.2017, https://zbp.pl/dla-konsumentow/edukacja-ekonomiczna.

[70] *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*, Organisation for Economic Co-operation and Development (OECD), 26.11.2009, http://www.oecd.org/corruption/anti-bribery/anti-briberyconvention/oecdantibriberyrecommendation2009.htm.

przestępczości" mają przyczynić się do stworzenia założeń planu wdrożenia rozwiązań opracowanych na potrzeby polityki antykorupcyjnej w organizacjach prywatnych i publicznych.

I. Dobre praktyki w instytucji

Efektywne kontrole wewnętrzne, promowanie postaw etycznych, programy mające na celu dostosowanie do bieżących regulacji i wymogów oraz środki zapobiegawcze pozwalające na wykrycie zagranicznego przekupstwa powinny być rozwijane na podstawie oceny ryzyka i szczególnej sytuacji danej instytucji, w tym zagrożenia zagranicznym przekupstwem. Takie okoliczności i ryzyko powinny być przedmiotem regularnej kontroli. Jest to niezbędne dla zapewnienia ustawicznej skuteczności wewnętrznej kontroli w danej instytucji, podtrzymania etyki organizacji i utrzymania ciągłych programów dot. integracji, których celem jest zapewnienie zgodności z wymogami, normami i regulacjami.

Firmy powinny rozważyć m.in. przestrzeganie dobrych praktyk dla zapewnienia efektywnej kontroli wewnętrznej, etyki oraz środków i programów dostosowawczych, tak aby wykrywać przypadki i próby korupcji dokonywane z zagranicy i im zapobiegać.

a. Silne, wyraźne i widoczne wsparcie oraz zaangażowanie ze strony kierownictwa wyższego szczebla w przeprowadzanych kontrolach wewnętrznych, etyce oraz środkach i programach mających na celu dostosowanie do bieżących regulacji i wymogów, ma na celu pomoc w wykrywaniu i zapobieganiu przypadkom zagranicznego przekupstwa.
b. Przejrzysta polityka korporacyjna powinna jasno zakazywać zagranicznego łapownictwa.
c. Przestrzeganie tego zakazu, jak i związanych z nim kontroli wewnętrznych, etyki i programów dostosowawczych jest obowiązkiem osób zatrudnionych na wyższych szczeblach w instytucji.
d. Nadzór nad etyką i programami dostosowanymi do bieżących regulacji oraz wymogów dotyczących zagranicznego przekupstwa powinien zostać powierzony co najmniej jednemu starszemu rangą urzędnikowi korporacyjnemu, który wykazywałby się odpowiednim autorytetem i dostatecznie wysokim poziomem niezależności od kadry zarządzającej.

e. Etyka, programy dostosowawcze lub środki wytworzone po to, aby wykryć oraz zapobiec zagranicznemu przekupstwu mają zastosowanie do wszystkich dyrektorów i pracowników (lub urzędników). Dodatkowo są użyteczne dla wszystkich podmiotów, nad którymi instytucja sprawuje skuteczną kontrolę. W szczególności mają one zastosowanie do następujących obszarów:
   i. prezenty,
   ii. rozrywka i wydatki reprezentacyjne,
   iii. podróże klientów,
   iv. zaangażowanie polityczne,
   v. darowizny na cele charytatywne i patronaty,
   vi. gratyfikacje,
   vii. wymuszenia.

f. Etyka i programy dostosowawcze lub środki zapobiegania i wykrywania przekupstwa zagranicznego mogą mieć również zastosowanie do stron trzecich, jednakże tylko przy zastrzeżeniu stosownych warunków w umowie. Za stronę trzecią uznaje się agentów, pośredników, konsultantów, przedstawicieli, dystrybutorów, kontrahentów i dostawców, konsorcja oraz partnerów *joint venture*, nazywanych *partnerami biznesowymi*. Wymienione środki mogą znaleźć zastosowanie w następujących obszarach:
   i. właściwie udokumentowana analiza *due diligence* dotycząca ryzyka związanego z zatrudnieniem, jak również właściwy i regularny nadzór nad partnerami biznesowymi;
   ii. informowanie partnerów biznesowych o zobowiązaniach instytucji do przestrzegania przepisów prawnych dotyczących zakazu przekupstwa zagranicznego, etyce i programach w celu dostosowania się do wymogów i regulacji zapobiegających oraz wykrywających przekupstwa;
   iii. dążenie do wzajemnego zobowiązania ze strony partnerów biznesowych.

g. System procedur finansowo-księgowych wyposażony w system wewnętrznej kontroli, zaprojektowany w sposób zapewniający utrzymanie dobrze prowadzonych ksiąg, ewidencji i rachunków, tak aby

uniemożliwić ich wykorzystanie do przekupstwa zagranicznego lub próby jego zatajenia.

h. Środki stworzone w celu zapewnienia okresowej komunikacji i udokumentowanego szkolenia na wszystkich poziomach instytucji w zakresie etyki, programów dostosowawczych i środków dotyczących przypadków zagranicznego przekupstwa.
i. Odpowiednie środki nastawione na zachęcenie i zapewnienie pozytywnego wsparcia w przestrzeganiu zasad etyki, programów dostosowawczych i środków zapobiegających zagranicznemu przekupstwu na wszystkich poziomach instytucji.
j. Odpowiednie procedury dyscyplinarne w celu zajęcia się m.in. naruszeniami przepisów prawa zakazującymi zagranicznego przejęcia na wszystkich szczeblach instytucji oraz jej etyką i programami dostosowawczymi.
k. Efektywne środki służące do:
    i. udzielania wskazówek i porad dyrektorom, urzędnikom, pracownikom oraz partnerom biznesowym, w stosownych przypadkach w zakresie programów mających na celu dostosowanie do bieżących wytycznych i regulacji oraz etyki, również wówczas, gdy wymagają oni pilnej porady w trudnych sytuacjach związanych z zagranicznymi jurysdykcjami;
    ii. wewnętrznego i, w miarę możliwości, poufnego raportowania i ochrony dyrektorów, urzędników, pracowników, a także – w stosownych przypadkach – partnerów biznesowych, którzy chcą uniknąć naruszania standardów zawodowych i etycznych pod presją przełożonych, a także dyrektorów, urzędników i pracowników gotowych do uzasadnionego i wykonywanego w dobrej wierze zgłaszania naruszeń prawa, standardów zawodowych czy też etyki w instytucji;
    iii. podejmowania odpowiednich działań w odpowiedzi na takie zgłoszenia.
l. Okresowe przeglądy programów etycznych i dostosowawczych, przeznaczone do oceny i poprawy ich efektywności w zapobieganiu i wykrywaniu zagranicznego przekupstwa z uwzględnieniem

istotnego rozwoju w tej dziedzinie, jak również zmieniających się standardów branżowych i międzynarodowych.

m. Działania podejmowane przez organizacje biznesowe i stowarzyszenia zawodowe.

Organizacje biznesowe i stowarzyszenia zawodowe mogą odgrywać istotną rolę w pomaganiu przedsiębiorstwom w tworzeniu skutecznej kontroli wewnętrznej, etyki oraz środków i programów dostosowawczych, a także w podejmowaniu działań nastawionych na zapobieganie i wykrywanie przekupstwa międzynarodowego. Takie wsparcie może obejmować między innymi:

a. propagowanie informacji na temat zagadnień dotyczących przekupstwa, w tym również tych odnoszących się do rozwoju na forach regionalnych i międzynarodowych oraz dostępu do istotnych baz danych;
b. udostępnianie szkoleń, analiz *due diligence* i innych narzędzi zmierzających do zapewnienia zgodności regulacyjno-prawnej;
c. ogólne doradztwo w zakresie przeprowadzania badania *due diligence*;
d. ogólne porady oraz wsparcie w zakresie przeciwstawiania się wymuszeniom.

W zakresie przeciwdziałania zjawisku korupcji w Polsce uczestnicy seminariów wskazywali na informacyjno-edukacyjną działalność Centralnego Biura Antykorupcyjnego, która aktualnie koncentruje się na monitorowaniu opinii społecznej w obszarze percepcji zjawiska korupcji wpisującej się w obszar propagowania zagadnień dotyczących przekupstwa[71]. Jednym z zaleceń zaproponowanych przez uczestników seminariów było zawiązanie inicjatywy mającej na celu upowszechnienie odpowiednich szkoleń i narzędzi stosowanych w rozważanym obszarze. W tym kontekście warto zwrócić uwagę na ważną rolę Krajowej Szkoły Administracji Publicznej (KSAP) w zakresie kształcenia pracowników administracji publicznej. Programy szkoleń oferowane przez tę instytucję powinny zapewniać ważny komponent zapobiegania korupcji przygotowany na podstawie powyższych rekomendacji.

Kolejnym kluczowym problemem jest obszar związany z kwestiami legislacyjnymi w postępowaniu prywatyzacyjnym oraz ochroną monopoli

[71] Źródło: CBA, http://antykorupcja.gov.pl/

naturalnych, szczególnie istotnych dla sektora energetyki. Stąd jednym ze sformułowanych przez uczestników zaleceń było stworzenie inicjatywy publiczno-prywatnej umożliwiającej skuteczne wdrażanie zmian regulacyjnych. Wedle rekomendacji uczestników, przedmiotem pierwszego etapu rozważanej inicjatywy powinno być utworzenie interdyscyplinarnego zespołu badawczego łączącego kompetencje z zakresu nauk prawnych z działalnością sektora energetycznego.

3.2.3. Cyberbezpieczeństwo

W ramach prac przeprowadzonych podczas pierwszego etapu niniejszego projektu badawczego cyberprzestępczość zidentyfikowano jako problem dotyczący wszystkich obszarów polskiej gospodarki. Uczestnicy i zaproszeni eksperci zgodnie stwierdzili, że istotnym zagrożeniem dla działań prewencyjnych w rozważanym obszarze jest brak transparentności w zgłaszaniu cyberataków oraz niska świadomość personelu organizacji w zakresie cyberbezpieczeństwa. Sformułowane przez uczestników i oparte na wytycznych organizacji OECD[72] rekomendacje powinny posłużyć do wdrożenia rozwiązań podnoszących poziom cyberbezpieczeństwa. Głównym celem poniższych zaleceń jest stworzenie inicjatyw zrzeszających jednostki z sektora publicznego i prywatnego (zwane dalej „partnerami"), które poprzez współpracę na poziomie krajowym i międzynarodowym wdrożą odpowiednie, dobre praktyki na poziomie organizacyjnym.

I. Ogólne zasady
   a. Świadomość, umiejętności i upodmiotowienie

   Wszyscy partnerzy powinni rozumieć ryzyko związane z bezpieczeństwem cyfrowym i umieć sobie z nim radzić.

Wszyscy uczestnicy powinni mieć świadomość, że ryzyko związane z bezpieczeństwem cyfrowym może wpływać na osiąganie ich ekonomicznych i społecznych celów, a ich sposób zarządzania tym zagrożeniem ma wpływ na innych ludzi. Powinni posiadać wiedzę i umiejętności niezbędne

[72] *Digital Security Risk Management for Economic and Social Prosperity OECD*, b.d., http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

do zrozumienia tego ryzyka, co z kolei może okazać się pomocne w zarządzaniu ryzykiem oraz ocenie potencjalnego wpływu podejmowanych decyzji dotyczących zarządzania bezpieczeństwem cyfrowym na działalność nie tylko ich, ale także całego środowiska cyfrowego.

b. Odpowiedzialność

Wszyscy partnerzy powinni wziąć odpowiedzialność za zarządzanie ryzykiem bezpieczeństwa cyfrowego.

Warto, aby działali zgodnie ze swoją rolą, kontekstem oraz zdolnością do działania w zakresie zarządzania ryzykiem związanym z bezpieczeństwem cyfrowym, a także brali pod rozwagę potencjalne konsekwencje. Powinni uznać, że musi istnieć pewien minimalny poziom ryzyka związanego z bezpieczeństwem cyfrowym umożliwiający osiągnięcie zamierzonych celów społecznych i ekonomicznych.

c. Prawa człowieka oraz fundamentalne wartości

Wszyscy partnerzy powinni zarządzać ryzykiem bezpieczeństwa cyfrowego w przejrzysty i konsekwentny sposób, uwzględniając prawa człowieka i fundamentalne wartości.

Zarządzanie zagrożeniem bezpieczeństwa cyfrowego należy wdrażać w sposób spójny z prawami człowieka i fundamentalnymi wartościami wyznawanymi w demokratycznych społeczeństwach, włącznie z wolnością wypowiedzi, wolnym przepływem wiadomości, poufnością informacji oraz komunikacji, ochroną prywatności i danych osobowych, otwartością, a także sprawiedliwym procesem. Dodatkowo zarządzanie ryzykiem bezpieczeństwa cyfrowego powinno opierać się na etycznym postępowaniu z poszanowaniem i uwzględnieniem uzasadnionych interesów innych ludzi oraz społeczeństwa jako całości. Organizacje powinny prowadzić politykę ogólnej przejrzystości odnośnie do ich praktyk i procedur dotyczących zarządzania ryzykiem związanym z bezpieczeństwem cyfrowym.

d. Współpraca

Wszyscy partnerzy powinni współpracować, włączając w to współpracę międzynarodową.

Wzajemne globalne powiązania tworzą współzależności pomiędzy zainteresowanymi stronami oraz skłaniają do współpracy nad zarządzaniem ryzykiem cyfrowym. Współpraca powinna obejmować wszystkich partnerów, zaangażowane powinny być również rządy, organizacje rządowe

i pozarządowe. Warto, aby współpraca rozciągała się również ponad granicami, tzn. na szczeblu zarówno regionalnym, jak i międzynarodowym.

II. Zasady operacyjne

a. Ocena ryzyka i cykl ciągłego procesu naprawczego

Przywódcy i osoby podejmujące decyzje powinny zapewnić, że ryzyko bezpieczeństwa cyfrowego jest i było traktowane na podstawie ciągłej oceny ryzyka.

Ocenę ryzyka bezpieczeństwa cyfrowego należy przeprowadzać systematycznie i cyklicznie. Ocena powinna dotyczyć potencjalnych konsekwencji i zagrożeń, z uwzględnieniem podatności zagrożonej działalności gospodarczej i społecznej, jak również dostarczać informacji o procedurze podejmowania decyzji dotyczących zmniejszenia ryzyka. Minimalizacja zagrożenia powinna być ukierunkowana na zmniejszenie ryzyka do poziomu akceptowalnego w stosunku do spodziewanych korzyści, jednocześnie uwzględniając ewentualny wpływ na uzasadnione interesy innych. Ciągły proces naprawczy obejmuje różne opcje takie jak akceptację, redukcję, unikanie ryzyka lub kombinację wymienionych opcji.

b. Środki ochrony

Przywódcy i osoby podejmujące decyzje powinni, upewnić się, czy środki ochrony są odpowiednie i współmierne do ryzyka.

Ocena ryzyka bezpieczeństwa cyfrowego powinna wskazywać na wybór, działanie i poprawę środków bezpieczeństwa w celu zmniejszenia ryzyka cyfrowego bezpieczeństwa do poziomu akceptowalnego i określonego w ocenie ryzyka oraz procesie naprawczym. Środki ochrony powinny być odpowiednie i współmierne do ryzyka, a ich wybór powinien uwzględniać ich potencjalny pozytywny i negatywny wpływ na działania gospodarcze oraz społeczne, które mają na celu ochronę w zakresie praw człowieka, fundamentalnych wartości oraz uzasadnionych interesów innych. Wszystkim rodzajom środków należy przyjrzeć się pod kątem ich powiązania fizycznego i cyfrowego z ludźmi, procesami czy technologiami zaangażowanymi w podejmowane działania. Organizacje powinny szukać luk w zabezpieczeniach oraz reagować na nie możliwie szybko i we właściwy sposób.

c. Innowacje

Przywódcy i osoby podejmujące decyzje powinny upewnić się, że przyjęto plan gotowości i ciągłości.

Innowacje należy traktować jako integralną część strategii obniżania ryzyka cyfrowego bezpieczeństwa do akceptowalnego poziomu określonego w ocenie ryzyka oraz planie naprawczym. Innowacje należy wspierać we wszelkich działaniach podejmowanych w środowisku cyfrowym, ze szczególnym uwzględnieniem tworzenia i rozwoju środków bezpieczeństwa.

d. Gotowość i ciągłość

Przywódcy i osoby podejmujące decyzje powinny upewnić się, że przyjęto plan gotowości i ciągłości.

Bazując na ocenie ryzyka bezpieczeństwa cyfrowego, plan gotowości i ciągłości powinien zostać przyjęty, tak aby zmniejszyć negatywne efekty incydentów związanych z bezpieczeństwem i wesprzeć ciągłość oraz wytrzymałość działalności społecznej i ekonomicznej. Zaleca się, by w planie określono środki mające na celu zapobieganie, wykrywanie, reagowanie i odzyskiwanie danych w reakcji na incydenty bezpieczeństwa cyfrowego. Dodatkowo w planie należy zawrzeć mechanizmy przypisywania jasnych poziomów eskalacji eskalacji, opierając się na wielkości i dotkliwości skutków incydentów cyfrowych związanych z bezpieczeństwem oraz ich potencjałem rozszerzania się w środowisku cyfrowym na innych ludzi. Należy również rozważyć włączenie odpowiednich procedur powiadamiania do realizacji planu.

Należy także rozważyć szersze wykorzystanie instrumentów prawnych wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[73]. Regulacje te obejmują obowiązkowo znaczną część sektora energetycznego i bankowo-finansowego[74]. Wspomniane podmioty mogą zostać zaliczone do operatorów usług kluczowych, co skutkowałoby nałożeniem na nie obowiązku stosowania zabezpieczeń systemów informacyjnych służących do świadczenia usług kluczowych, szacowania i zarządzania ryzykiem oraz realizowania procedur dotyczących zarządzania incydentem. Operatorzy ponoszą odpowiedzialność za zapewnienie bezpieczeństwa

[73] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)*, b.d.

[74] *Załącznik nr 1 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)*, b.d.

świadczonych usług kluczowych i ciągłości ich świadczenia. Ich głównym obowiązkiem jest wdrożenie systemu zarządzania bezpieczeństwem, na który składają się zabezpieczenia dotyczące bezpieczeństwa fizycznego, zarządzania ciągłością działania, obsługi i zarządzania incydentem, zarządzania podatnościami, objęcia systemem monitorowania w trybie ciągłym systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej oraz stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa[75].

Wprowadzenie całościowej regulacji dotyczącej cyberbezpieczeństwa może okazać się pomocne w osiągnięciu istotnego celu prewencyjnego, jakim jest budowanie świadomości zagrożeń. Powszechna świadomość występujących w cyberprzestrzeni zagrożeń oraz skutecznych metod zabezpieczenia się przed tego rodzaju zagrożeniami ma kluczowe znaczenie dla funkcjonowania całego systemu cyberbezpieczeństwa. Mimo ogromnego postępu technologicznego i dostępnych narzędzi czynnik ludzki jest wciąż najważniejszym ogniwem bezpieczeństwa w cyberprzestrzeni.

3.3. Podsumowanie i zalecenia końcowe

Zgodnie z opinią uczestników i zaproszonych ekspertów wprowadzenie powyższych rekomendacji wraz z zastosowaniem zaproponowanej metodyki wdrożeniowej znacząco zwiększy świadomość decydentów i społeczeństwa, skutecznie wypromuje postawy praworządności w obszarze działalności finansowej, usprawni działanie antykorupcyjne oraz zwiększy poziom cyberbezpieczeństwa, co pozytywnie wpłynie na redukcję skali przestępczości w omawianych sektorach, jak i w pozostałych obszarach polskiej gospodarki.

Uczestnicy dyskusji podsumowującej trzeci etap projektu badawczego „Prawo, gospodarka i technologie na rzecz zapobiegania przyczynom przestępczości" sformułowali zalecenie końcowe dotyczące stworzenia krajowej inicjatywy mającej na celu wykreowanie spójnej polityki międzysektorowej dotyczącej wdrażania rozwiązań z zakresu przeciwdziałania przestępczości.

[75] *Druk nr 2505 (Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa)*, b.d.

Oto najważniejsze wnioski trzeciego etapu seminariów prowadzonych w ramach niniejszego projektu badawczego:

- wdrożenie rozwiązań zapobiegających przestępczości musi opierać się nie tylko na formalnej strukturze organizacyjnej, lecz również na nieformalnych relacjach pomiędzy pracownikami danej organizacji;
- dla wdrożenia rozwiązań w zakresie zapobiegania przestępczości konieczne jest pozyskanie sojuszników; pracownicy danej organizacji, mieszkańcy miasta, obywatele państwa godzą się na wprowadzanie zmian zapewniających im bezpieczeństwo tylko wówczas, kiedy sami je poznają i zrozumieją; w przeciwnym razie potencjalni beneficjenci zmian okażą się ich przeciwnikami;
- koszty wdrożeń rozwiązań zapobiegających przestępczości są uzależnione od poziomu skomplikowania struktury organizacyjnej i procesów zarządczych występujących w organizacjach; im wyższy poziom skomplikowania tych struktur, tym dłuższy czas wdrożenia i tym wyższe koszty;
- przeciwdziałanie przestępczości rozpoczyna się nie w momencie stwierdzenia popełnienia przestępstwa lub rozpoczęcia jego ścigania, lecz w chwili projektowania i wdrażania rozwiązań organizacyjnych ukierunkowanych na przejrzystość działań organizacji; wyższa transparentność zniechęci potencjalnych przestępców do podejmowania prób oszustw, defraudacji etc.;
- rozwiązania w zakresie *Lean Management* mogą być wdrażane nie tylko w przedsiębiorstwach produkcyjnych, lecz również w przedsiębiorstwach z każdego sektora gospodarki, włączając w to sektor usług i administrację publiczną; we wszystkich tych podmiotach rozwiązania te przynoszą dobre rezultaty w zakresie zapobiegania przestępczości;
- sieci powiązań nieformalnych stanowią znaczne ułatwienie w procesie pozyskiwania sojuszników na rzecz wdrożenia zmian w organizacjach;
- analizę sieci powiązań można również wykorzystać jako narzędzie identyfikacji pracowników o zwiększonej skłonności do popełniania nadużyć. Niemniej jednak bardzo istotnym elementem tego procesu jest ciągłe monitorowanie sieci nieformalnych, a dzieje się tak z uwagi na ich zmienność w czasie;

- jednym ze sposobów wdrażania nowych rozwiązań na poziomie organizacji i kraju jest stosowanie metodyki rozwoju inteligentnych miast w drodze podejmowania lokalnych inicjatyw;
- koncepcja inteligentnych miast stanowi środek przeciwdziałania przestępczości na drodze niwelowania nierówności społecznych i promowania postaw praworządności;
- podstawowym czynnikiem sukcesu w ramach wdrażania zmian w organizacjach jest stworzenie sprzyjających okoliczności, a w szczególności powszechnej potrzeby wprowadzenia zmian; z uwagi na powszechny charakter zjawiska czynnik ten ma szczególne znaczenie w przypadku rozwiązań mających na celu zapobieganie przestępczości; z tego powodu przeprowadzona przez uczestników seminariów analiza w znacznej mierze skoncentrowała się na omówieniu skali zjawiska przestępczości w Polsce;
- proces wprowadzania zmian musi obejmować stworzenie wizji pozwalającej na skuteczne zaplanowanie działań krótko- i długoterminowych; ponadto ważne jest również, aby sformułowana wizja charakteryzowała się wysokim stopniem transparentności pozwalającym na zaangażowanie pracowników wszystkich szczebli w proces wprowadzania zmian;
- sformułowana strategia powinna zawierać mierzalne cele krótkoterminowe umożliwiające uwidocznienie postępów w procesie wdrażania rozwiązań i związanych z nimi efektów, a także odpowiednie nagradzanie osób odpowiedzialnych za wdrażanie zmian;
- istotnym elementem strategii wdrażania rozwiązań na rzecz zwalczania cyberprzestępczości jest ustanowienie procedury zgłaszania i reagowania na cyberatak;
- wdrażanie zmian i rozwiązań w organizacji to nie jednorazowy wysiłek, lecz ciągły proces. Kluczowe znaczenie dla zachowania skuteczności wprowadzanego rozwiązania ma ustawiczna adaptacja do zmiennych uwarunkowań wewnętrznych i zewnętrznych;
- tworzenie wizji strategicznej wdrażania zmian powinno ponadto obejmować aspekty związane z kapitałem ludzkim, włączając w to wprowadzanie stosownej kultury zgodności;
- przejrzystość i odpowiednie przekazanie wypracowanej strategii to jeden z kluczowych elementów wdrażania zmian w organizacjach;

szczególne znaczenie ma promowanie odpowiednich postaw w drodze naśladowania postaw reprezentowanych przez członków koalicji przewodniczącej wprowadzaniu rozwiązania;
- na rzecz zachowania ciągłości operacyjnej wdrażanego rozwiązania konieczne jest ustanowienie odpowiedniego organu nadzorującego dalszy rozwój zmiany, jak również zasady jego funkcjonowania;
- proces wdrażania danego rozwiązania stanowi sprzyjającą okoliczność dla wprowadzania dalszych zmian, co jest szczególnie istotne w przypadku złożonego procesu przeciwdziałania przestępczości, który to proces wymaga ciągłej adaptacji do zmiennych warunków;
- w ramach zapewniania ciągłości operacyjnej rozwiązania przeciwdziałającego przestępstwom, strategia wdrożenia zmiany powinna zawierać cykliczny program szkoleniowo-informacyjny mający na celu utrzymanie wysokiego poziomu bezpieczeństwa w organizacji i poczucia celu w dalszym stosowaniu wdrażanego rozwiązania; ma to szczególne znaczenie podczas wprowadzania rozwiązań na rzecz zapobiegania cyberatakom, które stanowią jeden z najbardziej dynamicznie rozwijających się obszarów przestępczości.

Część wniosków sformułowanych przez uczestników można uznać za proste obserwacje dotyczące istniejących zjawisk i zależności. Jednakże wybrana metoda seminaryjna, oparta na analizie studiów przypadków, sprzyja przede wszystkim lepszemu zrozumieniu zjawisk przez osoby zaangażowane w proces budowania odporności organizacji na ewentualne zagrożenia. W przypadku przedstawicieli wyższej kadry kierowniczej przedsiębiorstw państwowych i prywatnych przyjęta metoda służy również właściwej ocenie skali zjawisk, umieszczenia ich we właściwym kontekście i praktycznego wykorzystania odpowiednich instrumentów zaradczych w praktyce. Opinie uczestników potwierdzają, że ma to szczególne znaczenie w procesie przeciwdziałania przestępczości, gdzie sama literatura przedmiotu nie wystarcza dla pełnego zrozumienia zachodzących zjawisk, a konieczne staje się przeprowadzenie odpowiednio ukierunkowanej dyskusji.

Podziękowania

Podsumowane w niniejszym raporcie badania, jak również cały projekt badawczy „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" nie osiągnęłyby zakładanych celów bez zaangażowania grona zaproszonych uczestników, którzy hojnie dzielili się swoimi doświadczeniami wyniesionymi z wieloletniej służby na rzecz rozwoju, dobrobytu i bezpieczeństwa Rzeczypospolitej. Bez ich wnikliwych uwag i spostrzeżeń raport ten nie doszedłby do skutku.

Załącznik A. Informacje uzupełniające dotyczące prelegentów

Adrian Done, Ph.D.

POPROWADZONE PANELE	• Managing operations: simulation exercise • Managing people in service operations: Shouldice Hospital case
AKTUALNIE PEŁNIONE FUNKCJE	• Konsultant • Inwestor prywatny
NAJWAŻNIEJSZE PUBLIKACJE[76]	1. Done, C. Voss, N. G. Rytter, „Best practice interventions: Short-term impact and long-term outcomes", *Journal of Operations Management*, t. 29, nr 5, s. 500–513, lip. 2011. 2. Done, *Global Trends.* London: Palgrave Macmillan UK, 2012. 3. Done, „Supply-chain evolution: Knowledge-based perspectives", *IESE Business School*, 2011. 4. Done, „Supply chain knowledge management: A conceptual framework", *IESE Business School*, nr D/900, 2011. 5. Done, „Developing supply chain maturity", *IESE Business School*, 2011.

[76] Pięć najczęściej cytowanych prac spośród dorobku naukowego. Selekcja na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 25.11.2018).

Massimo Maoret, Ph.D.

POPROWADZONE PANELE	• Leading organizational change • Visualizing and understanding your network • Mastering organizational networks
AKTUALNIE PEŁNIONE FUNKCJE	• Adiunkt, Strategic Management Department w IESE Business School • Stypendysta, program *European Commission Marie Skłodowska-Curie Fellowship*
NAJWAŻNIEJSZE PUBLIKACJE[77]	1. C. Jones, F. G. Massa, M. Maoret, „Toward a Projects as Events Perspective", *Project-Based Organizing and Strategic Management*, t. 28, 0 t., Emerald Group Publishing Limited, 2011, s. 427–444. 2. C. Jones, M. Maoret, „Frontiers of Creative Industries: Exploring Structural and Categorical Dynamics", *Frontiers of Creative Industries: Exploring Structural and Categorical Dynamics*, t. 55, 0 t., Emerald Publishing Limited, 2018, s. 1–16. 3. F. Fonti, M. Maoret, R. Whitbred, „Free-riding in multi-party alliances: The role of perceived alliance effectiveness and peers' collaboration in a research consortium", *Strategic Management Journal*, t. 38, nr 2, s. 363–383, 2017. 4. F. Fonti, M. Maoret, „The direct and indirect effects of core and peripheral social capital on organizational performance", *Strategic Management Journal*, t. 37, nr 8, s. 1765–1786, 2016. 5. M. Maoret, „Reunited: Exploring the performance effects of newcomers' tie reactivation.", *Proceedings*, t. 2013, nr 1, s. 16605, sty. 2013.

Silvia King

POPROWADZONE PANELE	• City of Atlanta Police / US Department of Homeland Security – Implementing intelligence-led policing through advanced technology
AKTUALNIE PEŁNIONE FUNKCJE	• Senior Research Fellow w Center for Business in Society (IESE Business School) • Partner w i2O
NAJWAŻNIEJSZE PUBLIKACJE	1. Miller, C. S., King, S. M., 2007. *Southern Company: A Case Study in Corporate Responsibility Leadership.* International Corporate Responsibility Series, 3, 101–128. 2. Miller, C. S., King, S. M., 2008. *Transparency as the nexus between csr and financial and business model performance: a lesson for management.* Transparency, information and communication technology: social responsibility and accountability in business and education, 117. 3. Vaccaro, A., King, S., 2018. *Cybersecurity and Fraud in the Banking and Energy Sectors: Current landscape, best practices and organizational approaches – and options for Poland.* Zgłoszone do publikacji – czerwiec 2018

[77] Pięć najczęściej cytowanych prac spośród dorobku naukowego. Selekcja na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 25.11.2018).

Lucien Randazzese, Ph.D.

POPROWADZONE PANELE	• The Challenges of future Cities • Leadership in future Cities
AKTUALNIE PEŁNIONE FUNKCJE	• Dyrektor Center for Innovation Strategy and Policy w SRI International
NAJWAŻNIEJSZE PUBLIKACJE[78]	1. W. M. Cohen, R. Florida, L. Randazzese, J. Walsh, „Industry and the Academy: Uneasy Partners in the Cause of Technological Advance", *Challenges to Research Universities*, t. 171, nr 200, s. 59, 1998. 2. E. Kenneally, L. Randazzese, D. Balenson, „Cyber Risk Economics Capability Gaps Research Strategy", *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2018, s. 1–6. 3. L. P. Randazzese, „Exploring University-Industry Technology Transfer of CAD Technology", *IEEE Transactions on Engineering Management*, t. 43, nr 4, s. 393–401, 11.1996. 4. L. Randazzese, *Helios: Understanding Solar Evolution Through Text Analytics*, DE--EE0006130, 1336902, 12.2016. 5. L. P. Randazzese, *Semiconductor Subsidies, Scientific American*, t. 274, nr 6, s. 46–49, 1996.

[78] Pięć najczęściej cytowanych prac spośród dorobku naukowego. Selekcja na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 25.11.2018).

Załącznik B. Kwestionariusz ankietowy

(zachowano oryginalne formatowanie kwestionariusza)

Profil uczestnika oraz reprezentowanej organizacji

Doświadczenie zawodowe (w latach)	☐ <5	☐ 5–14	☐ 15–25	☐ > 25	
Typ organizacji	☐ przedsiębiorstwo	☐ instytucja rządowa bądź samorządowa	☐ instytucja niekomercyjna		
Wielkość organizacji (wg liczby pracowników)	☐ mała (<50)	☐ średnia (51–250)	☐ duża (>250)		
Reprezentowany sektor	☐ finanse	☐ ubez-pieczenia	☐ energia	☐ admini-stracja państwowa	☐ inne

Wyraź swoją opinię w poniższych kwestiach posługując się następującą skalą:

1 – Zdecydowanie nie; 2 – Raczej nie; 3 – Nie mam zdania; 4 – Raczej tak; 5 – Zdecydowanie tak

Transforming people and organizations

1. Czy uważa Pan/Pani, że zaprezentowane rozwiązania można by wdrożyć w organizacji, którą Pan/Pani reprezentuje?	1	2	3	4	5
2. Czy wdrożenie zaprezentowanych rozwiązań pozwoliłoby na zwiększenie wykrywalności przestępstw w organizacji, którą Pan/Pani reprezentuje?	1	2	3	4	5
3. Czy wdrożenie zaprezentowanych rozwiązań pozwoliłoby na uzyskanie większej efektywności?	1	2	3	4	5

4. Czy uważa Pan/Pani, że istniejące w Polsce regulacje prawne pozwalają na wdrożenie innowacji z zakresu zwalczania przestępczości prezentowanych na seminarium?	1	2	3	4	5
5. Czy uważa Pan/Pani, że regulacje prawne dotyczące wprowadzania innowacyjnych rozwiązań z zakresu zwalczania przestępczości w Polsce powinny ulec zmianie?	1	2	3	4	5
6. Czy uważa Pan/Pani, że uwarunkowania kulturowo-społeczne w Polsce sprzyjają wprowadzaniu innowacyjnych rozwiązań z zakresu zwalczania przestępczości?	1	2	3	4	5
7. Najważniejsze czynniki sprzyjające wdrażaniu nowych rozwiązań w zakresie bezpieczeństwa to:					
a. poczucie konieczności wprowadzenia zmian	1	2	3	4	5
b. tworzenie koalicji dla wprowadzenia zmian	1	2	3	4	5
c. tworzenie strategii oraz planu wdrażania	1	2	3	4	5
d. transparentność procesu oraz celów	1	2	3	4	5
e. gotowość na sprostanie wszelkim zagrożeniom	1	2	3	4	5
f. inny:	1	2	3	4	5
8. Sektor, w którym szczególnie potrzebne jest wdrożenie nowych rozwiązań z zakresu zwalczania przestępczości, to:					
a. sektor finansowy	1	2	3	4	5
b. sektor ubezpieczeń	1	2	3	4	5
c. sektor energetyki	1	2	3	4	5
d. handel detaliczny	1	2	3	4	5
e. handel hurtowy					
f. transport	1	2	3	4	5
g. inny:	1	2	3	4	5

Spis rysunków

Spis tabel

Bibliografia

Adamczyk M., *Przestępstwa stwierdzone a postępowania wszczęte i ich wykrywalność w Polsce w latach 2000–2012*, w: „Security, Economy & Law", b.d., nr 1/2016, s. 18–36.

Austin G., *Cyber Policy in China*, John Wiley & Sons, Cambridge, UK, 2014.

Bożewicz M., *Poczucie bezpieczeństwa i zagrożenia przestępczością*, Centrum Badania Opinii Społecznej (CBOS), 11.05.2018, https://www.cbos.pl/SPISKOM.POL/2018/K_061_18.PDF

Burton M.D., Lawrence K., *Jerry Sanders*, „Harvard Business Review Case Study", 1998, Leadership & Managing People.

Czepil B., *Kulturowe uwarunkowania korupcji w systemie demokratycznym i niedemokratycznym na przykładzie USA i ZSRR*, 2008, http://www.antykorupcja.gov.pl/download/4/8767/Kulturoweuwarunkowaniakorupcjiwsystemiedemokratycznyminiedemokratycznymnaprzykla.pdf

Czernek K., Jurek M., Marszałek P., *Mapa edukacji finansowej VI edycja*, Związek Banków Polskich, Poznań 03.2017, https://zbp.pl/dla-konsumentow/edukacja-ekonomiczna

Dominski R., *The Importance of Financial Literacy for a Secure Future*, 16.10.2017, https://www.washingtonpost.com/sf/brand-connect/wp/2017/10/16/usbank/the-importance-of-financial-literacy-for-a-secure-future/?utm_term=.b5d57e19b61a

Duke E.A., *The Importance of Financial Education*, zaprezentowano na Jump$tart Coalition Investing in Our Future: Financial Education and Washington Event, Washington 2010, https://www.federalreserve.gov/newsevents/speech/files/duke20100408a.pdf

Heskett J.L., *Shouldice Hospital Limited*, 1983, Harvard Business School Case 683-068.

Kotter J.P., *Leading Change*, Harvard Business School Press, Boston, Mass 1996.

———, *Leading Change: Why Transformation Efforts Fail*, „Harvard Business Review", 2007, t.85, nr 1, s. 96–103.

Lewicka-Strzałecka A., *Moralność finansowa Polaków Raport z badań*, Konferencja Przedsiębiorstw Finansowych w Polsce, Gdańsk-Warszawa 06.2018.

McPherson M., Smith-Lovin L., Cook J.M., *Birds of a Feather: Homophily in Social Networks*, „Annual Review of Sociology", 2001, t.27, nr 1, s. 415–444.

Mukunda G., Mazzanti L., Sesia A., *Cynthia Carroll at Anglo American (A)*, 2013, Harvard Business School Case 414–019.

Pérez López J.A., *Teoría de la acción humana en las organizaciones*, Rialp, Madryt 1991.

Poulsen P.B., Adamsen S., Vondeling H., Jørgensen T., *Diffusion of Laparoscopic Technologies in Denmark*, „Health Policy", 1998, t. 45, nr 2, s. 149–167.

Rudke M., *Banki: ile tracą na oszustwach pracowników i wyłudzeniach?*, 26.06.2018, https://www.parkiet.com/Parkiet-PLUS/306269958-Banki-ile-traca-na-oszustwach-pracownikow-i-wyludzeniach.html

Vella M., Calamatta C., *Why is Financial Education Important?*, b.d., Times of Malta wydanie, https://www.timesofmalta.com/articles/view/20180703/business-comment/why-is-financial-education-important.683446

Woan Jinq L., Yazdanifard R., *The Alarming Trend of Sexual Harassment Occurrences in the Workplace and What Can Be Done*, „International Journal of Management, Accounting and Economics", 2015, t.2, nr 5.

Recommendation on Principles and Good Practices for Financial Education and Awareness, Convention on the Organisation for Economic Co-operation and Development 07.2005, https://www.oecd.org/daf/fin/financial-education/35108560.pdf

Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions, Organisation for Economic Co-operation and Development (OECD), 26.11.2009, http://www.oecd.org/corruption/anti-bribery/anti-briberyconvention/oecdantibriberyrecommendation2009.htm

Raport o stanie bezpieczeństwa w Polsce w 2015 roku, Ministerstwo Spraw Wewnętrznych i Administracji 2015, https://bip.mswia.gov.pl/download/4/29642/file.file

Raport o stanie bezpieczeństwa w Polsce w 2016 roku, Ministerstwo Spraw Wewnętrznych i Administracji 2016, https://bip.mswia.gov.pl/download/4/31673/RaportostaniebezpieczenstwawPolscew2016roku.pdf

Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/obbc7a32-64df-b45e-b08c-dac59415f109

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku, Rządowy Zespół Reagowania Na Incydenty Komputerowe CERT.GOV.PL 2017, https://csirt.gov.pl/download/3/186/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2017roku.pdf

Cyber Security Breaches Survey 2018, Department for Digital, Culture, Media and Sport, London 2018, https://assets.publishing.service.gov.uk/government/

uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Atlanta Police Department: History of the APD, b.d., http://www.atlantapd.org/about-apd/apd-history (dostęp: 31.01.2019).

A/RES/3/217 A – Universal Declaration of Human Rights – UN Documents: Gathering a Body of Global Agreements, b.d., http://www.un-documents.net/a3r217a.htm (dostęp: 9.02.2019).

About Shouldice Hernia Clinic | Hernia Repair and Treatment Hospital Canada, b.d., https://www.shouldice.com/about/

Digital Security Risk Management for Economic and Social Prosperity OECD, b.d., http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), b.d.

Załącznik nr 1 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), b.d.

Druk nr 2505 (Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa), b.d.

CZĘŚĆ DRUGA

ZESPÓŁ IMPLEMENTACYJNY

AUTORZY:

Bartłomiej ORĘZIAK, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Marcin WIELEC, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Alina KLONOWSKA, Uniwersytet Ekonomiczny w Krakowie
Magdalena MAŁECKA-ŁYSZCZEK, Uniwersytet Ekonomiczny w Krakowie
Małgorzata SNARSKA, Uniwersytet Jagielloński
Joanna WYROBEK, Uniwersytet Ekonomiczny w Krakowie
Remigiusz ROSICKI, Uniwersytet im. Adama Mickiewicza w Poznaniu
Tomasz JEDYNAK, Uniwersytet Ekonomiczny w Krakowie
Artur MEZGLEWSKI, Akademia Sztuki Wojennej

ROZDZIAŁ I

Transforming People and Organizations. Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w kontekście implementacji najnowszych rozwiązań prawnych oraz organizacyjnych

BARTŁOMIEJ ORĘZIAK[1], MARCIN WIELEC[2]

1. Transforming People and Organizations: Wprowadzenie

Moduł „Transforming People and Organizations" dokonywał naukowej oceny metod zapobiegania przestępczości w module „Improving Performance" i odpowiadał na pytanie, jak rozwiązania te mogą zmieniać funkcjonowanie organizacji oraz ludzkie zachowania. Z tego powodu prawidłowa realizacja międzynarodowego projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości"[3] wymagała kolejnego etapu pogłębienia problematyki rynku finansowego, energetycznego, ubezpieczeniowego oraz zarządzania ludźmi w organizacji, aby wypracować analizy „Transforming People and Organizations". Zagadnieniem przewodnim było

[1] Doktorant w Katedrze Ochrony Praw Człowieka i Prawa Międzynarodowego Humanitarnego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Laureat Stypendium Ministra Nauki i Szkolnictwa Wyższego za wybitne osiągnięcia naukowe na rok akademicki 2017/18. Główne zainteresowania badawcze: prawo karne, prawo międzynarodowe, ochrona praw człowieka oraz prawo nowych technologii.

[2] Adiunkt w Katedrze Postępowania Karnego WPiA UKSW, pełni obowiązki kierownika Katedry Postępowania Karnego. Specjalista z zakresu prawa karnego procesowego, prawa karnego, prawa karnego wykonawczego oraz prawa karnego skarbowego, prawa i postępowania dyscyplinarnego. Autor artykułów naukowych, książek prawniczych i ekspertyz. Dyrektor Instytutu Wymiaru Sprawiedliwości, adwokat.

[3] Strona internetowa Projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" w strukturze Centrum Analiz Strategicznych Instytutu Wymiaru Sprawiedliwości, https://iws.gov.pl/centrum-analiz-strategicznych/prawo-gospodarka-i-technologia-na-rzecz-zapobiegania-przyczynom-przestepczosci/

Główna strona Projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości", https://iws.gov.pl/projekt-2/

opracowanie wdrożenia metod i instrumentów zapobiegania przestępczości (komparatystyczne ujęcie polskich problemów) na tle starannie wyselekcjonowanych zagadnień wspierających główne założenia projektowe. Niemniej jednak całościowo oraz finalnie prowadzone badania miały zamiar zwrócić uwagę na podejście analityczne dotyczące rynku finansowego, ubezpieczeniowego, energetycznego oraz zarządzania ludźmi w organizacji z wykorzystaniem technologii zapobiegającej przyczynom przestępczości nie tylko w wymiarze Transforming People and Organizations[4][5], ale także w świetle modułów Assessing Foundations, Improving Performance[6], oraz Heading Into the Future[7]. Oznacza to, że starano się skoncentrować na przedmiotowej problematyce oraz ewaluacji poziomu zaawansowania i zakresu wykorzystania takich technologii. Warto zasygnalizować również, że podczas prac projektowych pozyskano, a także zaktualizowano wiedzę na temat zagranicznych rozwiązań i zagrożeń dla podstawowych zasad polskiego porządku normatywnego. Natomiast zgodnie z założeniem wstępnym prac projektowych analiza przyczyn powstawania sytuacji, w których dochodzi do przestępstw w obszarze rynku finansowego, ubezpieczeniowego, energetycznego oraz zarządzania ludźmi w organizacji, została zakwalifikowana jako główny obszar badawczy oraz analityczny pryzmat Projektu[8], niezależnie od wewnętrznego podziału modułowego.

---

[4] Celem modułu Transforming People & Organisations było przybliżenie w jaki sposób te rozwiązania mogą zmieniać organizacje i ludzkie zachowania.

[5] Celem modułu Assessing Foundations było zidentyfikowanie problemu przestępczości w Polsce w świetle wybranych sektorów polskiej gospodarki.

[6] Celem modułu Improving Performance było znalezienie rozwiązań zidentyfikowanych problemów.

[7] Celem modułu Heading into the Future było debatowanie nad przyszłością i przyszłymi zmianami np. technologicznymi.

[8] Jednym ze sposobów realizacji przedmiotowego celu są publikacje będące wynikiem prac Zespołu Implementacyjnego finansowanego w ramach Projektu: G. Blicharz, B. Oręziak, M. Wielec (red.), *Rynek finansowy. Zapobieganie przyczynom przestępczości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2019; Ł. Wojcieszak, B. Oręziak, M. Wielec (red.), *Rynek energetyczny. Zapobieganie przyczynom przestępczości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości Warszawa 2019; M. Płonka, B. Oręziak, M. Wielec (red.), R*ynek ubezpieczeniowy. Zapobieganie przyczynom przestępczości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości Warszawa 2019; J. Taczkowska-Olszewska, B. Oręziak, M. Wielec (red.), *Zarządzanie Ludźmi w Organizacji. Zapobieganie przyczynom przestępczości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2019.

2. Transforming People and Organizations: Przedmiot prac

Transforming People and Organizations głównie polegało na przedstawieniu założeń związanych z implementacją najnowszych rozwiązań prawnych oraz organizacyjnych z zakresu przeciwdziałania przestępczości. Moduł Transforming People and Organizations został poświęcony problematyce zmian w organizacjach promujących postawy praworządności w aspektach związanych z bezpieczeństwem cybernetycznym w poszczególnych obszarach, wdrażania strategii biznesowych oraz zarządzania zmianą, a także analizy problemów przestępczości na rynku finansowym, energetycznym, ubezpieczeniowym oraz w zarządzaniu ludźmi w organizacji. Ponadto poruszono kwestie wdrożenia rozwiązań dla poszczególnych obszarów badawczych w Polsce. Relewantne dla przedmiotu prowadzonych badań okazały się zagadnienia dotyczące optymalnego modelu współpracy jednostek organizacyjnych oraz zagadnienia skuteczności stosowania zaawansowanych metod analitycznych w przeciwdziałaniu przestępczości.

Odpowiednie sprofilowanie wskazanych poniżej segmentów badawczych umożliwiło dokonanie analizy typu Transforming People and Organizations na rynku finansowym. Mowa tutaj o implementacji najnowszych rozwiązań prawnych oraz organizacyjnych z zakresu przeciwdziałania przestępczości, czyli zwrócenia uwagi w stronę: rozwiązań organizacyjnych ułatwiających zachowanie kontroli instytucji finansowej nad operacjami realizowanymi przez jej pracowników, procesu podejmowania decyzji, zarządzania operacjami i zarządzania ryzykiem w instytucjach finansowych, przygotowania obrony przed różnymi formami ataków na instytucje finansowe, działalności międzynarodowych grup przestępczych oraz metod zapobiegania im w instytucjach finansowych, jak i przestępstw finansowych dokonywanych przez klientów instytucji finansowych oraz metod zapobiegania im.

Odpowiednie sprofilowanie wskazanych poniżej segmentów badawczych umożliwiło dokonanie analizy typu Transforming People and Organizations na rynku energetycznym. Mowa tutaj o implementacji najnowszych rozwiązań prawnych oraz organizacyjnych z zakresu przeciwdziałania przestępczości, czyli zwrócenia uwagi w stronę: procesu podejmowania decyzji, zarządzania ryzykiem i operacjami oraz przestępstw, zorganizowanej przestępczości na rynku energetycznym, wykorzystania nowoczesnych technologii w energetyce,

jak i form dokonywania przestępstw na rynku energetycznym oraz metod zapobiegania im.

Odpowiednie sprofilowanie wskazanych poniżej segmentów badawczych umożliwiło dokonanie analizy typu Transforming People and Organizations na rynku ubezpieczeniowym. Mowa tutaj o implementacji najnowszych rozwiązań prawnych oraz organizacyjnych z zakresu przeciwdziałania przestępczości, czyli zwrócenia uwagi w stronę: procesu podejmowania decyzji w zakładzie ubezpieczeń, zarządzania ryzykiem na rynku ubezpieczeniowym, zarządzania operacjami w zakładzie ubezpieczeń, skali zjawiska przestępczości ubezpieczeniowej w Polsce wraz z identyfikacją głównych przyczyn jej występowania, skuteczności kierowania zawiadomień o podejrzeniu popełnienia przestępstwa przez zakład ubezpieczeń, przyczyn odmów wszczęcia postępowania oraz umorzeń postępowania (wraz z wypracowaniem rekomendacji postępowania dla zakładów ubezpieczeń podczas składania zawiadomień o podejrzeniu popełnienia przestępstwa), optymalnego modelu współpracy jednostek państwowych z zakładami ubezpieczeń, w tym wymiany danych celem skutecznego przeciwdziałania nadużyciom, problematyki skuteczności stosowania zaawansowanych metod analitycznych (analizy Big Data oraz techniki predykcyjne) w przeciwdziałaniu przestępczości ubezpieczeniowej, skuteczności nałożenia obowiązku naprawienia szkody wobec zakładu ubezpieczeń oraz statystki powrotu skazanych do działalności przestępczej wobec Towarzystw Ubezpieczeniowych w kontekście zapobiegania przyczynom przestępczości, jak i charakterystyki osób najczęściej popełniających przestępstwa ubezpieczeniowe (wzorzec Fraudera).

Odpowiednie sprofilowanie wskazanych poniżej segmentów badawczych umożliwiło dokonanie analizy typu Transforming People and Organizations w zarządzaniu ludźmi w organizacji. Mowa tutaj o implementacji najnowszych rozwiązań prawnych oraz organizacyjnych z zakresu przeciwdziałania przestępczości, czyli zwrócenia uwagi w stronę: prawa pracy, pakietów socjalnych i ich wykorzystania w świetle przepisów prawnych, ochrony danych osobowych w Polsce, Europie i na świecie, odpowiedzialności prawnej dyrektorów personalnych, *compliance* jako narzędzia zarządzania ryzykiem prawnym, kompetencji dyrektora personalnego i roli zarządzania ludźmi organizacji, problematyki różnorodności płci, kultur i generacji jako potencjału organizacyjnego, nowych standardów bezpieczeństwa w otoczeniu cyfrowym,

procesu negocjacji, stylów przywódczych, w tym przywództwa przez wartość, satysfakcji z równowagi w życiu zawodowym i rodzinnym, jak i masowych rekrutacji oraz zastosowania nowoczesnych technologii.

3. Transforming People and Organizations: Metodologia

Z uwagi na fakt, że każdy z modułów realizowanych w ramach prac projektowych stanowił część całości projektu, metodologia została przyjęta w sposób podobny do wcześniejszych części, w tym skupiała się na kryteriach ewaluacyjnych[9]. Zgodnie z tym wykorzystano klasyczną dla nauk prawnych metodę dogmatyczno-formalną oraz metodę prawno-porównawczą. W ramach tej ostatniej posłużono się metodą komparatystyki prawniczej Kötza i Zweigerta, która posiada pięć faz: a) sformułowanie problemu; b) wybór materiału do porównania; c) właściwe porównanie; d) budowanie systemu uwzględniającego rezultaty porównania w praktyce; e) krytyczna ocena wyników osiągniętych poprzez porównanie[10]. Do instrumentarium badawczego należały także inne metody: heurystyczne (odroczone wartościowanie, transpozycja, sugerowanie oraz metody złożone), funkcjonalne (hermeneutyka swobodna), analizy i krytyki piśmiennictwa, analizy i konstrukcji logicznej, badania dokumentów, monograficzne oraz obserwacyjne. Jako uzupełnienie powyższego, określono mate-językowo wskaźnik wpływu (liczba wypracowanych rozwiązań włączonych do głównego nurtu polityki; liczba wdrożonych strategii, dokumentów operacyjnych i konkretnych rozwiązań; liczba instytucji korzystających z wypracowanych rozwiązań; liczba osób korzystających z wypracowanych rozwiązań) i/albo wskaźnik rezultatu (liczba zakończonych pilotaży (wdrożeń) wypracowanych rozwiązań; liczba osób zaangażowanych w wypracowanie rozwiązań; liczba publikacji, w tym publikacji internetowych, na temat wypracowanych rozwiązań) i/albo wskaźnik produktu (liczba wypracowanych diagnoz; liczba wypracowanych polityk,

[9] Np. oryginalność, racjonalnośći praktyczność teorii, perspektywa, kompleksowość oraz kompatybilność badań, prawdopodobieństwo i perspektywa zastosowania, korzyści ekonomiczne oraz społeczne, promowanie efektów, przejrzystość i przystępność.

[10] Zob. ogólnie: R. Tokarczyk, *Komparatystyka prawnicza*, Warszawa 2008.

strategii oraz dokumentów operacyjnych; liczba opracowanych rozwiązań; liczba pilotaży (wdrożeń) wypracowanych rozwiązań).

4. Transforming People and Organizations: Potencjalni beneficjenci prac projektowych

Niezależnie od podziału modułowego każdy z obszarów (finanse, ubezpieczenia, energetyka oraz zarządzanie ludźmi w organizacji) posiada swoją specyficzną listę potencjalnych beneficjentów oraz wspólną listę podmiotów naukowych mogących być zainteresowanymi wynikami prowadzonych analiz. Celem było zbudowanie organizacyjnego obiegu informacji w ramach Projektu: „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości". Powyższego wymagała dystrybucja jasnych, praktycznych oraz użytecznych rekomendacji, wytycznych i wymiernych rezultatów.

LISTA POTENCJALNYCH BENEFICJENTÓW DLA RYNKU FINANSOWEGO

Podmioty państwowe
Agencja Bezpieczeństwa Wewnętrznego
Bankowy Fundusz Gwarancyjny
Centralne Biuro Antykorupcyjne
Kasa Rolniczego Ubezpieczenia Społecznego
Komisja Nadzoru Finansowego
Krajowa Administracja Skarbowa
Krajowy Depozyt Papierów Wartościowych
Ministerstwo Finansów
Ministerstwo Inwestycji i Rozwoju
Ministerstwo Przedsiębiorczości i Technologii
Ministerstwo Sprawiedliwości
Najwyższa Izba Kontroli
Narodowy Bank Polski
Polska Agencja Inwestycji i Handlu

Rzecznik Finansowy
Zakład Ubezpieczeń Społecznych

Podmioty prywatne z udziałem Skarbu Państwa

Agencja Kapitałowo-Rozliczeniowa
Aplikacje Krytyczne
Bank Gospodarstwa Krajowego
Fundusz Rozwoju Spółek
Giełda Papierów Wartościowych w Warszawie
Poczta Polska
Polska Wytwórnia Papierów Wartościowych
Polski Fundusz Rozwoju
Powszechna Kasa Oszczędności Bank Polski
Towarowa Giełda Energii

Integratory

ACCA (Association of Chartered Certified Accountants) Polska
FINEXA – Stowarzyszenie Dyrektorów Finansowych
Izba Domów Maklerskich
Korporacja Ubezpieczeń Kredytów Eksportowych
Polskie Towarzystwo Ekonomiczne
Polskie Towarzystwo Informatyczne
Stowarzyszenie Emitentów Giełdowych
Izba Gospodarcza Towarzystw Emerytalnych
Stowarzyszenie Księgowych w Polsce

LISTA POTENCJALNYCH BENEFICJENTÓW DLA RYNKU UBEZPIECZENIOWEGO

Podmioty państwowe

Agencja Bezpieczeństwa Wewnętrznego
Centralne Biuro Antykorupcyjne
Kasa Rolniczego Ubezpieczenia Społecznego

Komisja Nadzoru Finansowego
Krajowa Administracja Skarbowa
Ministerstwo Finansów
Ministerstwo Inwestycji i Rozwoju
Ministerstwo Przedsiębiorczości i Technologii
Ministerstwo Sprawiedliwości
Ministerstwo Zdrowia
Ministerstwo Rodziny, Pracy i Polityki Społecznej
Najwyższa Izba Kontroli
Rzecznik Finansowy
Ubezpieczeniowy Fundusz Gwarancyjny
Zakład Ubezpieczeń Społecznych
Podmioty prywatne z udziałem Skarbu Państwa
Fundusz Rozwoju Spółek
Narodowy Fundusz Zdrowia
Poczta Polska
Polski Fundusz Rozwoju
Powszechna Kasa Oszczędności Bank Polski
Powszechny Zakład Ubezpieczeń
Polskie Koleje Państwowe
„WĘGLOKOKS”
Jastrzębska Spółka Węglowa
Katowicki Holding Węglowy
KGHM Polska Miedź
Krajowa Spółka Cukrowa
Polska Grupa Górnicza
Polskie Górnictwo Naftowe i Gazownictwo
Integratory
ACCA (Association of Chartered Certified Accountants) Polska
FINEXA – Stowarzyszenie Dyrektorów Finansowych
Izba Gospodarcza Towarzystw Emerytalnych

Naczelna Izba Lekarska
Polska Izba Brokerów Ubezpieczeniowych i Reasekuracyjnych
Polska Izba Ubezpieczeń
Polskie Biuro Ubezpieczeń Komunikacyjnych
Polskie Towarzystwo Ekonomiczne
Polskie Towarzystwo Informatyczne
Polskie Towarzystwo Lekarskie
Stowarzyszenie Menadżerów Opieki Zdrowotnej
Stowarzyszenie Multiagentów i Agentów Ubezpieczeniowych Polski Południowej
Stowarzyszenie Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych

LISTA POTENCJALNYCH BENEFICJENTÓW DLA RYNKU ENERGETYCZNEGO

Podmioty państwowe

Agencja Bezpieczeństwa Wewnętrznego
Centralne Biuro Antykorupcyjne
Ministerstwo Energii
Ministerstwo Inwestycji i Rozwoju
Ministerstwo Przedsiębiorczości i Technologii
Ministerstwo Sprawiedliwości
Polska Agencja Rozwoju Przedsiębiorczości
Polski Komitet Normalizacyjny
Polskie Centrum Badań i Certyfikacji
Urząd Regulacji Energetyki

Podmioty prywatne z udziałem Skarbu Państwa

Agencja Rozwoju Przemysłu
ENEA
ENERGA
Grupa LOTOS
Katowicki Holding Węglowy

KGHM Polska Miedź
PGE Polska Grupa Energetyczna
Polski Fundusz Rozwoju
Polski Koncern Naftowy ORLEN
TAURON Polska Energia
Towarowa Giełda Energii
Instytut Energetyki

Integratory

Polska Sekcja IEEE
Polskie Towarzystwo Ekonomiczne
Polskie Towarzystwo Informatyczne
Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej
Polskie Towarzystwo Elektrotechniki Teoretycznej i Stosowanej
Stowarzyszenie Polskich Energetyków
Stowarzyszenie Elektryków Polskich
Federacja Stowarzyszeń Naukowo-Technicznych, Naczelna Organizacja Techniczna
Polska Izba Gospodarcza Elektrotechniki

LISTA POTENCJALNYCH BENEFICJENTÓW DLA ZARZĄDZANIA LUDŹMI W ORGANIZACJI

Podmioty państwowe

Agencja Bezpieczeństwa Wewnętrznego
Centralne Biuro Antykorupcyjne
Kasa Rolniczego Ubezpieczenia Społecznego
Krajowa Administracja Skarbowa
Ministerstwo Cyfryzacji
Ministerstwo Sprawiedliwości
Najwyższa Izba Kontroli
Państwowa Inspekcja Pracy
Zakład Ubezpieczeń Społecznych

Ministerstwo Rodziny, Pracy i Polityki Społecznej

Podmioty prywatne z udziałem Skarbu Państwa

Agencja Kapitałowo-Rozliczeniowa
Grupa LOTOS
PGE Polska Grupa Energetyczna
Poczta Polska
Polskie Koleje Państwowe
Polskie Linie Kolejowe
Polskie Linie Lotnicze
Powszechna Kasa Oszczędności Bank Polski
Powszechny Zakład Ubezpieczeń
Telewizja Polska

Integratory

ACCA (Association of Chartered Certified Accountants) Polska
Pracodawcy Rzeczpospolitej Polskiej
Konfederacja Lewiatan
Naczelna Izba Lekarska
Polska Izba Ubezpieczeń
Stowarzyszenie Emitentów Giełdowych
Stowarzyszenie Organizatorów Ośrodków Innowacji i Przedsiębiorczości w Polsce
Stowarzyszenie Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych
Związek Rzemiosła Polskiego

LISTA PODMIOTÓW NAUKOWYCH WSPÓLNA DLA WSZYSTKICH OBSZARÓW

Akademia Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni

Akademia Marynarki Wojennej w Gdyni
Akademia Sztuki Wojennej
Akademia Wojsk Lądowych im. gen. T. Kościuszki

Centrum Szkolenia Policji
Katolicki Uniwersytet Lubelski Jana Pawła II
Lotnicza Akademia Wojskowa w Dęblinie
Politechnika Białostocka
Politechnika Częstochowska
Politechnika Gdańska
Politechnika Koszalińska
Politechnika Krakowska
Politechnika Lubelska
Politechnika Łódzka
Politechnika Opolska
Politechnika Poznańska
Politechnika Rzeszowska
Politechnika Śląska
Politechnika Świętokrzyska
Politechnika Warszawska
Politechnika Wrocławska
Szkoła Główna Służby Pożarniczej w Warszawie
Szkoła Podoficerska Marynarki Wojennej w Ustce
Szkoła Podoficerska Sił Powietrznych w Dęblinie
Szkoła Podoficerska Wojsk Lądowych w Poznaniu
Szkoła Policji
Uniwersytet Ekonomiczny w Krakowie
Uniwersytet Ekonomiczny w Poznaniu
Uniwersytet Ekonomiczny we Wrocławiu
Uniwersytet Gdański
Uniwersytet im. Adama Mickiewicza w Poznaniu
Uniwersytet Jagielloński
Uniwersytet Jana Kochanowskiego w Kielcach
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Uniwersytet Kazimierza Wielkiego w Bydgoszczy
Uniwersytet Łódzki

Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Uniwersytet Mikołaja Kopernika w Toruniu
Uniwersytet Opolski
Uniwersytet Rzeszowski
Uniwersytet Szczeciński
Uniwersytet Śląski
Uniwersytet w Białymstoku
Uniwersytet Warmińsko-Mazurski w Olsztynie
Uniwersytet Warszawski
Uniwersytet Wrocławski
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
Wojskowe Centrum Kształcenia Służb Medycznych w Łodzi
Wyższa szkoła Kryminologii i Penitencjarystyki w Warszawie
Wyższa Szkoła Oficerska Sił Powietrznych w Dęblinie
Wyższa Szkoła Policji w Szczytnie
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

5. Transforming People and Organizations: Ochrona praw człowieka jako istotny element prac projektowych

Określanie, badanie oraz analizowanie wdrażania najnowocześniejszych metod zapobiegania przyczynom przestępczości już z samej definicji wymaga ciągłej konfrontacji z powszechnie obowiązującym systemem ochrony praw człowieka i wolności. Z uwagi jednak na fakt, że dla całego projektu została stworzona lista najbardziej narażonych praw człowieka, nieuzasadniona metodologicznie jest kreacja specyficznej listy dla modułu Transforming People and Organizations. Z tego powodu zapobieganie przyczynom przestępczości, w tym wdrażanie metod jej zwalczania, w finansach, energetyce, ubezpieczeniach oraz zarządzaniu ludźmi w organizacji wypada konfrontować z regulacjami z zakresu konstytucyjnej ochrony praw i wolności (Konstytucja

Rzeczypospolitej Polskiej[11]) oraz europejskiej ochrony praw człowieka (1. Unia Europejska – Karta praw podstawowych Unii Europejskiej[12]; 2. Rada Europy – Konwencja o ochronie praw człowieka i podstawowych wolności[13]), w szczególności z:

Prawem do zdrowia, jako prawem osobistym (prawo do ochrony zdrowia) i socjalnym (prawo do świadczeń opieki medycznej).

Zgodnie z Art. 68 Konstytucji Rzeczypospolitej: „1. Każdy ma prawo do ochrony zdrowia. 2. Obywatelom, niezależnie od ich sytuacji materialnej, władze publiczne zapewniają równy dostęp do świadczeń opieki zdrowotnej finansowanej ze środków publicznych. Warunki i zakres udzielania świadczeń określa ustawa. 3. Władze publiczne są obowiązane do zapewnienia szczególnej opieki zdrowotnej dzieciom, kobietom ciężarnym, osobom niepełnosprawnym i osobom w podeszłym wieku. 4. Władze publiczne są obowiązane do zwalczania chorób epidemicznych i zapobiegania negatywnym dla zdrowia skutkom degradacji środowiska. 5. Władze publiczne popierają rozwój kultury fizycznej, zwłaszcza wśród dzieci i młodzieży".

Zgodnie art. 35 Karty praw podstawowych Unii Europejskiej: „Każdy ma prawo dostępu do profilaktycznej opieki zdrowotnej i prawo do korzystania z leczenia na warunkach ustanowionych w ustawodawstwach i praktykach krajowych. Przy określaniu i realizowaniu wszystkich polityk i działań Unii zapewnia się wysoki poziom ochrony zdrowia ludzkiego".

---

[11] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 Nr 78 poz. 483; 2001 Nr 28 poz. 319; 2006 Nr 200 poz. 1471; 2009 Nr 114 poz. 946).*

[12] *Karta praw podstawowych Unii Europejskiej (Dz. Urz. Unii Europejskiej C 326, 26.10.2012, s. 391–407).*

[13] *Konwencja o ochronie praw człowieka i podstawowych Wolności (Dz.U. 1993 Nr 61 poz. 284).*

Prawem do wolności i bezpieczeństwa osobistego.

Zgodnie z art. 41 Konstytucji Rzeczypospolitej Polskiej: „1. Każdemu zapewnia się nietykalność osobistą i wolność osobistą. Pozbawienie lub ograniczenie wolności może nastąpić tylko na zasadach i w trybie określonych w ustawie. 2. Każdy pozbawiony wolności nie na podstawie wyroku sądowego ma prawo odwołania się do sądu w celu niezwłocznego ustalenia legalności tego pozbawienia. O pozbawieniu wolności powiadamia się niezwłocznie rodzinę lub osobę wskazaną przez pozbawionego wolności. 3. Każdy zatrzymany powinien być niezwłocznie i w sposób zrozumiały dla niego poinformowany o przyczynach zatrzymania. Powinien on być w ciągu 48 godzin od chwili zatrzymania przekazany do dyspozycji sądu. Zatrzymanego należy zwolnić, jeżeli w ciągu 24 godzin od przekazania do dyspozycji sądu nie zostanie mu doręczone postanowienie sądu o tymczasowym aresztowaniu wraz z przedstawionymi zarzutami. 4. Każdy pozbawiony wolności powinien być traktowany w sposób humanitarny. 5. Każdy bezprawnie pozbawiony wolności ma prawo do odszkodowania".

Zgodnie z art. 6 Karty praw podstawowych Unii Europejskiej: „Każdy ma prawo do wolności i bezpieczeństwa osobistego".

Zgodnie z art. 5 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy ma prawo do wolności i bezpieczeństwa osobistego. Nikt nie może być pozbawiony wolności, z wyjątkiem następujących przypadków i w trybie ustalonym przez prawo: a. zgodnie z prawem pozbawienia wolności w wyniku skazania przez właściwy sąd; b. zgodnego z prawem zatrzymania lub aresztowania w przypadku niepodporządkowania się wydanemu zgodnie z prawem orzeczeniu sądu lub w celu zapewnienia wykonania określonego w ustawie obowiązku; c. zgodnego z prawem zatrzymania lub aresztowania w celu postawienia przed właściwym organem, jeżeli istnieje uzasadnione podejrzenie popełnienia czynu zagrożonego karą lub jeśli jest to konieczne w celu zapobieżenia popełnienia takiego czynu lub uniemożliwienia ucieczki po jego dokonaniu; d. pozbawienia nieletniego wolności na podstawie zgodnego z prawem orzeczenia w celu ustanowienia nadzoru wychowawczego lub zgodnego z prawem pozbawienia nieletniego wolności w celu postawienia

go przed właściwym organem; e. zgodnego z prawem pozbawienia wolności osoby w celu zapobieżenia szerzeniu przez nią choroby zakaźnej, osoby umysłowo chorej, alkoholika, narkomana lub włóczęgi; f. zgodnego z prawem zatrzymania lub aresztowania osoby w celu zapobieżenia jej nielegalnemu wkroczeniu na terytorium państwa lub osoby, przeciwko której toczy się postępowanie o wydalenie lub ekstradycję. 2. Każdy, kto został zatrzymany, powinien zostać niezwłocznie i w zrozumiałym dla niego języku poinformowany o przyczynach zatrzymania i o stawianych mu zarzutach. 3. Każdy zatrzymany lub aresztowany zgodnie z postanowieniami ustępu 1 lit. c) niniejszego artykułu powinien zostać niezwłocznie postawiony przed sędzią lub innym urzędnikiem uprawnionym przez ustawę do wykonywania władzy sądowej i ma prawo być sądzony w rozsądnym terminie albo zwolniony na czas postępowania. Zwolnienie może zostać uzależnione od udzielenia gwarancji zapewniających stawienie się na rozprawę. 4. Każdy, kto został pozbawiony wolności przez zatrzymanie lub aresztowanie, ma prawo odwołania się do sądu w celu ustalenia bezzwłocznie przez sąd legalności pozbawienia wolności i zarządzenia zwolnienia, jeżeli pozbawienie wolności jest niezgodne z prawem.

Każdy, kto został pokrzywdzony przez niezgodne z treścią tego artykułu zatrzymanie lub aresztowanie, ma prawo do odszkodowania".

Prawem do rzetelnego procesu sądowego, w tym prawem do skutecznego środka prawnego i dostępu do bezstronnego sądu, domniemaniem niewinności i prawem do obrony.

Zgodnie z art. 45 Konstytucji Rzeczypospolitej Polskiej: „1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd. 2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie".

Zgodnie z art. 42 Konstytucji Rzeczypospolitej Polskiej: „1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą

kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu".

Zgodnie z art. 47 Karty praw podstawowych Unii Europejskiej: „Każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w niniejszym artykule. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony uprzednio na mocy ustawy. Każdy ma możliwość uzyskania porady prawnej, skorzystania z pomocy obrońcy i przedstawiciela. Pomoc prawna jest udzielana osobom, które nie posiadają wystarczających środków, w zakresie w jakim jest ona konieczna dla zapewnienia skutecznego dostępu do wymiaru sprawiedliwości".

Zgodnie z art. 48 Karty praw podstawowych Unii Europejskiej: „1. Każdego oskarżonego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona zgodnie z prawem. 2. Każdemu oskarżonemu gwarantuje się poszanowanie prawa do obrony".

Zgodnie z art. 6 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy ma prawo do sprawiedliwego i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony ustawą przy rozstrzyganiu o jego prawach i obowiązkach o charakterze cywilnym albo o zasadności każdego oskarżenia w wytoczonej przeciwko niemu sprawie karnej. Postępowanie przed sądem jest jawne, jednak prasa i publiczność mogą być wyłączone z całości lub części rozprawy sądowej ze względów obyczajowych, z uwagi na porządek publiczny lub bezpieczeństwo państwowe w społeczeństwie demokratycznym, gdy wymaga tego dobro małoletnich lub gdy służy to ochronie życia prywatnego stron albo też w okolicznościach

szczególnych, w granicach uznanych przez sąd za bezwzględnie konieczne, kiedy jawność mogłaby przynieść szkodę interesom wymiaru sprawiedliwości. 2. Każdego oskarżonego o popełnienie czynu zagrożonego karą uważa się za niewinnego do czasu udowodnienia mu winy zgodnie z ustawą. 3. Każdy oskarżony o popełnienie czynu zagrożonego karą ma co najmniej prawo do: a) niezwłocznego otrzymania szczegółowej informacji w języku dla niego zrozumiałym o istocie i przyczynie skierowanego przeciwko niemu oskarżeniu; b) posiadania odpowiedniego czasu i możliwości do przygotowania obrony; c) bronienia się osobiście lub przez ustanowionego przez siebie obrońcę, a jeśli nie ma wystarczających środków na pokrycie kosztów obrony, do bezpłatnego korzystania z pomocy obrońcy wyznaczonego z urzędu, gdy wymaga tego dobro wymiaru sprawiedliwości; d) przesłuchania lub spowodowania przesłuchania świadków oskarżenia oraz żądania obecności i przesłuchania świadków obrony na takich samych warunkach jak świadków oskarżenia; e) korzystania z bezpłatnej pomocy tłumacza, jeżeli nie rozumie lub nie mówi językiem używanym w sądzie".

Prawem do podstawy prawnej karania, w tym z zasadą legalności oraz proporcjonalności kary do czynów zabronionych pod groźbą kary oraz z zakazem karania bez podstawy prawnej.

Zgodnie z art. 42 Konstytucji Rzeczypospolitej Polskiej: „1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu".

Zgodnie z art. 49 Karty praw podstawowych Unii Europejskiej: „1. Nikt nie może zostać skazany za popełnienie czynu polegającego na działaniu lub zaniechaniu, który według prawa krajowego lub prawa międzynarodowego

nie stanowił czynu zabronionego pod groźbą kary w czasie jego popełnienia. Nie wymierza się również kary surowszej od tej, którą można było wymierzyć w czasie, gdy czyn zabroniony pod groźbą kary został popełniony. Jeśli ustawa, która weszła w życie po popełnieniu czynu zabronionego pod groźbą kary, przewiduje karę łagodniejszą, ta właśnie kara ma zastosowanie. 2. Niniejszy artykuł nie stanowi przeszkody w sądzeniu i karaniu osoby za działanie lub zaniechanie, które w czasie, gdy miało miejsce, stanowiło czyn zabroniony pod groźbą kary, zgodnie z ogólnymi zasadami uznanymi przez wspólnotę narodów. 3. Kary nie mogą być nieproporcjonalnie surowe w stosunku do czynu zabronionego pod groźbą kary".

Zgodnie z art. 7 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Nikt nie może być uznany za winnego popełnienia czynu polegającego na działaniu lub zaniechaniu działania, który według prawa wewnętrznego lub międzynarodowego nie stanowił czynu zagrożonego karą w czasie jego popełnienia. Nie będzie również wymierzona kara surowsza od tej, którą można było wymierzyć w czasie, gdy czyn zagrożony karą został popełniony. 2. Niniejszy artykuł nie stanowi przeszkody w sądzeniu i karaniu osoby winnej działania lub zaniechania, które w czasie popełnienia stanowiły czyn zagrożony karą według ogólnych zasad uznanych przez narody cywilizowane".

Prawem do poszanowania życia prywatnego i rodzinnego.

Zgodnie z art. 47 Konstytucji Rzeczypospolitej Polskiej: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym".

Zgodnie z art. 7 Karty praw podstawowych Unii Europejskiej: „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".

Zgodnie z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem

przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób".

Prawem do ochrony danych osobowych.

Zgodnie z art. 51 Konstytucji Rzeczypospolitej Polskiej: „1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa".

Zgodnie z art. 8 Karty praw podstawowych Unii Europejskiej: „1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą. 2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. 3. Przestrzeganie tych zasad podlega kontroli niezależnego organu".

Prawem do wolności opinii i informacji.

Zgodnie z art. 54 Konstytucji Rzeczypospolitej Polskiej: „1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. 2. Cenzura prewencyjna środków społecznego przekazu oraz koncesjonowanie prasy są zakazane. Ustawa może wprowadzić obowiązek uprzedniego uzyskania koncesji na prowadzenie stacji radiowej lub telewizyjnej".

Zgodnie z art. 11 Karty praw podstawowych Unii Europejskiej: „1. Każdy ma prawo do wolności wypowiedzi. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. 2. Szanuje się wolność i pluralizm mediów".

Zgodnie z art. 11 Karty praw podstawowych Unii Europejskiej: „1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa Państw do poddania procedurze zezwoleń przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych. 2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej".

Prawem do wolności zgromadzeń i stowarzyszania się.

Zgodnie z art. 57 Konstytucji Rzeczypospolitej Polskiej: „Każdemu zapewnia się wolność organizowania pokojowych zgromadzeń i uczestniczenia w nich. Ograniczenie tej wolności może określać ustawa.".

Zgodnie z art. 58 Konstytucji Rzeczypospolitej Polskiej: „1. Każdemu zapewnia się wolność zrzeszania się. 2. Zakazane są zrzeszenia, których cel lub działalność są sprzeczne z Konstytucją lub ustawą. O odmowie rejestracji lub zakazie działania takiego zrzeszenia orzeka sąd. 3. Ustawa określa rodzaje zrzeszeń podlegających sądowej rejestracji, tryb tej rejestracji oraz formy nadzoru nad tymi zrzeszeniami".

Zgodnie z art. 59 Konstytucji Rzeczypospolitej Polskiej: „1. Zapewnia się wolność zrzeszania się w związkach zawodowych, organizacjach społeczno-zawodowych rolników oraz w organizacjach pracodawców. 2. Związki zawodowe oraz pracodawcy i ich organizacje mają prawo do rokowań, w szczególności w celu rozwiązywania sporów zbiorowych, oraz do zawierania układów zbiorowych pracy i innych porozumień. 3. Związkom zawodowym przysługuje prawo do organizowania strajków pracowniczych i innych form protestu w granicach określonych w ustawie. Ze względu na dobro publiczne ustawa może ograniczyć prowadzenie strajku lub zakazać go w odniesieniu do określonych kategorii pracowników lub w określonych dziedzinach. 4. Zakres wolności zrzeszania się w związkach zawodowych i organizacjach pracodawców oraz innych wolności związkowych może podlegać tylko takim ograniczeniom ustawowym, jakie są dopuszczalne przez wiążące Rzeczpospolitą Polską umowy międzynarodowe".

Zgodnie z art. 12 Karty praw podstawowych Unii Europejskiej: „1. Każdy ma prawo do swobodnego, pokojowego zgromadzania się oraz do swobodnego stowarzyszania się na wszystkich poziomach, zwłaszcza w sprawach politycznych, związkowych i obywatelskich, z którego wynika prawo każdego do tworzenia związków zawodowych i przystępowania do nich dla obrony swoich interesów. 2. Partie polityczne na poziomie Unii przyczyniają się do wyrażania woli politycznej jej obywateli".

Zgodnie z art. 11 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy ma prawo do swobodnego, pokojowego zgromadzenia się oraz do swobodnego stowarzyszania się, włącznie z prawem tworzenia związków zawodowych i przystępowania do nich dla ochrony swoich interesów. 2. Wykonywanie tych praw nie może podlegać innym ograniczeniom niż te, które określa ustawa i które są konieczne w społeczeństwie demokratycznym z uwagi na interesy bezpieczeństwa państwowego lub publicznego, ochronę porządku i zapobieganie przestępstwu, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Niniejszy przepis nie stanowi przeszkody w nakładaniu zgodnych z prawem ograniczeń korzystania z tych praw przez członków sił zbrojnych, policji lub administracji państwowej".

Prawem do zakazu ponownego sądzenia lub karania, w tym z zakazem ponownego sądzenia lub karania w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary.

Zgodnie z art. 50 Karty praw podstawowych Unii Europejskiej: „Nikt nie może być ponownie sądzony lub ukarany w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary, w odniesieniu do którego zgodnie z ustawą został już uprzednio uniewinniony lub za który został już uprzednio skazany prawomocnym wyrokiem na terytorium Unii".

Zgodnie z art. 4 Protokołu nr 7 do Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Nikt nie może być ponownie sądzony lub ukarany w postępowaniu przed sądem tego samego Państwa za przestępstwo, za które został uprzednio skazany prawomocnym wyrokiem lub uniewinniony zgodnie z ustawą i zasadami postępowania karnego tego Państwa. 2. Postanowienia poprzedniego ustępu nie stoją na przeszkodzie wznowieniu postępowania zgodnie z ustawą i zasadami postępowania karnego danego Państwa, jeśli wyjdą na jaw nowo odkryte fakty lub jeśli w poprzednim postępowaniu popełniono poważną pomyłkę, która mogła mieć wpływ na wynik sprawy. 3. Żadne z postanowień niniejszego artykułu nie może być uchylone na podstawie artykułu 15 Konwencji (Uchylenie stosowania zobowiązań w stanie".

Zgodnie z art. 42 Konstytucji Rzeczypospolitej Polskiej: „1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu".

Zgodnie z art. 45 Konstytucji Rzeczypospolitej Polskiej: „1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki

przez właściwy, niezależny, bezstronny i niezawisły sąd. 2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie".

Prawem do odszkodowania za bezprawne skazanie.

Zgodnie z art. 4 Protokołu nr 7 do Konwencji o ochronie praw człowieka i podstawowych wolności: „Każdemu skazanemu prawomocnie za przestępstwo, który odbył karę w wyniku takiego skazania, a następnie został uniewinniony lub ułaskawiony na tej podstawie, że nowy lub nowo ujawniony fakt dowiódł, iż nastąpiła pomyłka sądowa, przysługuje odszkodowanie zgodnie z ustawą lub praktyką w danym Państwie, jeżeli nie udowodniono, że jest on całkowicie lub częściowo odpowiedzialny za nieujawnienie faktu we właściwym czasie".

Prawem do odwołania w sprawach karnych.

Zgodnie z art. 47 Karty praw podstawowych Unii Europejskiej: „Każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w niniejszym artykule. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony uprzednio na mocy ustawy. Każdy ma możliwość uzyskania porady prawnej, skorzystania z pomocy obrońcy i przedstawiciela. Pomoc prawna jest udzielana osobom, które nie posiadają wystarczających środków, w zakresie w jakim jest ona konieczna dla zapewnienia skutecznego dostępu do wymiaru sprawiedliwości".

Zgodnie z art. 2 Protokołu nr 7 do Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy, kto został uznany przez sąd za winnego popełnienia przestępstwa, ma prawo do rozpatrzenia przez sąd wyższej instancji jego sprawy, tak w przedmiocie orzeczenia o winie, jak i co do kary. Korzystanie z tego prawa, a także jego podstawy, reguluje ustawa. 2. Wyjątki od tego prawa mogą być stosowane w przypadku drobnych przestępstw, określonych

w ustawie, lub w przypadkach, gdy dana osoba była sądzona w pierwszej instancji przez sąd najwyższy albo została uznana za winną i skazana w wyniku zaskarżenia wyroku uniewinniającego sądu pierwszej instancji".

Zgodnie z art. 42 Konstytucji Rzeczypospolitej Polskiej: „1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu".

Art. 45 Konstytucji Rzeczypospolitej Polskiej: „1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd. 2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie".

Prawem do własności.

Zgodnie z art. 64 Konstytucji Rzeczypospolitej Polskiej: „1. Każdy ma prawo do własności, innych praw majątkowych oraz prawo dziedziczenia. 2. Własność, inne prawa majątkowe oraz prawo dziedziczenia podlegają równej dla wszystkich ochronie prawnej. 3. Własność może być ograniczona tylko w drodze ustawy i tylko w zakresie, w jakim nie narusza ona istoty prawa własności".

Zgodnie z art. 17 Karty praw podstawowych Unii Europejskiej: „1. Każdy ma prawo do władania, używania, rozporządzania i przekazania w drodze spadku mienia nabytego zgodnie z prawem. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym, w przypadkach i na warunkach

przewidzianych w ustawie, za słusznym odszkodowaniem za jej utratę wypłaconym we właściwym terminie. Korzystanie z mienia może podlegać regulacji ustawowej w zakresie, w jakim jest to konieczne ze względu na interes ogólny. 2. Własność intelektualna podlega ochronie".

Zgodnie z art. 1 Protokołu dodatkowego do Konwencji o ochronie praw człowieka i podstawowych wolności: „Każda osoba fizyczna i prawna ma prawo do poszanowania swego mienia. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym i na warunkach przewidzianych przez ustawę oraz zgodnie z podstawowymi zasadami prawa międzynarodowego. Powyższe postanowienia nie będą jednak w żaden sposób naruszać prawa Państwa do wydawania takich ustaw, jakie uzna za konieczne dla uregulowania sposobu korzystania z własności zgodnie z interesem powszechnym lub w celu zapewnienia uiszczania podatków bądź innych należności lub kar pieniężnych".

6. Transforming People and Organizations: Uzasadnienie prowadzenia prac badawczych

Implementacja najnowocześniejszych oraz prowadzących do najlepszych efektów metod zapobiegania przyczynom przestępczości w finansach, energetyce, ubezpieczeniach oraz w zarządzaniu ludźmi w organizacji jest zasadne ze wszech miar. Po pierwsze, w ramach rynku finansowego może być to fakt nadużyć finansowych, które charakteryzują się cechą zmienności. Po drugie, w ramach rynku energetycznego może być to fakt strat dla zakładów energetycznych, które są powodowane patologiami czynów zabronionych. Po trzecie, w ramach rynku ubezpieczeniowego może być to fakt odczucia ważności społecznej tej problematyki. Po czwarte, w ramach zarządzania ludźmi w organizacji może być dbałość o zachowanie odpowiedniej równowagi pomiędzy czasem przeznaczanym na pracę oraz na rodzinę. Naukowa analiza prawa, gospodarki i technologii w kontekście zapobiegania przyczynom przestępczości finansowej, energetycznej, ubezpieczeniowej oraz w zarządzaniu ludźmi w organizacji, w szczególności w ramach modułu dotyczącego wdrażania metod, jest niezbędna do odkrycia nowych i nieeksploatowanych jeszcze płaszczyzn badawczych.

ROZDZIAŁ II

Implementacja systemów prewencyjnych

ALINA KLONOWSKA[1], MAGDALENA MAŁECKA-ŁYSZCZEK[2], MAŁGORZATA SNARSKA[3], JOANNA WYROBEK

1. Transformacja instytucji w celu zapobiegania przestępczości finansowej

Jak zostało już wielokrotnie podkreślone wcześniej, w przypadku problematyki przestępczości na rynkach finansowych mamy do czynienia ze zjawiskiem szerokim i wielowątkowym. Dlatego jego analiza wymaga również podejścia wieloaspektowego. W niniejszym rozdziale rozważania skupiono na wskazaniu pola możliwych regulacji, które odnosząc się do działalności podmiotów funkcjonujących na rynkach finansowych, mają na celu zapobieganie przestępstwom na rynkach finansowych. Swoją istotną rolę odgrywają tutaj również pozakarne instrumenty eliminowania patologii poprzez: określone wymogi (kapitałowe i inne) co do możliwości utworzenia podmiotów

[1] Doktor nauk ekonomicznych, adiunkt w Katedrze Zarządzania Ryzykiem i Ubezpieczeń w Kolegium Ekonomii, Finansów i Prawa, Uniwersytetu Ekonomicznego w Krakowie. Dorobek naukowy gromadzony od 2007 r. obejmuje zagadnienia związane z polityką fiskalną państwa, a w szczególności problematykę voluntary tax compliance, ryzyka podatkowego i metod skutecznego zarządzania nim. Adres email: klonowsa@uek.krakow.pl.

[2] Profesor nadzwyczajny w Katedrze Prawa Konstytucyjnego, Administracyjnego i Zamówień Publicznych Uniwersytetu Ekonomicznego w Krakowie, specjalizuje się w problematyce prawa administracyjnego z wpływem prawa konstytucyjnego, prowadzi również wykłady specjalistyczne w zakresie zwalczania przestępczości na rynkach finansowych. Autorka licznych opracowań i ekspertyz.

[3] Doktor fizyki teoretycznej Uniwersytetu Jagiellońskiego, adiunkt w Katedrze Rynków Finansowych, a wcześniej na stanowisku asystenta w Katedrze Ekonometrii i Badań Operacyjnych w Kolegium Ekonomii, Finansów i Prawa, Uniwersytetu Ekonomicznego w Krakowie, profesor wizytujący na Uniwersytecie w Lille oraz IESEG School of Management w Paryżu. Zainteresowania naukowe obejmują zagadnienia z zakresu statystyki matematycznej, teorii ekonometrii oraz finansów empirycznych i wyceny instrumentów pochodnych.

gospodarczych, właściwy nadzór, propagowanie pozaprawnych środków intensyfikujących świadomość etyczną[4].

Pragnąc jak najbardziej uporządkować czynione rozważania należy zauważyć, że w przypadku regulacji, które mogą przyczyniać się do zapobiegania przestępczości na rynkach finansowych warto wskazać zarówno na obszar regulacji prawa powszechnie obowiązującego, ale również na regulacje o charakterze wewnętrznym, które generowane są w ramach i na potrzeby funkcjonowania konkretnego podmiotu. **Szczególne znaczenie ma tutaj *internal control*, nakierowana na konieczność jak najwcześniejszego reagowania na pojawiające się nieprawidłowości, które mogą się zmaterializować jako konkretny rodzaj przestępstwa.** W przypadku kontroli wewnętrznej **niezwykle istotny jest aspekt prawny, ale i silne wyeksponowanie znaczenia prawidłowego zarządzania. To są procesy powiązane, scalone w odniesieniu do prawidłowo funkcjonującego przedsiębiorstwa**. Dodatkowo na powyższe należy nałożyć spostrzeżenie, iż **procesy te muszą być podparte również silnym nakierowaniem na aspekty natury etycznej**. Działania nieetyczne to naturalne podglebie dla działalności korupcyjnej, przestępczej. W ramach nniejszej publikacji nie zagłębiono się w złożone problemy natury definicyjno-konceptualnej, niemniej jednak wskazać należy, iż etyka to nauka o moralności. Chcąc spojrzeć na niniejszą problematykę z pełnym poszanowaniem filozoficznej tradycji terminologicznej, z całą pewnością terminów „moralność" i „etyka" nie należy ujmować synonimicznie. Moralność obejmuje ludzkie zachowania i motywy wyborów decyzji, etyka zaś powinna być postrzegana jako (wyrażana regulacjami i nauczaniem) refleksja nad nimi[5]. Oczywiście w praktyce dnia codziennego to, co etyczne, przeplata się z tym, co moralne. Dodatkowo na to wszystko nakłada się teoria wartości (aksjologia), która w węższym znaczeniu oznacza moralność ustalającą hierarchiczny układ wartości[6]. Należy zauważyć, że problematyka rynku finansowego jest silnie uwarunkowania aksjologicznie[7]. Bezpieczeństwo, stabilność, zaufanie – to

[4] *Zalecenia Rady Europy Nr R(81)12 w sprawie przestępstw gospodarczych (Council of Europe Committee of Ministers, Recommendation No. R (81) 12 z 26.06.1981 r.*

[5] R. Tokarczyk, *Etyka prawnicza*, Warszawa 2006, s. 15.

[6] Tak D. Julia, *Słownik filozofii*, Katowice 1992, s. 15.

[7] Problematyka wartości, choć w różnym natężeniu, mieści się w rozmaitych obszarach prawnych. Por.: M. Wielec, *Wartości – analiza z perspektywy osobliwości postępowania karnego,* Lublin 2017, s. 22.

niewątpliwie wartości, które stara się chronić tak ustawodawca krajowy, jak i regulacje stanowione na poziomie unijnym, czy też patrząc z jeszcze szerszej perspektywy – prawa międzynarodowego. Sięgając chociażby do art. 2 u.n.r.f. można zaważyć, że ustawodawca *expressis verbis* przywołuje tutaj fundamentalne wartości, takie jak: prawidłowe funkcjonowanie rynku finansowego, jego stabilność, bezpieczeństwo, przejrzystość, zaufanie, a także zapewnienie ochrony interesów uczestników tego rynku. Na niniejsze kwestie można też popatrzeć przez pryzmat ustawy zasadniczej, skoro zgodnie z art. 20 Konstytucji społeczna gospodarka rynkowa oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych stanowi podstawę ustroju gospodarczego Rzeczypospolitej Polskiej, co odnosi się również do działalności gospodarczej na poziomie rynku finansowego. Ten obszar stanowi dobro wspólne wszystkich jego uczestników (podmiotów finansowych, jakimi są osoby fizyczne, prawne lub inne jednostki organizacyjne oferujące produkty lub usługi finansowe, a także ich klientów oraz innych instytucji i organizacji na nim działających). Dlatego podstawą zrównoważonego rozwoju i bezpieczeństwa tego rynku jest etyczny wymiar działań podmiotów finansowych[8]. Wszędzie bowiem, niezależnie od konkretnego systemu prawnego i przyjmowanych rozwiązań szczegółowych, widoczna jest troska o należyte uregulowanie zagadnień, które służyć mają prawidłowemu funkcjonowaniu podmiotów na rynku finansowym. Można tutaj mówić zarówno o podmiotach, które świadczą swoje usługi (stąd regulacje reglamentujące, ustanawiające wymogi konieczne do spełnienia dla podejmowania określonego rodzaju działalności), jak i o inwestorach, ale także mając na uwadze kształtowanie ram dla funkcjonowania stosownych organów nadzoru (również z uwagi na rozkład kompetencji pomiędzy organy krajowe a unijne). Spektrum możliwych zagadnień jest tutaj niezwykle szerokie. Niewątpliwie zadaniem racjonalnego i odpowiedzialnego ustawodawcy jest kreowanie przepisów, które będą sprzyjały należytemu/optymalnemu funkcjonowaniu rynku opartego na przyjmowanych wartościach, a eliminowały dysfunkcje, niewydolności, a zwłaszcza patologie, które mu zagrażają, godząc tak w instytucje finansowe, jak i klientów usług

[8] Zob.: *Kanon Dobrych Praktyk Rynku Finansowego, jak i Uchwała Nr 99/08 Komisji Nadzoru Finansowego z dnia 18 marca 2008 r. w sprawie rekomendacji stosowania Kanonu Dobrych Praktyk Rynku Finansowego (Dz. Urz. KNF 2008 Nr 3 poz. 9).*

finansowych, a emanując szerzej – w ogół społeczeństwa. Przestępstwa na rynkach finansowych generują przecież straty nie tylko w wymiarze finansowym, ale równie poważne koszty społeczne, takie jak spadek/utrata zaufania społecznego do funkcjonowania rynków. Dysfunkcje na rynku finansowym odbijają się nie tylko na stabilności i funkcjonowaniu poszczególnych państw, ale z uwagi na istniejące powiązania i przepływy kapitału należy mieć również na uwadze wymiar europejski, czy też międzynarodowy. Mając na uwadze dzisiejszy stopień globalizacji, zagrożenia (jakie pojawiają się w bezpiecznym prowadzeniu działalności przez instytucje finansowe) wykraczają poza granice poszczególnych państw i nabierają charakteru międzynarodowego. Dlatego też zapewnienie bezpieczeństwa i stabilności finansowej stanowi nowy paradygmat regulacji rynku finansowego[9].

Konkludując, swoją istotną rolę w obszarze zapobiegania przestępstwom na rynkach finansowych mają do odegrania:

1. regulacje prawa powszechnie obowiązującego,
2. **regulacje o charakterze wewnętrznym** stanowione przez umocowane ku temu organy przedsiębiorstwa (regulaminy, statuty, procedury wewnętrzne),
3. również **regulacje natury etycznej**, kształtujące właściwe postawy wśród pracowników (kodeksy etyki).

Istotna jest zarówno warstwa regulacji prawnych, jak i kompatybilna z nimi warstwa rozwiązań z obszaru zarządzania. Z uwagi na złożoność problematyki przestępstw na rynku finansowym trzeba działać wielopłaszczyznowo, wykorzystując wszelkie dostępne instrumenty. I dopiero efekt ich wzajemnej synergii może przełożyć się na jak najbardziej pożądane rezultaty. Jak już wskazano, w działalności konkretnego podmiotu funkcjonującego na rynku finansowym szczególne znaczenie mają regulacje w zakresie *internal control*. Spoglądając na stosowne w tym obszarze regulacje u.p.b. (art. 9c), cele systemu kontroli wewnętrznej obejmują mi.in zgodności działania banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi. Przenosząc powyższe na inne podmioty funkcjonujące na rynku finansowym

[9] M. Olszak, A. Jurkowska-Zeidler, *Wprowadzenie*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, 29.06.2019, https://sip.lex.pl/#/monograph/369380982/3 (dostęp: 7.08.2019).

i przywołując opracowane przez KNF Zasady ładu korporacyjnego dla instytucji nadzorowanych, instytucja taka powinna posiadać adekwatny, efektywny i skuteczny system kontroli wewnętrznej mający na celu zapewnienie m.in. **zgodności działania z przepisami prawa i regulacjami wewnętrznymi oraz z uwzględnieniem rekomendacji nadzorczych**[10]. Chodzi tu oczywiście o tzw. **funkcję *compliance***, wywodzącą się z modelu COSO (*The Committee of Sponsoring Organizations of the Treadway Commission*)[11], czyli zgodności (zarówno z przepisami prawa, jak i regulacjami wewnętrznymi podmiotu). Siłą rzeczy wpisują się tutaj także działania dla zapewnienia zgodności z przepisami w obszarze przestępstw przeciwko rynkowo finansowemu. Jednocześnie funkcja *compliance* jest ujmowana jako element zarządzania ryzykiem[12], a zatem w odniesieniu ściśle do przestępstw chodzi tu o ryzyko sankcji karnych, co powiązać należy z pojawiającym się jednocześnie ryzykiem utraty, jakże ważnej na rynku finansowym, reputacji przez dany podmiot.

Formułując rozważania w obranym zakresie tematycznym, **konieczne jest poszerzanie regulacji w obszarze whistleblowingu** (rozumianego jako raportowanie przez obecnych lub byłych pracowników o nielegalnych, niewłaściwych, niebezpiecznych lub nieetycznych praktykach pracodawców). A zatem whistleblower/sygnalista to osoba dokonująca zgłoszenia naruszeń w ramach whistleblowingu[13]. Można wyróżnić whistleblowing wewnętrzny (w ramach danej organizacji, np. banku.) oraz whistleblowing zewnętrzny. Na podstawie art. 9 ust. 2a-2b u.p.b (whistelblowing wewnętrzny) system zarządzania obejmuje procedury anonimowego zgłaszania wskazanemu członkowi zarządu, a w szczególnych przypadkach – radzie nadzorczej banku, naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych. W ramach tych procedur bank zapewnia pracownikom, którzy zgłaszają dysfunkcje, ochronę co najmniej przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania[14]. Natomiast

[10] § 45 Zasad ładu korporacyjnego dla instytucji nadzorowanych, dokument przyjęty uchwałą KNF z dnia 22 lipca 2014 roku.

[11] Szerzej: Coso, https://www.coso.org

[12] Ł. Cichy, *Funkcja compliance w bankach*, KNF, Warszawa 2015, s. 7.

[13] Ł. Cichy, *Whistleblowing w bankach*, KNF, Warszawa 2017, s. 6.

[14] Zob. szerzej: K. Majewski, *Funkcjonowanie w banku procedury anonimowego zgłaszania naruszeń*, „Monitor Prawa Bankowego", 2018, nr 12, s. 67–77.

z whistelblowingiem zewnętrznym mamy do czynienia w oparciu o 133a ust. 9 i 10 u.p.b, zgodnie z którymi KNF przyjmuje zgłoszenia naruszeń lub potencjalnych naruszeń przepisów u.p.b. oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniającego rozporządzenie (UE) nr 648/2012 (Dz.U. UE. L. z 2013 r. Nr 176, str. 1 z późn. zm.). Informacje uzyskane w tym trybie, w tym takie, które mogłyby umożliwić identyfikację osoby dokonującej zgłoszenia oraz osoby, której zarzuca się naruszenie, a także informacja o dokonaniu zgłoszenia, mogą być ujawnione tylko: 1) w zawiadomieniu o podejrzeniu popełnienia przestępstwa oraz w dokumentach przekazywanych w uzupełnieniu takiego zawiadomienia; 2) na żądanie sądu lub prokuratora w związku z toczącym się postępowaniem karnym lub postępowaniem w sprawach o przestępstwa skarbowe. Jak zatem widać, obszar niniejszy wykazuje ścisłe powiazanie z przestępstwami przeciwko rynkowi finansowemu. Również na podstawie art. 3a u.n.r.k. KNF przyjmuje zgłoszenia naruszeń lub potencjalnych naruszeń przepisów MAR. Przekazanie Komisji zgłoszenia nie narusza obowiązku zachowania tajemnicy zawodowej, a także innych obowiązków zachowania poufności informacji, wynikających z obowiązujących przepisów prawa lub umowy. Ponadto ich przekazanie Komisji nie może stanowić przyczyny rozwiązania z osobą zgłaszającą umowy o pracę, umowy zlecenia, umowy o dzieło lub innej umowy o podobnym charakterze. Informacje mogą być ujawnione wyłącznie: 1) w zawiadomieniu o podejrzeniu popełnienia przestępstwa oraz w dokumentach przekazywanych w uzupełnieniu takiego zawiadomienia; 2) na żądanie sądu lub prokuratora w związku z toczącym się postępowaniem karnym lub postępowaniem w sprawie o przestępstwo skarbowe; 3) w ramach współpracy międzynarodowej z państwami trzecimi, na zasadach określonych w porozumieniach zawieranych na podstawie MAR. Szczegółowo niniejsze kwestie reguluje Rozporządzenie Ministra Finansów z dnia 25 czerwca 2018 r. w sprawie odbierania przez Komisję Nadzoru Finansowego zgłoszeń naruszeń rozporządzenia 596/2014 (Dz.U. z 2018 poz. 1262). Z uwagi na istotne znaczenie niniejszych zagadnień samo MAR w art. 32 odnosi się *expressis verbis* do zgłaszania naruszeń. Zgodnie z nim państwa członkowskie zapewniają ustanowienie przez właściwe organy skutecznych mechanizmów umożliwiających zgłaszanie właściwym organom rzeczywistych lub potencjalnych

naruszeń MAR. Mechanizmy te obejmują co najmniej: a) szczególne procedury odbierania zgłoszeń w sprawie naruszeń oraz działania następcze, w tym ustanowienie bezpiecznych kanałów komunikacji dla takich zgłoszeń; b) w ramach zatrudnienia – stosowną ochronę osób zatrudnionych na podstawie umowy o pracę, które ujawniają naruszenia lub którym zarzuca się naruszenia – co najmniej przed odwetem, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania; oraz c) ochronę danych osobowych zarówno osoby zgłaszającej naruszenie, jak i osoby fizycznej podejrzewanej o jego popełnienie, w tym ochronę w zakresie zachowania poufnego charakteru ich tożsamości na wszystkich etapach postępowania, bez uszczerbku dla wymogu ujawnienia informacji na gruncie prawa krajowego w kontekście czynności wyjaśniających lub późniejszych postępowań sądowych. Ponadto państwa członkowskie wymagają, aby pracodawcy prowadzący działalność regulowaną przepisami w sprawie usług finansowych dysponowali odpowiednimi wewnętrznymi procedurami zgłaszania naruszeń niniejszego rozporządzenia przez ich pracowników. Co więcej, państwa członkowskie mogą przewidzieć zachęty finansowe dla osób oferujących istotne informacje dotyczące potencjalnych naruszeń przepisów MAR, które przyznawane są zgodnie z prawem krajowym, w przypadku gdy takie osoby nie mają innych istniejących uprzednio obowiązków zgłaszania takich informacji wynikających z przepisów prawa lub umowy i pod warunkiem, że informacje te są nowe oraz że skutkują nałożeniem sankcji administracyjnej lub karnej bądź zastosowaniem innego środka administracyjnego z tytułu naruszenia MAR. Powyższe spostrzeżenia należy uzupełnić raz jeszcze podkreśleniem, iż kwestie niniejsze w sposób nierozerwalny wiążą się z właściwym zarządzaniem konkretnym podmiotem, do którego są odnoszone. W ramach czynionych analiz nie sposób pominąć zagadnień uregulowanych w rozporządzeniu Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz.U. z 2017 poz. 637), które określa m.in. szczegółowy sposób funkcjonowania w bankach systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, w tym tryb anonimowego zgłaszania wskazanemu członkowi zarządu lub rady nadzorczej naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych. Zgodnie z jego § 45 bank opracowuje i wdraża procedury anonimowego

zgłaszania przez pracowników naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych. Przez obowiązujące w banku procedury rozumie się wszelkie akty wewnętrzne, w tym regulaminy, instrukcje, systemy i rozwiązania przyjęte w danym banku. Dla należytego funkcjonowania niniejszych regulacji bank zapewnia możliwość zgłaszania przez pracowników naruszeń za pośrednictwem specjalnego, niezależnego i autonomicznego kanału komunikacji. Procedury anonimowego zgłaszania przez pracowników naruszeń określają co najmniej: 1) sposób odbierania zgłoszeń w sprawie naruszeń, zapewniający w szczególności możliwość odbioru zgłoszeń bez podawania tożsamości przez pracownika dokonującego zgłoszenia; 2) sposób ochrony pracownika dokonującego zgłoszenia, zapewniający co najmniej zabezpieczenie przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania; 3) sposób ochrony danych osobowych pracownika dokonującego zgłoszenia oraz osoby, której zarzuca się dokonanie naruszenia, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922); 4) zasady zapewniające zachowanie poufności pracownikowi dokonującemu zgłoszenia, w przypadku gdy pracownik ten ujawnił swoją tożsamość lub jego tożsamość jest możliwa do ustalenia; 5) wskazanie osób odpowiedzialnych za odbieranie zgłoszeń naruszeń z uwzględnieniem, że w przypadku, gdy zgłoszenie dotyczy członka zarządu, powinno być ono przyjęte przez radę nadzorczą; 6) sposób przekazywania informacji związanych ze zgłoszeniem naruszenia, niezbędnych do prawidłowej weryfikacji tego zgłoszenia, z uwzględnieniem ograniczenia zakresu przekazywanych informacji odpowiednio do celów realizowanych przez procedurę oraz treści zgłoszenia naruszenia; 7) rodzaj i charakter działań następczych podejmowanych na skutek: odebrania zgłoszenia naruszenia, weryfikacji zgłoszenia naruszenia – oraz sposób koordynacji tych działań; 8) termin usunięcia przez bank danych osobowych zawartych w zgłoszeniach naruszeń; 9) w przypadku pozytywnej weryfikacji zasadności zgłoszenia naruszenia termin powiadomienia osoby, której zarzuca się dokonanie naruszenia, o dokonanym zgłoszeniu naruszenia oraz o przeprowadzonej procedurze weryfikacji zasadności zgłoszenia naruszenia. Zarząd ustala wewnętrzny podział kompetencji wskazujący członka zarządu, do którego są zgłaszane naruszenia oraz odpowiedzialnego za bieżące funkcjonowanie procedur anonimowego zgłaszania naruszeń. Wewnętrzny

podział kompetencji podlega zatwierdzeniu przez radę nadzorczą. Zarząd jest odpowiedzialny za adekwatność i skuteczność procedur anonimowego zgłaszania przez pracowników naruszeń. Rada nadzorcza – w zależności od potrzeb – nie rzadziej jednak niż raz w roku, ocenia adekwatność i skuteczność procedury anonimowego zgłaszania przez pracowników naruszeń. Co niezwykle istotne w obliczu ewoluującej sytuacji, bank przeprowadza wstępne i regularne szkolenia pracowników w zakresie zgłaszania naruszeń, w szczególności obowiązujących w tym zakresie procedur. Wskazana regulacje adresowane są do banków, niemniej jednak zaprezentowane mechanizmy można przenosić również na inne podmioty sektora finansowego, mając na uwadze ich potencjalne przełożenie na wychwytywanie działań niezgodnych z prawem (w tym i przestępstw), skoro zakres przedmiotowy zgłoszeń w ramach whistleblowingu jest szeroki i dotyczy naruszeń prawa oraz obowiązujących procedur i standardów etycznych. Należy tu przywołać § 6 opracowanych przez KNF Zasad ładu korporacyjnego dla instytucji nadzorowanych, gdzie zawarto informację, iż w przypadku wprowadzenia w instytucji nadzorowanej anonimowego sposobu powiadamiania organu zarządzającego lub organu nadzorującego o nadużyciach w tejże instytucji powinna być zapewniona możliwość korzystania z tego narzędzia przez pracowników bez obawy negatywnych konsekwencji ze strony kierownictwa i innych pracowników. Równocześnie organ zarządzający powinien przedstawiać organowi nadzorującemu raporty dotyczące powiadomień o poważnych nadużyciach[15]. Spoglądając w jeszcze szerszej perspektywie na projekt ustawy o jawności życia publicznego[16], tu również pojawiają się sygnaliści (osoby, których współpraca z wymiarem sprawiedliwości polegająca na zgłoszeniu informacji o możliwości popełnienia przestępstwa przez podmiot, z którym jest związana umową o pracę lub innym stosunkiem umownym może niekorzystnie wpłynąć na ich sytuację życiową, zawodową, materialną), dążąc do możliwości wychwycenia, że mogło dojść do przestępstwa, zwiększając możliwości wykrycia nieprawidłowości (żeby następnie oszacować, czy chodzi o przestępstwo).

[15] *Zasady ładu korporacyjnego dla instytucji nadzorowanych, dokument przyjęty uchwałą KNF z dnia 22 lipca 2014 roku.*

[16] Rządowe Centrum Legislacji, *Ustawa o jawności życia publicznego*, https://legislacja.rcl.gov.pl/projekt/12304351

Widoczne jest tutaj również silne nakierowanie na przeciwdziałanie praktykom korupcyjnym m.in. w sferze gospodarczej.

Powyższe procesy powiązane są oczywiście z **należytą komunikacją, konieczną dla prawidłowego przepływu informacji**. Niezbędne są adekwatne regulacje w obszarze komunikacji wewnętrznej (np. co do samego poinformowania, że istnieje możliwość zgłaszania nieprawidłowości, sposobu tego zgłaszania), ale i zewnętrznej. Warto zauważyć, że problematyka informacji jako ważnego zasobu jest niezwykle istotna i wieloaspektowa na poziomie funkcjonowania rynków finansowych. Rozwój rynku finansowego, a co z tym związane – pojawiające się nowe formy inwestowania oraz zwiększająca się liczba podmiotów, które są jego aktorami sprawia, że prawna ochrona informacji w tym obszarze nabiera coraz istotniejszego znaczenia. Na to wszystko trzeba nałożyć postępującą informatyzację w tym sektorze. W efekcie wzrasta ryzyko co do możliwości ochrony informacji na rynku finansowym. Co więcej, należy prognozować, że trend ten będzie wzrastał[17]. Trudność polega na tym, że trzeba zbalansować z jednej strony dostęp do informacji, a z drugiej jej ochronę. Oba aspekty mają swoje niebagatelne znaczenie dla należytego funkcjonowania rynku finansowego i dotykają problematyki kluczowej dla niniejszego opracowania.

W puli działań przeciwdziałających przestępczości w ramach aktywności danego podmiotu musi mieścić się **stałe podnoszenie kompetencji (tak kadry zarządzającej, jak i pracowników)**, np. poprzez szkolenia, aby przygotować się na nowe wyzwania i podejmowanie adekwatnych reakcji na stale zmieniające się ryzyka z uwagi na złożoność i zmianę w obszarze problematyki przestępczości na rynkach finansowych.

Swoje znaczenie – tak z perspektywy należytego funkcjonowania danego podmiotu, jak i przeciwdziałając przestępczości *in genere* – mają także **przepisy eliminujące określone osoby od możliwości pełnienia określonych funkcji: orzeczenie zakazu zajmowania stanowiska, prowadzenia działalności**.

[17] Por.: A. Płońska, *Karnoprawna ochrona informacji na rynku kapitałowym*, Wrocław 2012, s. 17 in.

2. Wdrażanie systemów monitorowania pracowników i rynku

Tak jak to już zostało wspomniane wcześniej, państwowe oraz międzynarodowe systemy nadzoru i kontroli w zakresie przestępczości finansowej są wspierane przez przedsiębiorstwa i instytucje finansowe. W małych jednostkach kontrolę taką może sprawować jedna osoba, ale w większych podmiotach jest to zwykle cały wydział zajmujący się ryzykiem, spełnieniem przepisów z zakresu bezpieczeństwa i walki z przestępstwami finansowymi oraz inwigilacją[18].

W przypadku instytucji finansowych inwigilacja istnieje zawsze wobec zawieranych transakcji (są one rejestrowane przez system), większe instytucje mogą mieć także systemy monitorowania rynku[19]. Inwigilacja nie sprowadza się tylko do rejestrowania transakcji, ale także zakresu obowiązków traderów, brokerów czy pracowników back-office, do których zakresu obowiązków należy zgłaszanie podejrzanych transakcji do osoby odpowiedzialnej za analizę takich spraw. Pracownicy zwykle mają od razu zawiadamiać o nich, bez prowadzenia własnego dochodzenia ponieważ nawet jeżeli nie brakuje im doświadczenia, to mogą nie być na bieżąco ze wszystkimi regulacjami dotyczącymi danego problemu ani nie być w kontakcie z odpowiednimi organizacjami czy organami.

Monitorowanie rynku (obejmujące także transakcje spoza miejscem obrotu) wykonywane przez organizacje zwykle opiera się zarówno na systemach automatycznych, jak i na ludziach oraz bada naturę ekonomiczną zawieranych transakcji – czy służą zabezpieczaniu pozycji czy też stanowią potencjalne ryzyko prób zarobienia na oszustwie lub przestępstwie. Systemy analizują nie tylko transakcje, ale także komunikację internetową powiązaną z transakcjami. Wykrywanie nieprawidłowości powinno być traktowane jako unikanie ryzyka utraty reputacji przez przedsiębiorstwo, a nie tylko ryzyka potencjalnych kar za nieefektywną kontrolę. Skala monitorowania powinna

[18] J. Leeuw, *Monitoring & Surveillance*, *About financial crime, prevention of market abuse and detecting suspicious trading behavior*, Entrima, dokument elektroniczny, 2019.

[19] Wymagają tego m.in. następujące regulacje REMIT (*Rozporządzenie Parlamentu Europejskiego i Rady nr 1227/2011 z 25 października 2011 r. w sprawie integralności i przejrzystości hurtowego rynku energii*) oraz MAR (*Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 roku w sprawie nadużyć na rynku*).

być dostosowana do poziomu i zakresu ryzyka jednostki, jeżeli wykonuje ona niewiele transakcji rynkowych, to często wystarczy kontrola manualna, a jeżeli przeprowadza ich wiele, wtedy zwykle niezbędne jest rejestrowanie transakcji i oprogramowanie monitorujące[20]. Obowiązkiem podmiotów jest także odpowiednie szkolenie pracowników, aby byli w stanie wykrywać także skomplikowane nieprawidłowości.

Oprócz wykrywania podejrzanych przypadków podmioty muszą rejestrować występujące przypadki, a także sposób, w jaki zarządzali pojawiającym się przez takie transakcje ryzykiem. Zapisywanie szczegółów pozwala ich nie zapomnieć mimo upływu czasu. Opisane obowiązki dotyczą w szczególności wszystkich kanałów handlowych, brokerów, a także traderów. Aby ujednolicić sposób takiego dokumentowania często wykorzystuje się standardy ESMA[21]. W ramach wspomnianych standardów wymaga się profilowania transakcji i klientów, dzięki czemu automatyczny system może wyłapywać nieregularności (system bada nie tylko wykonane transakcje, ale także korekty i anulowane transakcje), które jako alarm trafiają do dalszego przetwarzania. Następnie podejrzane transakcje są porównywane ze wzorcami zachowań i transakcji danej firmy i innych znanych jej wzorców. Jeżeli sprawa nadal wydaje się podejrzana, wtedy zwykle zaczyna się dochodzenie, w którym w pierwszym kroku pytane są osoby, które daną czynność wykonały. Mają oni wyjaśnić cel ich działania. Jeżeli po tych wyjaśnienia pozostają wątpliwości, to sprawa jest kierowana do odpowiedniej instytucji nadzoru, a osoby w nią zamieszane nie są informowane o postępach dochodzenia. Cały proces śledztwa musi być przeprowadzony z zachowaniem najwyższej dyskrecji, gdyż chodzi o reputację osób i podmiotów związanych ze sprawą, a także o to, aby nie zniszczono dowodów związanych ze sprawą.

Instytucje muszą także wdrażać odpowiednie procedury do identyfikowania nieprawidłowości. Muszą one być sporządzone na piśmie i dostosowane do specyfiki każdej części instytucji czy przedsiębiorstwa. Powinny opisywać rolę i odpowiedzialność każdego departamentu, a także zatrudnionych w nim osób. Z uwagi na różnorodność rynków, na jakich mogą działać poszczególne

[20] J. Leeuw, *Monitoring & Surveillance…*, op. cit.

[21] ESMA – Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ang. *European Securities and Markets Authority*).

podmioty (energia, gaz, spot, futures itd.), nie da się ustalić uniwersalnych procedur i każde przedsiębiorstwo czy instytucja musi je stworzyć samodzielnie na własne potrzeby.

3. Rozwiązania organizacyjne w zakresie monitorowania pracowników dokonujących transakcji na rynkach finansowych

Pewne ramy dotyczące rozwiązań organizacyjnych można znaleźć w sugestiach agencji ACER (ang. The Agency for the Cooperation of Energy Regulators). Sugestie dotyczą następujących obszarów: tworzenie procedur, pracownicy oraz systemy. Jeżeli chodzi o tworzenie procedur, to ACER opublikował zalecenia dotyczące strategii monitorowania rynku, procedur związanych z zasobami ludzkimi, komunikacji oraz procedur związanych z identyfikowalnością transakcji. Przede wszystkim procedury muszą być udokumentowane, jak również ich wszelkie zmiany. Udokumentowane ma być również ich wdrożenie i stosowanie przez instytucję zasad w nich opisanych. Obydwa rodzaje dokumentacji muszą być utrzymywane przez co najmniej 5 lat.

Jeżeli chodzi o pracowników, to wszyscy pracownicy, których czynności są podporządkowane określonym uregulowaniom prawnym, nie tylko muszą być tego świadomi, ale również rozumieć znaczenie tekstu prawniczego co do jego istoty. Dotyczy to m.in. osób posiadających dostęp do wewnętrznch informacji, takich jak akcjonariusze, dyrektorzy, menedżerowie, a także traderzy, brokerzy, osoby z komórek nadzoru i kontroli. Ci, którzy monitorują rynek albo uczestniczą w rynku muszą posiadać odpowiednie umiejętności i kwalifikacje. Muszą oni rozumieć i znać aktualne przepisy prawne oraz znać i rozumieć wszystkie rodzaje nadużyć, jakie mogą napotkać. Traderzy muszą także oprócz wiedzy posiadać odpowiednią samokontrolę i zdolność do panowania nad emocjami i uczuciami, aby podejmować racjonalne decyzje bez konieczności nieustannego nadzoru zwierzchników. Dlatego przy tworzeniu systemu zarządzaniu traderami i ich doborze oprócz kompetencji twardych należy oceniać ich cechy charakteru i miękkie umiejętności. Instytucja wprowadzająca strategie przeciwdziałania nadużyciom finansowym,

jeżeli jest emitentem, to na podstawie rozporządzenia MAR[22] musi stworzyć i aktualizować listę osób posiadających dostęp do poufnych informacji. MAR i inne przepisy dopuszczają bowiem nieujawnianie od razu informacji poufnych, ale występując do władz nadzoru o wyjątek, emitent musi także przekazać listę osób posiadających dostęp do informacji poufnych (które potencjalnie mogą się dopuścić insider tradingu). Lista insiderów musi posiadać informacje, takie jak: imię i nazwisko danej osoby, od kiedy i do jakich informacji posiada dostęp oraz dlaczego go otrzymała (a także datę, kiedy sporządzono samą listę).

Zalecenia ACER co do systemów monitoringu to przede wszystkim nieustanna weryfikacja wszystkich zleceń i transakcji. Oznacza to nadzór nad księgą zleceń oraz transakcjami, aby można było w każdym momencie powiązać je ze sobą.

Na temat monitorowania rynku więcej zaleceń można znaleźć w dokumencie „Praktyki uzyskiwania Efektywnego Handlu Energią zgodnego z regulacjami[23]" opublikowanym przez Federalną Komisję Regulacji Energetyki (ang. *Federal Energy Regulatory Commission* – FERC). Zawiera ona listę sprawdzonych w praktyce technik monitoringu transakcji, które sprawdziły się w różnych organizacjach. Należą do nich:

1. Przeglądy statystyczne, czyli zestawienia i statystyki opisujące koncentrację pozycji oraz opisujące aktywność firmy na poszczególnych rynkach i rynkach z nimi związanymi. Analizowane są zrealizowane transakcje, złożone zlecenia, i zajmowane w danym czasie pozycje. Zestawienia takie pozwalają identyfikować słabe punkty oraz miejsca, gdzie najbardziej należy spodziewać się nadużyć finansowych. Statystyki takie pozwalają m.in. identyfikować próby traderów do manipulowania cenami instrumentów finansowych. Analiza powinna obejmować badanie zmienności, płynności rynku, korelacji z innymi rynkami, aby określić do jakiego stopnia dany uczestnik rynku jest w stanie wpływać na cenę rynkową danego instrumentu. Analizowane

[22] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 roku w sprawie nadużyć na rynku.*

[23] Federal Energy Regulatory Commission, *Staff White Paper on Effective Energy Trading Compliancy Practices*, listopad 2016, s. 14–18, https://www.ferc.gov/CalendarFiles/20161117125529-WhitePaperCompliance.pdf (dostęp: 19.09.2019).

powinny być także ekspozycja cenowa i wolumenowa, gdyż pozwalają one określić, które manipulacyjne transakcje są najbardziej prawdopodobne, gdyż przyniosłyby traderom zysk. Szczególna kontrola powinna obejmować transakcje na 2 rynkach, np.: fizycznym i finansowym, może opierać się na próbkowaniu lub nadzorze automatycznym. Podobnym handlem jest handel wirtualny (także dokonuje się na 2 rynkach), gdzie następuje wirtualna wymiana instrumentów bazowych i praw własności.

2. Kontrola wyniku finansowego powinna analizować nie tylko całokształt rachunku zysków i strat, ale także wynik finansowy na poszczególnych transakcjach (wynik zrealizowany lub niezrealizowany), wynik na danym instrumencie finansowym, na danej lokalizacji. Wyniki powinny być porównywane z wielkością otwartych pozycji.
3. Okresowa kontrola ofert opartych na kosztach (ang. *cost based offers*), jakie otrzymują firmy zajmujące się przesyłem albo dystrybucją energii za jednostkę wytwórczą[24], aby nie manipulowali tą ceną w celu wpływania na to, jak często jednostka wytwórcza jest wzywana do produkcji energii oraz jakie otrzymuje opłaty.
4. Kontrola przesyłu gazu i zestawienie go z nominacjami złożonymi na dany okres, sprawdzanie, czy nie manipulowano nominacjami, aby otrzymać wyższy udział w przesyle w okresach nadmiaru nominacji oraz czy nie wykonywano dosyłu.
5. Rejestrowanie całej komunikacji traderów w firmach tradingowych ze wszystkich platform komunikacyjnych. W tym celu organizacja powinna przygotować regulamin określający których telefonów, komputerów, e-maili, komunikatorów traderzy mogą używać oraz informować o tym, że cała komunikacja jest rejetrowana i archiwizowana na co najmniej 5 lat. Zarejestrowana komunikacja powinna być analizowana przez oprogramowanie wyszukujące podejrzane kontakty. Oprogramowanie powinno być regularnie uaktualniane i rozwijane.

[24] Por. *Regulacja UE No 543/2013 on submission and publication of data in electricity markets*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0543&from=EN (dostęp: 10.09.2019).

6. Instytucje powinny stworzyć środowisko zachęcające menedżerów i pracowników do omawiania zgodności działań i regulaminów instytucji z wymogami prawa, a także problemów, jakie z tym wystąpiły w praktyce. Osoby, które napotkały nieprawidłowości, powinny nie bać się je zgłosić natychmiast po ich wystąpieniu bez obaw o zemstę. Każdy pracownik nie może się bać zadawać pytań kolegom o sprawy, które wydają mu się podejrzane. Instytucje mają obowiązek chronienia takich osób i nieujawniania ich danych osobowych, jeżeli zgłosili nieprawidłowości.
7. Instytucje powinny założyć portal pozwalający pracownikom anonimowo zgłaszać zaobserwowane nieprawidłowości lub podejrzane transakcje.

4. Regulacje polskie oraz unijne obowiązujące w Polsce dotyczące systemów zapobiegających praniu brudnych pieniędzy i finansowaniu terroryzmu w bankach i instytucjach finansowych

Bardzo dużo zaleceń wobec organizacji stworzono w zakresie walki z praniem brudnych pieniędzy i finansowaniem terroryzmu. Jedne z najstarszych pochodzą z 1989 r.[25] i są to zalecenia FATF z zakresu przeciwdziałania praniu brudnych pieniędzy i finansowaniu terroryzmu i proliferacji. W odniesieniu do instytucji finansowych (w 2019 r. grupa ta obejmuje: banki, instytucje pożyczkowe, SKOKi, firmy zajmujące się transferami pieniędzy, firmy zajmujące się obrotem nieruchomościami, fundusze inwestycyjne, instytucje finansowe, spółki prowadzące rynki uregulowane, zakłady ubezpieczeń, kantory i firmy prowadzące działalność kantorową, w ograniczonym zakresie także adwokaci, notariusze, księgowi, przedsiębiorstwa zajmujące się tworzeniem jednostek organizacyjnych, przedsiębiorstwa dokonujące transakcji gotówkowych o wartości co najmniej 10 tys. euro w powiązanych transakcjach[26])

[25] Urząd Komisji Nadzoru Finansowego, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy i Finansowania Terroryzmu oraz Proliferacji*, Warszawa [b.r.].

[26] A. Berger, *Kogo dotyczy ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu*, Rzeczpospolita, 18.05.2018, https://www.rp.pl/Firma/305189982-Kogo-dotyczy-ustawa-o-przeciwdzialaniu-praniu-pieniedzy-i-finansowaniu-terroryzmu.html (dostęp: 1.09.2019).

nałożono na nie obowiązki opisane poniżej. Wydaje się, że poprawę bezpieczeństwa systemu finansowego można by osiągnąć, gdyby objąć chociaż częścią z tych regulacji jednostki obecnie wyjęte spod tych przepisów, a prowadzące zbliżoną działalność – platformy internetowe pozwalające dokonywać transakcji finansowych, być może także wirtualne kasyna.

1. Badanie klienta, co oznacza m.in. zakaz tworzenia rachunków anonimowych albo na fałszywe dane osobowe, ale także obowiązkowe badanie klienta, jeżeli instytucja finansowa nawiązuje z kimś relacje biznesowe, przy przekroczeniu progu kwotowego jednej transakcji, kiedy system nadzoru sygnalizuje ryzyko prania brudnych pieniędzy, jeżeli instytucja ma wątpliwości co do prawdziwości podanych danych.
2. Przechowywanie dokumentacji przez okres co najmniej 5 lat od zakończenia współpracy z klientem. Przechowywanie dotyczy wszystkich informacji o kliencie: dane identyfikacyjne, dane dotyczące kont, korespondencję, wyniki wszystkich przeprowadzonych analiz.
3. W przypadku osób zagranicznych zajmujących eksponowane stanowiska polityczne instytucje finansowe powinny dodatkowo posiadać odpowiednie systemy zarządzania ryzykiem, aby określić, czy dany klient kwalifikuje się pod tę kategorię, uzyskać zgodę kadry zarządzającej na współpracę z taką osobą, ustalić źródła majątku i jego pochodzenie od takich osób, stale monitorować relacje biznesowe.
4. W przypadku bankowości korespondencyjnej instytucje finansowe powinny zebrać dane o kliencie korespondencyjnym, aby zrozumieć naturę jego działalności i reputację, oraz czy jednostka była przedmiotem śledztwa w zakresie prania brudnych pieniędzy bądź finansowania terroryzmu albo sankcji regulatora, a także ocenić sprawność systemów kontroli klienta przeciwko praniu pieniędzy i finansowaniu terroryzmu. Przed nawiązaniem współpracy biznesowej konieczna jest zgoda kadry zarządzającej, a po jej nawiązaniu właściwe rozumienie obowiązków poszczególnych instytucji i sprawdzanie w przypadku kont przejściowych, że bank korespondent zweryfikował tożsamość oraz przeprowadził badanie klientów mających bezpośredni dostęp do kont korespondenta (oraz że jest w stanie dostarczeć dane dotyczące identyfikacji tych klientów).

5. W przypadku usług przekazywania pieniędzy lub środków każda osoba fizyczna lub prawna działająca jako agent powinna być licencjonowana i objęta monitorowaniem, czy realizuje programy przeciwdziałania praniu pieniędzy i finansowania terroryzmu.
6. W przypadku klientów lub transakcji z krajów podwyższonego ryzyka instytucje finansowe mają obowiązek wzmożonego badania klientów.
7. Instytucje finansowe mają obowiązek raportowania podejrzanych klientów i są chronione przed konsekwencjami złamania tajemnicy bankowej i poufności.
8. Oprócz instytucji finansowych obowiązek badania klienta i przechowywania danych obejmuje także: kasyna, pośredników nieruchomości, dilerów kamieni i metali szlachetnych, prawników i notariuszy oraz księgowych (jeżeli wykonują dla klienta transakcje finansowe lub na nieruchomościach), podmioty świadczące usługi prawne dla trustów i spółek (jeżeli zakładają dla nich lub zarządzają spółkami).

Kolejna grupa zaleceń została utworzona przez Grupę Wolfsberg[27]:

W zakresie prania pieniędzy:

1. Banki i instytucje finansowe powinny szacować ryzyko prania pieniędzy przez klienta i w zależności od poziomu tego ryzyka stosować odpowiednie procedury.
2. W stosunku do istniejących klientów, kiedy wdrażane są nowe przepisy, instytucje mogą same ocenić, czy mają dodatkowo badać istniejących klientów, czy też istniejące systemy kontroli są wystarczające i klienci zostali wystarczająco zbadani.
3. Przy ocenie ryzyka danego klienta bierze się pod uwagę wartość jego aktywów, rozmiar transakcji, jakie przepisy aplikują się do danego klienta, czas i regularność współpracy z klientem, znajomość jurysdykcji, której podlega klient, do jakiego stopnia klient wykorzystuje dziwne narzędzia i instrumenty niemające uzasadnienia w jego działalności.

[27] Wolfsberg Group, *Guidance on a Risk Based Approach for Managing Money Laundering Risk*s, 2006, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf (dostęp: 20.08.2019).

4. W przypadku wysokiego ryzyka instytucje finansowe powinny uruchomić posiadane procedury i narzędzia kontroli, aby zapobiec praniu pieniędzy.
5. Instytucje powinny brać pod uwagę ryzyko kraju klienta (w zakresie prania pieniędzy), ryzyko klienta, ryzyko usług.
6. Instytucje powinny szkolić pracowników w zakresie zapobiegania praniu pieniędzy.

W zakresie finansowania terroryzmu[28]:

1. Instytucje powinny dokładnie znać swoich klientów, aby mieć pewność, że nie uczestniczą w finansowaniu terroryzmu.
2. Instytucje finansowe powinny przeprowadzić szczególnie dokładną weryfikację klientów, jeżeli są związani z sektorami wysokiego ryzyka i aktywnościami wysokiego ryzyka (przekazy pieniężne, kantory, biura wymiany).
3. Instytucje powinny monitorować transakcje pod kątem finansowania terroryzmu, biorąc pod uwagę zagrożone tym kraje i sektory, listy od władz z osobami podejrzanymi o terroryzm, współpracować z instytucjami zapobiegającymi terroryzmowi, zmieniać strategie monitorowania, aby dopasować się do zachodzących zmian.
4. Instytucje finansowe powinny zgłaszać klientów podejrzanych o terroryzm na listę prowadzoną przez grupę Wolfsberg z uzasadnieniem, dlaczego ten klient jest podejrzewany o terroryzm.

Kolejne wytyczne można znaleźć w dokumencie zatytułowanym: Łączne wytyczne określone artykułami 17 i 18(4) Dyrektywy (EU)2015/849 o uproszczonym i rozszerzonym badaniu *due dilligence* oraz czynnikami, jakie instytucje finansowe i kredytowe powinny rozważyć, kiedy oceniają ryzyko prania pieniędzy i finansowania terroryzmu związane ze związkami biznesowymi i okazjonalnymi transakcjami[29].

---

[28] Wolfsberg Group, *Wolfsberg Statement on the Suppression of the Financing of Terrorism*, 2002, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/16.%20Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_%282002%29.pdf

[29] *Joint Guidelines under Articles 17 and 18(4) of Directive (EU)2015/849 on simplified and enhanced customer due diligence andthe factors credit and financial institutions should consider whenassessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions*, https://eba.europa.eu/

1. Instytucja w ocenie zagrożenia powinna brać pod uwagę, jak ryzykowna jest branża w której działa klient, przeprowadzać badanie *due diligence* klienta, uzyskać ogólną, holistyczną ocenę ryzyka danego klienta, moniotorować to ryzyko i przeprowadzać okresową aktualizację tej oceny.
2. Instytucje powinny oceniać poziom ryzyka (prania pieniędzy lub finansowania terroryzmu), zanim nawiążą z danym klientem współpracę lub wykonają określoną transakcję.
3. Instytucje powinny korzystać z wielu źródeł informacji przy ocenie ryzyka (o ile jest to możliwe).
4. Instytucje finansowe powinny korzystać z informacji dotyczących ryzyka pochodzących z Komisji Europejskiej, rządu, instytucji rządowych, GIIF, regulacji prawnych, ale także z własnego doświadczenia, innych instytucji z własnej branży, wskaźników korupcji i raportów o danym kraju, danych statystycznych i opracowań uniwersyteckich.
5. Przy ocenie ryzyka klienta (i osoby, na której rzecz działa klient) instytucja powinna brać uwagę charakterystykę samego klienta, czym się zajmuje zawodowo, reputację klienta i osoby, na rzecz której on działa, a także naturę i zachowanie obydwu.
6. Instytucja powinna przy ocenie ryzyka brać pod uwagę, czy klient i osoba, na rzecz której działa, mają powiązania z sektorami biznesowego podwyższonego ryzyka (także łapówek i korupcji), takimi jak budownictwo, przemysł farmaceutyczny, opieka zdrowotna, transfery pieniężne, kasyna, handel cennymi metalami, czy klient posiada powiązania z sektorami działalności gospodarczej wymagającymi dużych kwot pieniężnych.
7. Instytucja powinna w przypadku klienta będącego osobą prawną ustalić, czym się firma dokładnie zajmuje.
8. Instytucja powinna ustalić, czy klient nie jest osobą PEP (ang. *politically exposed person*), czyli osobą zajmującą eksponowane stanowisko polityczne, albo działa na rzecz takiej osoby, albo posiada powiązania z taką osobą. Jeżeli tak, to musi zastosować stały nadzór nad jego

documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf, (dostęp: 11.09.2019).

rachunkiem. Podobnie instytucja musi postąpić, jeżeli osoba ma duży wpływ na życie publiczne kraju, zawierane umowy, decyzjelub na wysokiej rangi komitety sportowe albo posiada kontakty z takimi osobami.

9. Instytucja musi sprawdzić, czy klient nie jest powiązany albo nie kieruje spółką notowaną na giełdzie. Również tutaj obowiązuje szczególny nadzór.
10. Jeżeli klient jest instytucją kredytową albo finansową, to instutucja prowadząca jej rachunek musi się upewnić, że klient stosuje wszystkie przepisy dotyczące prania pieniędzy i finansowania terroryzmu.
11. Jeżeli klientem instytucji finansowej są władze lub administracja albo spółka, to instytucja ma obowiązek sprawdzić, czy działają na terenach z niską korupcją.
12. Instytucja musi sprawdzić, czy dane podane przez klienta oraz dane o osobie, na której rzecz klient działa, są zgodne z rzeczywistością.
13. Instytucja musi sprawdzić, czy w mediach nie ma publikacji o działalności przestępczej klienta (w zakresie prania pieniędzy i finansowania terroryzmu), a także czy klient nie miał zamrożonych aktywów w związku praniem pieniędzy i finansowaniem terroryzmu albo w przeszłości nie wykonywał podejrzanych transakcji.
14. Instytucja musi sprawdzić, czy nie posiada danych o długoletniej współpracy z danym klientem.
15. Instytucja finansowa musi sprawdzić, czy nie zachodzi ryzyko, że klient jest słupem (smerfem).
16. Instytucja finansowa ma obowiązek sprawdzić, czy operacje klienta nie są nadmiernie skomplikowane, ustrukturyzowane oraz czy mają uzasadnienie ekonomiczne.
17. Instytucja finansowa musi sprawdzić, czy klient nie domaga się nadmiernego poziomu utajnienia transakcji.
18. Instytucja musi upewnić się, że majątek klienta i jego dochody pochodzą z legalnych źródeł i są możliwe do uzyskania w wyniku prowadzonej przez klienta działalności.
19. Instytucja musi upewnić się, że klient regularnie używa usług finansowych, jakie chciał przy nawiązaniu współpracy.
20. Instytucja musi upewnić się, że potrzeby klienta zagranicznego nie zostałyby dużo lepiej zaspokojone przez instytucje w jego kraju.

21. Instutucja musi sprawdzić poziom ryzyka prania pieniędzy i finansowania terroryzmu dla jurysdykcji, gdzie klient ma siedzibę, gdzie prowadzi działalność i gdzie ma powiązania biznesowe.
22. W przypadku, gdy pieniądze klienta zostały zarobione za granicą, bank musi ocenić, jak duże jest ryzyko, że są związane z nielegalną działalnością i jak dobre są w tym kraju procedury walki z praniem pieniędzy i finansowaniem oraz czy kraj wdrożył procedury walki z praniem pieniędzy i finansowaniem terroryzmu i innych przestępstw finansowych.
23. Kiedy instytucje określają poziom ryzyka związany z oferowanymi przez nie produktami, usługami i transakcjami, firmy powinny rozważyć takie czynniki ryzyka jak: poziom transparentności i skomplikowania produktu, wartość, czy klient nie zachowuje anonimowości, czy nie wykonuje poleceń innych osób, ile jurysdykcji jest zaangażowanych, czy strony transakcji przyjmują nadpłaty albo wpłaty od osób trzecich, czy instytucja rozumie ryzyko swoich produktów, usług i transakcji i czy wykorzystują one innowacyjne i nowatorskie technologie, jak duże są transakcje i na ile angażują rozliczenia gotówkowe.
24. Instytucja powinna badać ryzyko kanałów dostarczania usług – na ile są anonimowe, ilu bierze w nich udział pośredników i jak są powiązani z klientem.
25. Instytucja powinna odnotować, czy klient realizując usługę, pojawił się osobiście, aby go zidentyfikować, jeżeli rekomenduje go inna osoba, na ile można jej zaufać, jeżeli klient korzysta z pośrednika, czy nie jest on powiązany z zagrożeniem praniem pieniędzy lub finansowaniem terroryzmu.
26. Instytucja powinna stosować inne wagi, obliczając ostateczny scoring fraudowy klienta w zależności od tego, czy jest to stała współpraca czy jednorazowa transakcja.

Kolejne wymogi dotyczące procedur zapobiegające praniu pieniędzy i finansowania terroryzmu znajdują się w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych. Nakłada ona m.in. następujące obowiązki:

1. Aby sprawdzić, czy wymagane informacje o płatniku i odbiorcy są dołączane do transferów środków pieniężnych oraz pomóc

w identyfikowaniu podejrzanych transakcji, dostawca usług płatniczych odbiorcy i pośredniczący dostawca usług płatniczych powinni posiadać skuteczne procedury pozwalające wykryć ewentualny brak lub niekompletność informacji o płatniku i odbiorcy. Procedury te powinny w stosownych przypadkach obejmować monitorowanie po zdarzeniu lub monitorowanie w czasie rzeczywistym. Właściwe organy powinny zatem dać możliwość zamieszczania przez dostawców usług wymaganych informacji o transakcji w przekazach pieniężnych lub powiązanych komunikatach na każdym etapie łańcucha płatności[30].

2. Ze względu na potencjalne zagrożenie praniem pieniędzy oraz finansowaniem terroryzmu, jakie stwarzają transfery anonimowe, dostawców usług płatniczych należy zobowiązać do tego, by żądali podania informacji o płatniku i odbiorcy. Zgodnie z opracowanym przez FATF podejściem opartym na analizie ryzyka należy określić obszary charakteryzujące się wyższym i niższym ryzykiem w celu skuteczniejszego zwalczania ryzyk związanych z praniem pieniędzy i finansowaniem terroryzmu. Dostawca usług płatniczych odbiorcy oraz pośredniczący dostawca usług płatniczych powinni zatem posiadać skuteczne procedury oparte na analizie ryzyka mające zastosowanie w przypadkach, gdy transfer środków pieniężnych nie zawiera wymaganych informacji o płatniku lub odbiorcy, pozwalających na zdecydowanie, czy dany transfer należy zrealizować, odrzucić lub wstrzymać oraz aby określić stosowne dalsze kroki, jakie należy podjąć.
3. Dostawca usług płatniczych odbiorcy oraz pośredniczący dostawca usług płatniczych powinni – dokonując oceny ryzyk – zachowywać szczególną czujność, gdy stwierdzą brak albo niekompletność informacji o płatniku lub odbiorcy, oraz powinni zgłaszać właściwym organom podejrzane transakcje zgodnie z obowiązkami zgłaszania określonymi w dyrektywie (UE) 2015/849 oraz z krajowymi środkami transponującymi tę dyrektywę.

[30] *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015, Regulation (EU) 2015/847 Of The European Parliament And Of The Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.*

4. Instytucje finansowe muszą niezwłocznie odpowiadać na żądania o udzielenie informacji o płatniku i odbiorcy kierowane przez organy odpowiedzialne za zwalczanie prania pieniędzy lub finansowania terroryzmu w państwach członkowskich, w których ci dostawcy usług płatniczych mają siedziby.
5. Liczba dni przewidzianych na udzielenie odpowiedzi na żądanie o udzielenie informacji o płatniku uzależniona jest od liczby dni roboczych w państwie członkowskim dostawcy usług płatniczych płatnika.

Dodatkowych wytycznych dostarcza Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu[31]. Dyrektywa wnosi następujące wymogi:

1. Instytucje finansowe mają obowiązek gromadzić szczegółowe informacje o trustach, strukturach własnościowych spółek i innych podmiotów gospodarczych.
2. Instytucje finansowe muszą szczególnie dokładnie monitorować transakcje z krajami wysokiego ryzyka.
3. Instytucja musi starannie nadzorować swoich pracowników, bo brak skutecznej kontroli będzie traktowany jako przestępstwo korporacyjne.
4. Dyrektywa wdraża także scenralizowany rejestr beneficjentów rzeczywistych i klienci instytucji finansowych działający na rzecz innych osób będą musieli podać szczegółowe dane na temat beneficjenta, który zostanie umieszczony w scentralizowanym rejestrze.

W dużym stopniu implementację tych wytycznych dla Polski wdrożyła nowa ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, która weszła w życie 13 lipca 2018 r. Ustawa określa także, które instytucje podlegają określonym w przepisach wymaganiom. Są to m.in.: banki, SKOKi, firmy inwestycyjne, firmy ubezpieczeniowe, adwokaci, radcy prawni, doradcy podatkowi, notariuze, stowarzyszenia posiadające osobowość prawną, przyjmujące płatność w gotówce o wartości min. 10 tys

[31] *Directive (Eu) 2015/849 Of The European Parliament And Of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.*

euro, lombardy, kantory, Poczta Polska S.A., podmioty prowadzące działalność gospodarczą, świadczące usługi i pośredniczące w zakresie wymiany walut wirtualnych. Instytucje te muszą wobec swoich klientów stosować środki bezpieczeństwa finansowego, do których należą: identyfikacja klienta, weryfikacja jego tożsamości, a także identyfikacja beneficjenta rzeczywistego.

W końcu należy wspomnieć o Dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE. Wzmacnia ona monitorowanie transakcji, których stroną jest podmiot z państwa tzw. wysokiego ryzyka. Dyrektywa dokonuje też centralizacji krajowych rejestrów kont bankowych i płatniczych. Została opublikowana 19 czerwca 2018 r., a 9 lipca 2018 r. weszła w życie (dyrektywa UE 2018/843 z dnia 30 maja 2018 r., Dz.U. UE nr L 156/43).

Dodatkowe obowiązki związane z zapobieganiem przestępstwom finansowym narzuca Rozporządzenie Ochronie Danych Osobowych[32], popularnie nazywane w Polsce RODO. W Polsce zostało wdrożone na mocy ustawy z dnia 10 maja 2018 r. ochronie danych osobowych[33]. W myśl przepisów instytucje finansowe, ale również przedsiębiorstwa niefinansowe mają obowiązek szczególnej ochrony danych osobowych ich klientów (zdefiniowano także dane wrażliwe, czyli dane o pochodzeniu etnicznym, wyznaniu, opiniach politycznych, stanie zdrowia, karach i skazaniach). Obejmuje to m.in.:

1. Jednostka ma obowiązek usunięcia danych osobowych, jeżeli nie są już potrzebne.
2. Jednostka ma dawać możliwość wglądu, edycji lub usunięcia danych na żądanie osoby, której dotyczą.
3. W każdym przedsiębiorstwie musi być powołany inspektor ochrony danych.
4. Przedsiębiorstwo musi prowadzić rejestr, w jakim celu, w jaki sposób i przez kogo dane są przetwarzane.

---

[32] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych.*

[33] *Ustawa z dnia 10 maja 2018 roku ochronie danych osobowych (Dz.U. 2018 poz 1000).*

5. Przedsiębiorstwo musi chronić komputery firmowe i urządzenia mobilne przez używanie legalnych i aktualnych systemów operacyjnych, programów antywirusowych oraz oprogramowania użytkowego.
6. Przedsiębiorstwo musi zapobiegać wyciekom danych, szyfrować dane, monitorować zasoby własnych danych i nadzorować uprawnienia.
7. Przedsiębiortwo musi prowadzić rejestry przetwarzania danych osobowych i w bezpieczny sposób wymieniać sprzęt (trwale usuwać zapisane na nim dane).

5. Nowe rozwiązania i propozycje zwalczania nadużyć podatkowych

Pomimo aktywności podejmowanych przez zarówno krajowe, jak i międzynarodowe władze, ustalenie skutecznych metod ograniczenia skali ucieczki od podatku wydaje się wciąż nierozwiązane. Obok stosowanych narzędzi o długoletniej tradycji, tj. kontrola podatkowa, czynności sprawdzające czy mechanizm odwrotnego obciążenia, do systemów implementowane są także innowacyjne rozwiązania, które mają zapewnić prawidłowe rozliczanie się z podatków. Są to obowiązujący w wielu krajach, a od niedawna także w Polsce np. mechanizm podzielonej płatności (*split payment*) bądź tzw. mały punkt kompleksowej obsługi (*mini one stop shop* – MOSS)[34]. Nowo adoptowane narzędzia nierzadko wykorzystywane są do wzmocnienia lub zastąpienia istniejących rozwiązań. Jak dowodzi praktyka, poddane rzeczywistej weryfikacji narzędzia nie zawsze okazują się bowiem wystarczająco skuteczne. Jednym z takich przykładów jest mechanizm odwrotnego obciążenia, który z uwagi na przesuwanie się oszustw na inne branże lub towary obejmuje coraz to większą liczbę produktów. W 2018 r. na wniosek niektórych krajów UE[35] Komisja

[34] *VAT on digital services (MOSS scheme)*, https://europa.eu/youreurope/business/taxation/vat/vat-digital-services-moss-scheme/index_en.htm (dostęp: 26.08.2019); *Analysis of the impact of the split payment mechanism as an alternative VAT collection method,* Final Report, Publications Office of the European Union 2017, s. 9.

[35] Pierwszymi krajami proponującymi to rozwiązanie były Niemcy i Austria, które w 2006 r. wnioskowały do Komisji Europejskiej o zgodę na zastosowanie mechanizmu dla dostaw towarów (na kwotę powyżej 5000 Euro) i świadczenia usług (na kwotę powyżej 10 000 Euro). W 2019 r. z wnioskiem wystąpiły Czechy, a Rumunia może być drugim z kolei państwem, które wyraża zainteresowanie implementacją powszechnego odwrotnego

Europejska wyraziła zgodę na zastosowanie czasowego powszechnego odwrotnego obciążenia (*gener-alised reverse charge mechanizm*)[36], z obawy o to, że mechanizm ten choć zaadoptowany, aby eliminować oszustwa podatkowe, to w dłuższej perspektywie może przyczynić się do powstawania nieprawidłowości. Stąd niektóre kraje rozważają zastąpienie w ogóle mechanizmu odwrotnego obciążenia systemem podzielonej płatności. Wśród nich są Włochy, Rumunia, a także Polska. Komisja Europejska wydała zgodę, aby w Polsce wprowadzić obowiązkowy *split payment* do 28 lutego 2022 r. m.in. dla wyrobów ze stali, smartfonów, laptopów czy robót budowlanych.

Natomiast mały punkt kompleksowej obsługi, który obecnie stanowi w Polsce fakultatywne rozwiązanie upraszczające[37], jest jednym z elementów propozycji Komisji Europejskiej zawartych Action Plan z 2016 r. dotyczącego utworzenia jednego europejskiego obszaru VAT (*single VAT area*). Co do istoty, jednolity system VAT opierałby się na kilku zasadach, z których pierwsza zakłada, aby wewnątrzwspólnotowa dostawa towarów była opodatkowana jak transakcja krajowa, według stawki VAT obowiązującej w państwie nabywcy. Podatek byłby pobierany przez organy podatkowe kraju dostawcy, a następnie przekazywany do kraju nabywcy. Zgodnie z propozycją Komisji przedsiębiorcy mogliby rozliczać transakcje wewnątrzwspólnotowe

obciążenia. Ibid., s. 23. P. Arak i in., *Krótka historia VAT w Polsce*, Polski Instytut Ekonomiczny, „Policy Paper", 2019, nr 3, s. 23.

[36] Podstawą wprowadzenia zmian jest *decyzja wykonawcza Rady (UE) 2019/310 z dnia 18 lutego 2019 r. upoważniająca Polskę do wprowadzenia szczególnego środka stanowiącego odstępstwo od art. 226 dyrektywy 2006/112/WE w sprawie wspólnego systemu podatku od wartości dodanej (Dz. Urz. UE L 51/19).*

[37] MOSS umożliwia elektroniczne złożenie kwartalnej deklaracji VAT, jak również wpłacenie należnego właściwym państwom członkowskim UE VAT z tytułu świadczenia wybranych usług. Wpłacony podatek jest przekazywany za pośrednictwem krajowej administracji do państw członkowskich kraju konsumpcji. *Rozporządzenie wykonawcze Rady (UE) nr 1042/2013 z dnia 7 października 2013 r. zmieniające rozporządzenie wykonawcze (UE) nr 282/2011 w odniesieniu do miejsca świadczenia (Dz. Urz. UE L 284 z 26.10.2013, str. 1), rozporządzenie Rady (UE) nr 967/2012 z dnia 9 października 2012 r. zmieniające rozporządzenie wykonawcze (UE) nr 282/2011 w odniesieniu do procedur szczególnych dotyczących podatników niemających siedziby, którzy świadczą usługi telekomunikacyjne, usługi nadawcze lub usługi elektroniczne na rzecz osób niebędących podatnikami (Dz. Urz. UE L 290 z 20.10.2012).*

za pośrednictwem punktów kompleksowej obsługi. Oznacza to, że podmioty mogłyby składać deklaracje i opłacać VAT za pomocą jednego portalu internetowego[38].

Kolejnym założeniem wynikającym z Planu jest uproszczenie przepisów dotyczących wystawiania faktur. Podatnicy dokonujący dostawy towarów/świadczenia usług mogliby wystawiać faktury zgodnie z przepisami obowiązującymi w państwie ich siedziby. Ponadto zniesiony zostałby obowiązek przygotowywania tzw. informacji podsumowującej. Interesującym rozwiązaniem jest również propozycja powołania instytucji certyfikowanego podatnika (*certified taxable person*). Uzyskanie takiego statusu uprawniałoby do stosowania uproszczonych procedur w zakresie deklarowania i zapłaty VAT transgranicznego[39]. Status zaufanego podatnika byłby honorowany przez wszystkie państwa UE. Wprowadzenie nowego modelu opodatkowania transakcji wewnątrzwspólnotowych planowane jest na 2023 r. Przewiduje się, że proponowane zmiany wpłyną na m.in. ograniczenie wyłudzeń VAT z uwagi na eliminację stosowania stawki 0% i uproszczą kontrolę rozliczenia VAT[40].

Z kolei w 2018 r. Komisja Europejska zaproponowała wprowadzenie do systemów krajowych tzw. podatku od usług cyfrowych. Z uwagi na trudności w określeniu jednego standardu, chociaż obecnie to OECD pracuje nad międzynarodowym rozwiązaniem, niektóre kraje podjęły działania w tym kierunku. Francja i Węgry przyjęły swoistego rodzaju podatek od usług cyfrowych. Natomiast Austria, Belgia, Czechy, Włochy, a także Polska, Słowenia, Hiszpania i Wielka Brytania ogłosiły lub opublikowały propozycję wprowadzenia podatku od usług cyfrowych, którego stawka w zależności od kraju wahać się może w przedziale 2–7,5%[41].

---

[38] European Commission – Press Release, *VAT: More flexibility on VAT rates, less rade tape for small businesses, Brussels*, 18 January 2018, http://europa.eu/rapid/press-release_IP-18-185_en.htm (dostęp: 16.05.2018).

[39] Dostawca nie naliczałby VAT zgodnie ze stawką obowiązującą w kraju odbiorcy, a jedynie wskazywałby na fakturze, że VAT zostanie rozliczony przez nabywcę na zasadzie mechanizmu odwrotnego obciążenia.

[40] T. Michalik, *How the European Commission and European countries fight VAT fraud*. mBank – „CASE Seminar Proceedings", 2017, nr 147, s. 20–28.

[41] E. Asen, *Announced, Proposed, and Implemented Digital Services Taxes in Europe,* https://taxfoundation.org/digital-taxes-europe-2019/ (dostęp: 12.08.2019).

Na wzór rozwiązań stosowanych przez kraje UE[42] także w warunkach krajowych zaplanowano wdrożenie nowych rozwiązań instytucjonalnych i systemowych. Zasadniczo sprowadzają się do ochrony podatników i wspierania w wypełnianiu obowiązków podatkowych, a także monitorowania i wykrywania nieprawidłowości, tym samym zwiększenia skuteczności i efektywności poboru podatków. Wiele inicjatyw związanych jest z nową Ordynacją podatkową[43], której generalne przeredagowanie wynikało m.in. z braku konsensualnych metod załatwiania spraw podatkowych. W celu złagodzenia rygoryzmu tej ustawy wprowadzono mechanizmy prawne chroniące pozycję podatnika, np. umowę podatkową, mediacje czy umowę o współdziałanie. Natomiast w zakresie procedur zapewniających wzrost efektywności realizacji zobowiązań podatkowych zaproponowano m.in. wprowadzenie postępowań uproszczonych, postępowań reprezentatywnych, a także upowszechnianie stosowania komunikacji elektronicznej. Przewiduje się ponadto powołanie instytucji Rzecznika Praw Podatnika[44], który co do istoty ma podejmować działania służące ochronie podatnika, aby zwiększyć poczucie bezpieczeństwa w kontaktach z organami administracji skarbowej. Podmiot ten będzie promował mediację między podatnikami a organami podatkowymi i występował jako mediator w postępowaniu podatkowym, administracyjnym i sądowo-administracyjnym. Przygotowano także projekt ustawy – Karta

[42] *Tackling tax avoidance, evasion, and other forms of non-compliance*, HM Revenue and Customs, 2019, s. 2–3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785551/tackling_tax_avoidance_evasion_and_other_forms_of_non-compliance_web.pdf (dostęp: 18.08.2019).

[43] Projektowany akt jest formą tzw. kodyfikacji częściowej prawa podatkowego, obejmującą część ogólną prawa podatkowego. Podobne akty obowiązują m.in. w Niemczech, Austrii, Włoszech, Hiszpanii, a także na Węgrzech, w Czechach, Słowacji czy Litwie. Projekt Ustawy Ordynacja podatkowa wpłynął do Sejmu 4.06.2019 r. Planowane wejście w życie 1.01.2021 r. *Ustawa Ordynacja podatkowa (projekt), Druk 3517*, 4.06.2019, http://orka.sejm.gov.pl/Druki8ka.nsf/o/B670900845B482D9C12584170033BE62/%24File/3517.pdf (dostęp: 20.08.2019).

[44] Projekt Ustawy o Rzeczniku Praw Podatnika wpłynął do Sejmu 4.06.2019. Przewiduje się, że ustawa wejdzie w życie 1 stycznia 2020 r. *Ustawa o Rzeczniku Praw Podatnika (projekt), z dnia 31.05.2019, druk 3516*, http://orka.sejm.gov.pl/Druki8ka.nsf/o/699CD4599E86A183C1258417003123B2/%24File/3516.pdf (dostęp: 15.08.2019).

Praw Podatnika[45], która stanowi katalog wyartykułowanych uprawnień i obowiązków podatników[46].

Podejmowane działania zmierzają również do uruchomienia Centralnego Rejestru Faktur[47], który będzie służyć bieżącej i zautomatyzowanej kontroli. System ten umożliwia wystawianie faktur przy pomocy certyfikowanego oprogramowania, które następnie będą przesyłane w czasie rzeczywistym na serwery organów podatkowych. Prawdopodobnie polski model Rejestru będzie pozwalał na integrację danych z faktur elektronicznych z danymi raportowanymi w plikach JPK. Takie rozwiązanie obowiązuje w Portugalii, która w 2013 r. jako pierwsza zaadoptowała Rejestr, a także w Hiszpanii (2017), w Czechach i Słowacji. W Polsce Rejestr będzie obowiązywać prawdopodobnie od 1 stycznia 2020 r.

Wśród innowacyjnych rozwiązań należy wskazać również na kasy fiskalne online z elektroniczną transmisją danych o obrotach przesyłanych do Centralnego Repozytorium Kas[48]. Przewiduje się również adoptowanie kas rejestrujących na urządzeniach mobilnych[49]. Kasy online funkcjonują w wielu krajach, takich jak Argentyna (1990), Austria, Czechy (2016), Belgia i Węgry (2014), a także Włochy (2017). W wyniku prowadzonych analiz w zakresie

---

[45] Karta Praw Podatnika ma długoletnią tradycję na świecie. Pierwsza powstała w Stanach Zjednoczonych. Do swych systemów wprowadziły ją także: Francja (1975), Wielka Brytania (1986), Niemcy (1919), a także Australia.
Komisja Europejska przygotowała zaś *Wytyczne dotyczące wzoru Kodeksu podatników Unii Europejskiej* 2016 r., https://ec.europa.eu/taxation_customs/sites/taxation/files/guidelines_for_a_model_for_a_european_taxpayers_code_pl.pdf (dostęp: 19.8.2019).

[46] Ustawa *Karta Praw Podatnika* (projekt) z dnia 25.04.2019, druk 3458, http://orka.sejm.gov.pl/Druki8ka.nsf/0/51D2C4AE6F7553ACC12583FB0033A569/%24File/3458.pdf (dostęp: 19.08.2019).

[47] Pomysł utworzenia Rejestru zrodził się w UE w 2010 r. Obecnie, system ten rekomendowany jest przez Komisję Europejską. C*entralny Rejestr Faktur w polskim wydaniu. Jaki system stworzy spółka Aplikacje Krytyczne?*, https://www2.deloitte.com/pl/pl/pages/tax/topics/taxCube/centralny-rejestr-faktur.html# (dostęp: 10.08.2019).

[48] *Implementing Online Cash Registers: Benefits, Considerations and Guidance,* OECD Publishing 2019, s. 12, www.oecd.org/tax/forum-on-tax-administration/publications-and-products/implementing-online-cash-registers-benefits-considerations-and-guidance.htm, (dostęp: 7.08.2019).

[49] Ministerstwo finansów opracowało i skierowało do konsultacji projekt rozporządzenia w tej sprawie. *Kasa fiskalna na smartfonie? Projekt trafił do konsultacji,* 16.08.2019, https://podatki.gazetaprawna.pl/artykuly/1426298,kasy-rejestrujace-smartfony-projekt-konsultacje.html (dostęp: 19.08.2019).

możliwości wykorzystania nowych technologii władze krajowe zmierzają do zastosowania technologii *Blockchain* do przechowywania i przesyłania informacji o e-handlu. To umożliwi bieżące śledzenie obrotu gospodarczego przy zachowaniu warunków bezpieczeństwa danych.

Ponadto w ramach działań wspierających uszczelnianie systemu podatkowego w latach 2017–2020 Ministerstwo Finansów wskazało na konieczność opracowania metodyki szacowania luki podatkowej w VAT oraz założeń dla pomiaru luki w podatku dochodowym płaconym przez osoby fizyczne, podatku dochodowym płaconym przez osoby prawne, a także w podatku akcyzowym. Ten słuszny kierunek jest wyrazem ogólnoświatowego trendu. Do prowadzenia szacunków w zakresie luki podatkowej kraje zachęcane są przez międzynarodowe instytucje, tj. Bank Światowy, OECD czy Międzynarodowy Fundusz Walutowy. W krajach wysoko rozwiniętych od lat wykorzystywane są bowiem narzędzia służące monitorowaniu skali niezgodnych z prawem zachowań podatników. Prawie połowa z 55 zbadanych przez OECD państw szacuje lukę podatkową. Szczególnie zaawansowane są Stany Zjednoczone i Australia. Wśród krajów Unii Europejskiej szacunki luki podatkowej prowadzą[50]:

- w podatku dochodowym płaconym przez osoby fizyczne – Estonia, Włochy, Łotwa, Wielka Brytania,
- w podatku dochodowym płaconym przez osoby prawne – Niemcy, Włochy, Wielka Brytania,
- w podatku od towarów i usług – Czechy, Estonia, Finlandia, Francja, Niemcy, Włochy, Łotwa, Polska, Portugalia, Słowacja, Słowenia i Wielka Brytania,
- dla składek ubezpieczeniowych – Estonia, Łotwa, Wielka Brytania.

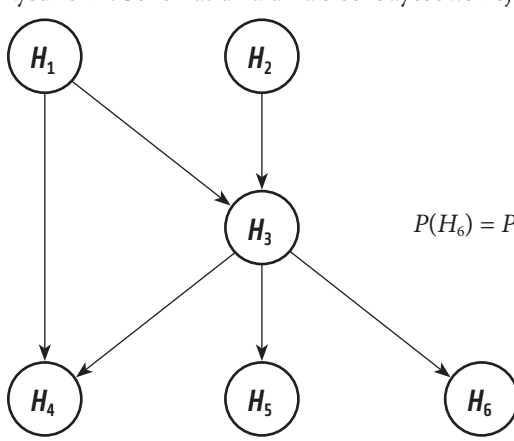
[50] *Tax Administration…*, op. cit., s. 63; R. Murphy, *The European Tax Gap. A report for the Socialists and Democrats Group in the European Parliament 2019*, https://www.socialistsanddemocrats.eu/sites/default/files/2019-01/the_european_tax_gap_en_190123.pdf, s. 8, dostęp: 5.08.2019; The concept of tax gaps. Corporate income tax gap estimation methodologies. European Commission, (FPG/041) 2016. The concept of tax gaps Report II: Corporate Income Tax Gap Estimation Methodologies, FISCALIS Tax Gap Project Group (FPG/041) 2018.

6. Rozwój narzędzi ilościowych wykorzystywanych do wykrywania przestępstw finansowych

Obecnie w instytucjach finansowych wdrażane są techniki sztucznej inteligencji i uczenia maszynowego poprawiające skuteczność rozpoznawania podejrzanych transakcji. Omówione zostaną następujące narzędzia: sieć bayesowska, analiza odstających obserwacji, ekstremalne uczenie głębokie metodą zwiększania gradientu, modelowanie probabilistyczne oraz *text-mining*.

Sieć bayesowska służy do przedstawiania zależności pomiędzy zdarzeniami, bazując na rachunku prawdopodobieństwa. Formalnie taka sieć jest modelowana za pomocą skierowanego grafu acyklicznego, w którym wierzchołki reprezentują zdarzenia, a łuki związki przyczynowe pomiędzy tymi zdarzeniami. Brakujące krawędzie mogą następnie określać, że dwie zmienne lub dwa zdarzenia są od siebie niezależne. Jeśli od wierzchołka A prowadzi ścieżka do wierzchołka B to B jest potomkiem A. Podstawowym założeniem sieci bayesowskiej jest niezależność danego zdarzenia od wszystkich innych, które nie są jego potomkami.

Rysunek 1. Schemat działania sieci bayesowskiej dla testowania układu hipotez



Źródło: J. West, M. Bhattacharya, *Intelligent financial fraud detection: a comprehensive review*, „Computers & security", 2016, nr 57, s. 47–66

Bayesowskie sieci są techniką klasyfikacji statystycznej, która wykorzystuje twierdzenie Bayesa, metodę ustalania prawdopodobieństwa, że dana hipoteza jest prawdziwa. Twierdzenie to stwierdza, że dla hipotezy H (czy obiekt X można zaklasyfikować w ramach danej klasy – np. czy dana transakcja należy do transakcji typowych czy nietypowych), prawdopodobieństwo P jest dane przez[51]:

$$P(H|X) = \frac{P(X|H) \cdot P(H)}{P(X)}$$

Sieci bayesowskie wykorzystują klasyfikator do policzenia $P(C_i|X)$ dla wszystkich możliwych klas i przypisują zdarzenie X do klasy z najwyższym prawdopodobieństwem a posteriori $P(C_i|X)$. Można więc powiedzieć w uproszczony sposób, że sieć bayesowska koduje informacje o określonej dziedzinie za pomocą wykresu, którego wierzchołki wyrażają zmienne losowe, a krawędzie obrazują probabilistyczne zależności między nimi. Wnioskowanie w danym węźle odbywa się tylko na podstawie własnego wartościowania i wiadomości uzyskanych od wszystkich sąsiadów bezpośrednich. Węzeł wysyła do drugiego węzła wiadomość będącą złożeniem wiadomości uzyskanych od wszystkich pozostałych sąsiadów i własnego wartościowania. Gdy węzeł uzyska wiadomości od wszystkich sąsiadów, wówczas na ich podstawie aktualizuje własne wartościowanie, otrzymując wartościowanie pod warunkiem zadanych obserwacji. Wykrywanie nadużyć finansowych w tym podejściu opiera się na wnioskowaniu bayesowskim. Jeśli np. rozważa się populację zleceń giełdowych w celu wyszukania anomalii wyceny, to można założyć, że rozważaną właściwością zlecenia X jest wartość zlecenia i jego charakter – np. typowe zlecenie na zakup pojedynczego pakietu instrumentów finansowych po każdej cenie. Hipotezą H jest natomiast to, że zlecenie jest poprawne. Wówczas $P(H|X)$ wyraża subiektywne przekonanie, że rozważana transakcja jest poprawna, jeśli zaobserwowano zlecenie po każdej cenie kupna pakietu akcji[52].

---

[51] E. Kirkos, C. Spathis, Y. Manolopoulos, *Data mining techniques for the detection of fraudulent financial statements*, „Expert Systems with Applications", 2007, nr 32, 995–1003.

[52] E. Ngai i in., *The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature*, „Decision Support Systems", 2011, nr 50, 559–569.

Użytecznych informacji na temat manipulacji cenami może dostarczyć też sama analiza śródddziennych wykresów notowań cenowych. Przesunięcia w poziomach szeregu czasowego, których nie da się wyjaśnić zwykłą dynamiką amplitudy wahań, można nazwać **wartościami odstającymi**. W praktyce obserwacje te są po prostu niespójne z pozostałymi danymi w szeregu. Addytywna wartość odstająca pojawia się jako zaskakująco duża lub zaskakująco mała wartość występująca dla pojedynczej obserwacji. Addytywna wartość odstająca nie ma wpływu na kolejne obserwacje. Innowacyjna wartość odstająca charakteryzuje się wpływem początkowym z efektami opóźnionymi i rozciągniętymi na kolejne obserwacje. Wpływ wartości odstających może zwiększać się w miarę upływu czasu. W przypadku przesunięcia poziomu wszystkie obserwacje za wartością odstającą przesuwają się na nowy poziom. Inaczej niż w przypadku addytywnych wartości odstających, wartość odstająca przesunięcia poziomu wpływa na wiele obserwacji, a wpływ ten jest trwały. Wartości odstające zmiany przemijającej przypominają wartości odstające przesunięcia poziomu, przy czym wpływ wartości odstającej wygasza się wykładniczo w miarę kolejnych obserwacji. Ostatecznie szereg powraca do normalnego poziomu. Wartość odstająca sezonowo addytywna pojawia się jako zaskakująco duża lub zaskakująco mała wartość występująca okresowo, w regularnych odstępach. Wartość odstająca trendu lokalnego powoduje ogólne przesunięcie w szeregu spowodowane przez wzorzec powstały w wartościach odstających po wystąpieniu początkowej wartości odstającej. Wykrywanie wartości odstających w szeregach czasowych wymaga określenia lokalizacji, typu i wartości bezwzględnej dla każdej występującej wartości odstającej. Ruey Tsay (1988) zaproponował procedurę iteracyjną wykrywania zmiany poziomu średniej z myślą o identyfikacji deterministycznych wartości odstających. Proces ten wymaga porównania modelu szeregów czasowych uznawanego za niezawierający wartości odstających z drugim modelem, w którym wartości odstające występują. Różnice między modelami stanowią oszacowanie wpływu traktowania danego punktu jako wartości odstającej.

Uczenie głębokie jest elementem metod sztucznej inteligencji związanych z uczeniem maszynowym. O ile pod pojęciem sztucznej inteligencji zwykle rozumiany jest zabieg mający na celu automatyzację procesu myślowego standardowo wykonywanego przez ludzi, o tyle uczenie maszynowe w przeciwieństwie do programowania klasycznego, gdzie człowiek wprowadza

reguły, tworząc oprogramowanie, oraz dane, które mają być przetworzone zgodnie z tymi regułami, dając rezultat wyjściowy, wymaga wprowadzenia jedynie danych na wejściu, a także oczekiwanych odpowiedzi. Komputer tworzy reguły pozwalające na przekształcenie impulsów wejściowych w wyniki końcowe. Reguły te mogą być następnie wykorzystane w celu przetworzenia nowych danych i uzyskania nowych odpowiedzi. System uczenia maszynowego podlega treningowi. Oznacza to, że nie programuje się go w sposób jawny. Przedstawia się mu jedynie wiele przykładów wyników, a system określa ich statystyczną strukturę i buduje reguły pozwalające na automatyzację procesu. Uczenie maszynowe w przeciwieństwie do wnioskowania statystycznego zwykle jest stosowane do dużych i rozbudowanych zbiorów danych. W przypadku takich zbiorów klasyczna analiza statystyczna, taka jak wnioskowanie bayesowskie, nie ma odpowiednich własności i dlatego przestaje być praktycznym rozwiązaniem.

W celu przeprowadzenia uczenia maszynowego w wykrywaniu nadużyć finansowych potrzebne są dane wejściowe, przykładowe oczekiwane wyniki oraz sposób pomiaru tego, czy algorytm działa poprawnie. Taki sposób działania zwany jest niekiedy walidacją krzyżową. Jeśli zadaniem dla uczenia maszynowego jest rozpoznawanie nadużyć w sprawozdaniach finansowych, to danymi wejściowymi są wskaźniki finansowe i dane ze sprawozdań spółek giełdowych. W przypadku wykrywania anomalii wycen rynkowych danymi wejściowymi są notowania spółek lub instrumentów na rynku finansowym zarówno regulowanym, jak i nieregulowanym. W przypadku oczekiwanych wyników można posłużyć się ręcznie wykrytymi nadużyciami w sprawozdaniach finansowych badanych przez audytorów i biegłych rewidentów. Dla określenia tego, czy algorytm działa poprawnie, konieczne jest wyznaczenie odległości między aktualnie generowanymi przez algorytm danymi wyjściowymi, a oczekiwanymi danymi wejściowymi. Model uczenia maszynowego przekształca dane wejściowe w konkretne sensowne rezultaty wyjściowe. Mówi się, że proces ten został „wyuczony" na drodze analizy znanych przykładowych danych na wejściu i wyjściu. Proces właściwego przekształcenia danych ma na celu poznanie sposobu uzyskania oczekiwanej reprezentacji danych wejściowych, czyli sposobu ich przedstawiania i kodowania. Aby lepiej zrozumieć, czym jest reprezentacja danych w przypadku wykrywania nadużyć finansowych przypuśćmy, że dane wejściowe mogą dotyczyć

wartości konkretnego wskaźnika w sprawozdaniu finansowym, np. wskaźnika ogólnego zadłużenia. Oczekiwanymi danymi wyjściowymi jest konkretna klasa wiarygodności kredytowej, a sposobem pomiaru poprawności pracy algorytmu jest np. procentowa wartość określająca liczbę poprawnie sklasyfikowanych sprawozdań. Algorytmy uczenia maszynowego zawierają mechanizmy automatycznego poszukiwania sposobu przekształcenia danych do reprezentacji, która ułatwi wykonanie konkretnego zadnia. Nie są one na tyle kreatywne, aby samodzielnie wymyślać takie transformacje, ale korzystają one ze z góry zdefiniowanego zbioru operacji określanego mianem przestrzeni hipotez. Technicznie więc uczenie maszynowego sprowadza się do poszukiwania właściwej reprezentacji danych na podstawie sygnału informacji zwrotnej w ramach zdefiniowanej przestrzeni możliwości.

Uczenie głębokie nie odwołuje się do lepszego zrozumienia osiąganego przez tę technikę, ale do tworzenia warstwowej reprezentacji danych. Głębokością modelu jest po prostu liczba warstw. Warstwowe reprezentacje tworzone są za pomocą sieci neuronowych. Sieć neuronowa przekształca dane wejściowe na reprezentacje, które coraz bardziej odbiegają od początkowego zbioru, a coraz bardziej są zbliżone do wyjściowego zbioru wyników. Jest to zatem swoista hierarchiczna destylacja informacji, podczas której dane przechodzą przez kolejne filtry i stają się coraz bardziej czyste. Takim filtrem może być w szczególności dla szeregów notowań cen aktywów model ARIMA(p,d.q) i następnie model z klasy GARCH(m,n). Każda kolejna reprezentacja ma w strukturze algorytmu pewną określoną wagę. W celu określenia działania modelu wyznacza się funkcję straty sieci zwaną też funkcją celu. Funkcja straty przyjmuje argumenty w postaci przewidywanych wartości generowanych przez sieć i prawdziwych docelowych wartości. Najważniejszym elementem uczenia głębokiego jest użycie wyniku jako informacji zwrotnej umożliwiającej dostrojenie wag w drodze wykorzystania optymalizacji metodą propagacji wstecznej.

Przykładem dla zastosowania metod uczenia głębokiego jest wykrywanie umów typu piramida finansowa za pomocą ulepszonego wzmocnienia drzewa gradientowego, która pozwala analizować zbiór N umów finansowych określanych przez x cech i przypisanych do y grup na podstawie regularyzacji funkcji celu i przycinania, aby uniknąć nadmiernego dopasowania. W przeciwieństwie do tradycyjnego modelu klasyfikacji, który zwraca bezpośrednio

etykiecie klasy, szkoli się model regresji logistycznej do klasyfikacji binarnej, który generuje prawdopodobieństwo. Każdy kontrakt o przewidywanym prawdopodobieństwie większym niż 0,5 jest uważany za piramidę finansową.

Modelowanie probabilistyczne i text-mining polega na zastosowaniu zasad statystyki w analizie danych. Jednym z najbardziej znanych algorytmów jest naiwny klasyfikator bayesowski. Zadaniem klasyfikatora Bayesa jest przyporządkowanie nowego przypadku do jednej z klas, przy czym ich zbiór musi być skończony i zdefiniowany a priori. Każdy przykład uczący opisany jest przy pomocy zbioru atrybutów warunkowych $\{A_i\}$ i jednego atrybutu decyzyjnego D. W odróżnieniu od wielu innych technik uczenia maszynowego, tutaj nie zakłada się, że każdy przykład opisany jest przy pomocy takiego samego zbioru atrybutów warunkowych (z drugiej strony, aby zachować spójność z innymi podejściami, można przyjąć interpretację, że zbiór atrybutów warunkowych jest stały dla wszystkich przykładów, natomiast poszczególne przykłady mogą zawierać wartości brakujące, które nie są brane pod uwagę zarówno podczas uczenia, jak i podczas klasyfikacji). W myśl teorii Bayesa, najbardziej prawdopodobną klasą, do której należy przypisać nowy obiekt, opisany wartościami n-atrybutów warunkowych $A_{j1} = v_{j1}, A_{j2} = v_{j2} \ldots A_{jn} = v_{jn}$ (lub w skrócie $<v_{j1}, v_{j2} \ldots v_{jn}>$), jest klasa d_i, która maksymalizuje prawdopodobieństwo warunkowe $P(d_i \mid v_{j1}, v_{j2} \ldots v_{jn})$.

Każdy dokument tekstowy, np. sprawozdanie finansowe, opisany jest przy pomocy zbioru atrybutów warunkowych $\{A_i\}$. Atrybut A_i oznacza i-tą pozycję słowa w dokumencie (np. przy założeniu, że ten akapit stanowi oddzielny dokument, atrybut A_1 oznacza pierwszy wyraz w akapicie, a jego wartość wynosi 'każdy'). Należy zauważyć, że liczba atrybutów warunkowych (oznaczająca długością tekstu) może być zmienna. Każdy przykład (dokument) uczący opisany jest również przy pomocy wartości atrybutu decyzyjnego. Zbiór klas decyzyjnych jest zależny od zastosowania – może on zawierać oceny tekstu (np. *dobry, zły* …).

Nowy dokument, zawierający n słów, z których pierwsze – A_1 to w_{A1}, drugie $A_2 = w_{A2}$, … ostatnie $A_n = w_{An}$, przyporządkowywany jest do klasy d_{NB}, wyznaczonej jako:

$$d_{NB} = \arg\max_{d_i \in V_D} p(d_i) \prod_{j=1}^{n} p(w_{Aj}|d_i)$$

Bibliografia

Analysis of the impact of the split payment mechanism as an alternative VAT collection method, Final Report, Publications Office of the European Union 2017.

Arak P. i in., *Krótka historia VAT w Polsce*, Polski Instytut Ekonomiczny, „Policy Paper", 2019, nr 3, s. 23.

Asen E., *Announced, Proposed, and Implemented Digital Services Taxes in Europe*, https://taxfoundation.org/digital-taxes-europe-2019/

Berger A., *Kogo dotyczy ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu*, „Rzeczpospolita", 18.05.2018. https://www.rp.pl/Firma/305189982-Kogo-dotyczy-ustawa-o-przeciwdzialaniu-praniu-pieniedzy-i-finansowaniu-terroryzmu.html (dostęp: 1.09.2019).

Centralny Rejestr Faktur w polskim wydaniu. Jaki system stworzy spółka Aplikacje Krytyczne?, https://www2.deloitte.com/pl/pl/pages/tax/topics/taxCube/centralny-rejestr-faktur.html#

Cichy Ł., *Funkcja compliance w bankach*, KNF, Warszawa 2015.

Cichy Ł., *Whistleblowing w bankach*, KNF, Warszawa 2017.

Decyzja wykonawcza Rady (UE) 2019/310 z dnia 18 lutego 2019 r. upoważniająca Polskę do wprowadzenia szczególnego środka stanowiącego odstępstwo od art. 226 dyrektywy 2006/112/WE w sprawie wspólnego systemu podatku od wartości dodanej (Dz. Urz. UE L 51/19).

Dyrektywa Komisji 2006/70/WE z dnia 1 sierpnia 2006 r. ustanawiająca środki wykonawcze do dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady w odniesieniu do definicji osoby zajmującej eksponowane stanowisko polityczne, jak również w odniesieniu do technicznych kryteriów stosowania uproszczonych zasad należytej staranności wobec klienta oraz wyłączenia z uwagi na działalność finansową prowadzoną w sposób sporadyczny lub w bardzo ograniczonym zakresie.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

Działania zwiększające stopień przestrzegania przepisów podatkowych i poprawiające efektywność administracji podatkowej w latach 2014–2017. Ministerstwo Finansów, http://www.kic.gov.pl/documents/764034/1002171/Monitoring

European Commission – Press Release, *VAT: More flexibility on VAT rates, less rade tape for small businesses*, Brussels, 18 January 2018, http://europa.eu/rapid/press-release_IP-18-185_en.htm (dostęp: 16.05.2018).

Guidance for the Standard Audit File – Tax, https://www.oecd.org/tax/administration/45167181.pdf

Implementing Online Cash Registers: Benefits, Considerations and Guidance, OECD, 2019, Paris, www.oecd.org/tax/forum-on-tax-administration/publications-and-products/implementing-online-cash-registers-benefits-considerations-and-guidance.htms.12

Julia D., *Słownik filozofii*, Katowice 1992.

Kasa fiskalna na smartfonie? Projekt trafił do konsultacji, https://podatki.gazetaprawna.pl/artykuly/1426298,kasy-rejestrujace-smartfony-projekt-konsultacje.html

Łączne wytyczne określone artykułami 17 i 18(4) Dyrektywy (EU)2015/849 o uproszczonym i rozszerzonym badaniu due dilligence oraz czynnikami, jakie instytucje finansowe i kredytowe powinny rozważyć kiedy oceniają ryzyko prania pieniędzy i finansowania terroryzmu związane ze związkami biznesowymi i okazjonalnymi transakcjami, https://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf.

Leeuw J., *Monitoring & Surveillance*, "About financial crime, prevention of market abuse and detecting suspicious trading behavior", Entrima, document elektroniczny, 2019.

Majewski K., *Funkcjonowanie w banku procedury anonimowego zgłaszania naruszeń*, „Monitor Prawa Bankowego", 2018, nr 12.

Michalik, *How the European Commission and European countries fight VAT fraud*, "mBank – CASE Seminar Proceedings", 2017, nr 147, s. 20–28.

Murphy R., *The European Tax Gap. A report for the Socialists and Democrats Group in the European Parliament 2019*, https://www.socialistsanddemocrats.eu/sites/default/files/2019-01/the_european_tax_gap_en_190123.pdf, s. 8, dostęp: 5.08.2019

Olszak M., Jurkowska-Zeidler A., *Wprowadzenie*, *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, https://sip.lex.pl/#/monograph/369380982/3

Płońska A., *Karnoprawna ochrona informacji na rynku kapitałowym*, Wrocław 2012.

Regulacja UE No 543/2013 on submission and publication of data in electricity markets.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 roku w sprawie nadużyć na rynku.

Rozporządzenie Parlamentu Europejskiego i Rady nr 1227/2011 z 25 października 2011 r. w sprawie integralności i przejrzystości hurtowego rynku energii).

Rozporządzenie Rady (UE) 967/2012 z dnia 9 października 2012 r. zmieniające rozporządzenie wykonawcze (UE) nr 282/2011 w odniesieniu do procedur szczególnych dotyczących podatników niemających siedziby, którzy świadczą usługi telekomunikacyjne, usługi nadawcze lub usługi elektroniczne na rzecz osób niebędących podatnikami (Dz. Urz. UE L 290 z 20.10.2012)

Rozporządzenie wykonawcze Rady (UE) 1042/2013 z dnia 7 października 2013 r. zmieniające rozporządzenie wykonawcze (UE) nr 282/2011 w odniesieniu do miejsca świadczenia (Dz. Urz. UE L 284 z 26.10.2013).

Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015.

Strategia Zarządzania Ryzykiem Zewnętrznym. Polska Administracja Podatkowa, Ministerstwo Finansów 2004.

Tackling tax avoidance, evasion, and other forms of non-compliance, HM Revenue and Customs, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785551/tackling_tax_avoidance_evasion_and_other_forms_of_non-compliance_web.pdf (dostęp: 18.08.2019).

Tax Administration 2017: Comparative Information on OECD and Other Advanced and Emerging Economies, OECD Publishing 2017, http://dx.doi.org/10.1787/tax_admin-2017-en

The Concept of Tax Gaps. Corporate Income Tax Gap Estimation Methodologies, European Commission, Taxation Papers, „Working Paper" 2018.

Tokarczyk R., *Etyka prawnicza*, Warszawa 2006.

Urząd Komisji Nadzoru Finansowego, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy i Finansowania Terroryzmu oraz Proliferacji*, Warszawa [b.r.].

Ustawa Karta Praw Podatnika (projekt) z dnia 25.04.2019, druk 3458, http://orka.sejm.gov.pl/Druki8ka.nsf/o/51D2C4AE6F7553ACC12583FB0033A569/%24File/3458.pdf

Ustawa o Rzeczniku Praw Podatnika (projekt) z dnia 31.05.2019, druk 3516, http://orka.sejm.gov.pl/Druki8ka.nsf/o/699CD4599E86A183C1258417003123B2/%24File/3516.pdf

Ustawa Ordynacja podatkowa (projekt) z dnia 4.06.2019, druk 3517, http://orka.sejm.gov.pl/Druki8ka.nsf/o/B670900845B482D9C12584170033BE62/%24File/3517.pdf

Ustawa z dnia 10 maja 2018 roku ochronie danych osobowych (Dz.U. 2018 poz 1000).

Ustawa z dnia 24 listopada 2017 r. o zmianie niektórych ustaw w celu przeciwdziałania wykorzystywaniu sektora finansowego do wyłudzeń skarbowych (Dz.U. 2017 poz. 2491 z późn. zm.).

VAT on digital services (MOSS scheme), https://europa.eu/youreurope/business/taxation/vat/vat-digital-services-moss-scheme/index_en.htm

West J., Bhattacharya M., *Intelligent financial fraud detection: a comprehensive review*. „Computers & security", 2016, nr 57, s. 47–66.

Wielec M., *Wartości – analiza z perspektywy osobliwości postępowania karnego*, Lublin 2017.

Wolfsberg Group, *Guidance on a Risk Based Approach for Managing Money Laundering Risks*, 2006, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf (dostęp: 20.08.2019).

Working smarter in structuring the administration, in compliance, and through legislation, Information note, OECD Publishing 2012.
Wytyczne dotyczące wzoru Kodeksu podatników Unii Europejskiej, https://ec.europa.eu/taxation_customs/sites/taxation/files/guidelines_for_a_model_for_a_european_taxpayers_code_pl.pdf

ROZDZIAŁ III

Bezpieczeństwo informacji i bezpieczeństwo energetyczne na przykładzie przestępstw przeciwko ochronie informacji

REMIGIUSZ ROSICKI[1]

1. Wprowadzenie

Zakres przedmiotowy analizy w tekście obejmuje wybrane aspekty bezpieczeństwa informacji i bezpieczeństwa energetycznego na przykładzie przestępstw przeciwko ochronie informacji, które potocznie określane są mianem cyberterroryzmu. Analiza skupia się na problematyce karnomaterialnej przestępstw sabotażu komputerowego (spenalizowanej w art. 269 k.k.) i zakłóceniach pracy w sieci (spenalizowanych w art. 269a k.k.) w kontekście energetyki[2]. Głównym celem tekstu jest prezentacja wybranych rozwiązań w zakresie przestępstwa sabotażu i sabotażu komputerowego w polskim prawie karnym. W zaprezentowanej analizie wykorzystano interpretację doktrynalną, historyczną i funkcjonalną przepisów dotyczących tej problematyki. Punktem wyjścia jest szersza interpretacja przestępstwa sabotażu w kontekście historycznych zmian znaczenia tego terminu i kategorii prawnej. W dalszej kolejności w interpretacji sensu tego typu przestępstw sięgnięto do rozwiązań historycznych w polskim prawie karnym. Z kolei przestępstwo

[1] Doktor habilitowany w zakresie nauk politycznych i administracji, jest prawnikiem, politologiem i filozofem. Ukończył również studia podyplomowe w zakresie: prawa gospodarczego (na Uniwersytecie Ekonomicznym w Poznaniu), administracji europejskiej (na Uniwersytecie im. Adama Mickiewicza w Poznaniu), odnawialnych źródeł energii (w Wyższej Szkole Bankowej w Poznaniu). Kształcił się również w Södertörns Högskola w Sztokholmie (Szwecja). Jego zainteresowania badawcze skupiają się na polityce bezpieczeństwa, polityce kryminalnej, polityce prawa, prawie energetycznym, polityce energetycznej i gospodarce energetycznej (remigiusz.rosicki@amu.edu.pl); ORCID: https://orcid.org/0000-0002-1187-5895

[2] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 Nr 88 poz. 553 ze zm.)*; dalej: k.k.

sabotażu komputerowego i zakłócania pracy w sieci, spenalizowane w aktualnych przepisach karnych, rozważano z punktu widzenia doktrynalnego i funkcjonalnego z uwzględnieniem kontekstu bezpieczeństwa energetycznego państwa.

W celu uszczegółowienia zakresu przedmiotowego problemu badawczego w tekście przedstawiono następujące pytania badawcze: 1) Jakie powinny być kierunki zmian w zakresie penalizacji czynów określanych mianem sabotażu komputerowego (informatycznego) w ramach polityki karnej?; 2) Jaki wpływ na zmiany w zakresie penalizacji czynów określanych mianem sabotażu komputerowego (informatycznego) powinny mieć zagrożenia w zakresie bezpieczeństwa energetycznego?

W analizie wykorzystano historyczne i aktualne akty prawne, np. Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. – Kodeks karny, Dekret z dnia 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy państwa, ustawę z dnia 19 kwietnia 1969 r. – Przepisy wprowadzające Kodeks karny i ustawę z dnia 6 czerwca 1997 r. – Kodeks karny. Ponadto w celu uzupełnienia interpretacji językowej przepisów wykorzystano szereg publikacji stanowiących komentarze do wybranych historycznych i aktualnych zapisów prawa karnego. Z kolei do analizy terminologii i znaczenia sabotażu wykorzystano historyczne słowniki języka francuskiego (Ch.-L. D'Hautel, G.A.J. Hécart i É. Littré), tekst É. Pougeta pt. *Le Sabotage* z 1911 roku, a także monografię L. Faragó pt. *Wojna mózgów. Anatomia szpiegostwa i wywiadu* z 1961 roku.

2. Zagadnienia wprowadzające

2.1. Bezpieczeństwo informacji

Bezpieczeństwo informacji można rozpatrywać w kontekście nauk społecznych i humanistycznych, ale również jako kategorię prawną, tj. jako element (przedmiot) przestępstwa[3]. W pierwszym przypadku bezpieczeństwo

[3] L. Gardocki, *Prawo karne*, Warszawa 2002, s. 83–88; J.W. Giezek, *Przedmiot prawnokarnej ochrony*, w: M. Bojarski (red.), *Prawo karne materialne. Część ogólna i szczególna*, Warszawa 2017, s. 101–107; T. Dukiet-Nagórska (red.), *Prawo karne. Część ogólna, szczególna*

informacji będzie ujęciem przedmiotowym szerokiej problematyki bezpieczeństwa, czyli jednym z jej zakresów[4], natomiast w drugim przypadku należałoby je rozpatrywać jako dobro prawne, w które godzi sprawca przestępstwa. Z punktu widzenia rozpatrywania informacji jako dobra chronionego właściwy jest rozdział XXXIII k.k. z 1997 roku pt. *Przestępstwa przeciwko ochronie informacji*. Penalizuje on czyny przeciwko tajemnicy państwowej i służbowej, nielegalnego uzyskania informacji, niszczenia informacji, wyrządzenia szkody na bazach danych, sabotażu komputerowego, zakłócania pracy sieci, bezprawnego wykorzystania programów i danych. Część tych przepisów przyjęło się określać mianem przestępstw cyberterrorystycznych i to niezależenie od funkcjonowania w k.k. definicji przestępstwa o charakterze terrorystycznym.

W tekście szczególną uwagę skupiono na przestępstwach sabotażu komputerowego (informatycznego) i zakłócania pracy w sieci jako przykładów przestępstw przeciwko ochronie informacji. Jakkolwiek trzeba pamiętać, że szersze rozumienie bezpieczeństwa informacji, wychodzące poza kryteria prawnokarnej oceny przedmiotu przestępstwa, każe uznawać inne kategorie przestępstw za powiązane. Przykładem może być przestępstwo szpiegostwa, które w polskich przepisach karnych zaliczane jest do przestępstw przeciwko państwu. Przedmiot ochrony w tej grupie przestępstw związany jest m.in. z obronnością i bezpieczeństwem państwa, a więc dobrami pobocznymi chronionymi przez przepis penalizujący czyny sabotażu komputerowego.

Niezależnie od analizy dokonanej w tekście warto w tym miejscu zwrócić uwagę na konieczność przemyślenia rozwiązań kodeksowych w zakresie przestępstw przeciwko ochronie informacji i przeciwko państwu. Uwaga ta dotyczy zarówno jasności stosowania przepisów, jak i systemowych rozwiązań, które dałyby możliwość efektywnego zwalczania zagrożeń bezpieczeństwa informacji, szczególnie w kontekście ciągłego rozwoju technologicznego i zagrożeń zewnętrznych państwa.

---

i wojskowa, Warszawa 2018, s. 109–111; Ł. Pohl, *Prawo karne. Wykład części ogólnej*, Warszawa 2019, s. 180–184.

[4] R. Rosicki, *O pojęciu i istocie bezpieczeństwa*, „Przegląd Politologiczny", 2010, nr 3, s. 24–32.

2.2. Bezpieczeństwo energetyczne

Należy zauważyć, że kategoria bezpieczeństwa energetycznego mimo prezentowania wielu definicji nie jest w sposób jednoznaczny rozgraniczona od innych jej podobnych. Przykładem może być zamienne stosowanie kategorii polityki energetycznej i bezpieczeństwa energetycznego, czego skutkiem jest używanie w analizie tożsamych cech mających je charakteryzować lub wskaźników, których wartości mają służyć ich ocenie. W przypadku badań ilościowych nad bezpieczeństwem energetycznym stosuje się wiele definicji operacyjnych tej kategorii. W tego typu ujęciach kategorii bezpieczeństwa energetycznego przypisuje się określone cechy wraz z reprezentującymi je wskaźnikami, czego skutkiem mogą być różne skale bezpieczeństwa energetycznego i ich oceny[5].

Z kolei w polskiej ustawie – Prawo energetyczne ustawodawca uznał za właściwe wprowadzić definicję legalną bezpieczeństwa energetycznego, zgodnie z którą jest to „stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska"[6]. Definicja ta jest tożsama z definicjami bezpieczeństwa energetycznego, jakie prezentowane są w dokumentacji Unii Europejskiej[7]. Obok definicji bezpieczeństwa energetycznego ustawodawca wprowadził w ustawie – Prawo energetyczne definicje legalne dwóch innych terminów – bezpieczeństwa dostaw energii elektrycznej i bezpieczeństwa pracy sieci elektroenergetycznej. O ile definicja bezpieczeństwa energetycznego kładzie nacisk na bezpieczeństwo dostaw w perspektywie całego systemu gospodarczego, o tyle definicja bezpieczeństwa dostaw energii elektrycznej skupia się na systemie elektroenergetycznym, a więc na aspekcie infrastrukturalnym. Natomiast definicja bezpieczeństwa pracy sieci elektroenergetycznej dotyczy

[5] Por. R. Rosicki, *Kultury energetyczne Unii Europejskiej*, Poznań 2018, s. 230–232.

[6] *Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 1997 Nr 54 poz. 348 ze zm.).*

[7] K. Kałążna, R. Rosicki, *Wymiary bezpieczeństwa energetycznego Unii Europejskiej*, Poznań 2010, s. 14–29, 129–164; R. Rosicki, *Pojęcie i definicje bezpieczeństwa energetycznego*, w: T.Z. Leszczyński (red.), *Bezpieczeństwo energetyczne Polski w Unii Europejskiej – wizja czy rzeczywistość?*, Warszawa 2012, s. 35–65.

stabilnej pracy systemu i spełniania standardów jakościowych dostarczanej energii elektrycznej[8].

Syntetyczne ujęcie kategorii bezpieczeństwa energetycznego przedstawili Aleh Cherp i Jessica Jewell m.in. w tekście pt. *The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration*. Wedle autorów do trzech głównych perspektyw badawczych bezpieczeństwa energetycznego należy zaliczyć dorobek związany z naukami politycznymi, przyrodniczymi i technicznymi oraz ekonomicznymi. Każdej z dyscyplin A. Cherp i J. Jewell przypisali swoiste paradygmaty badań nad bezpieczeństwem energetycznym. W przypadku szeroko rozumianych nauk politycznych paradygmatem badawczym jest suwerenność. Z kolei w przypadku nauk przyrodniczych i technicznych jest nim pewność i stabilność dostaw energii z punktu widzenia technicznego, ale i z perspektywy dostępu do zasobów surowców energetycznych. Natomiast w ostatnim przypadku, tj. nauk ekonomicznych, paradygmatem jest głównie elastyczność i odporność na kryzysy rynków energetycznych. Każdej z trzech wymienionych perspektyw badawczych można przypisać punkty historyczne stanowiące początek rozważań na temat szczególnego ujęcia bezpieczeństwa energetycznego w poszczególnych dyscyplinach. Będą to zatem: kryzys naftowy w latach 70. XX w. (suwerenność), naruszenia infrastruktury energetycznej, awarie zasilania i zmniejszające się zasoby surowców (pewność i stabilność dostaw energii oraz dostęp do zasobów), liberalizacja rynków energii (elastyczność i odporność systemów energetycznych)[9]. Niezależnie od perspektywy badawczej głównym elementem bezpieczeństwa energetycznego jest bezpieczeństwo dostaw energii elektrycznej i surowców, które można rozpatrywać z punktu widzenia fizycznych dostaw z określonych kierunków i źródeł, a także pod względem ich technicznej i ekonomicznej pewności oraz stabilności.

---

[8] *Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 1997 Nr 54 poz. 348 ze zm.)*.

[9] A. Cherp, J. Jewell, *The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration*, „Current Opinion in Environmental Sustainability", 2011, wol. 3, nr 4, s. 202–212.

3. Sabotaż i dywersja

Interesującą kwestią jest samo pojęcie sabotażu, w słownikowym i powszechnym rozumieniu ma ono bowiem przynajmniej dwa znaczenia. W pierwszym oznacza zaplanowaną dezorganizację czynności przez odstąpienie lub uchylenie się od ich wykonywania. W tym sensie sabotaż może też polegać na wadliwym wykonywaniu czynności. Natomiast w drugim znaczeniu oznacza on nieformalne i ukryte czynności, które mają na celu udaremnienie realizacji jakichś planów[10].

Dyskusyjne jest wskazywanie na pochodzenie samego słowa „sabotaż" od francuskich butów sabotów (czyli prostego drewnianego obuwia – chodaków). Wynika to z faktu, że za symbol akcji sabotażu podawano w literaturze wkładanie przez robotników sabotów do maszyn w fabrykach. Zatrzymanie pracy maszyn fabrycznych za pomocą butów stanowiło część strajku robotniczego. Tę błędną interpretację powiela wiele specjalistycznych publikacji. O tej konotacji terminu „sabotaż" wspomina m.in. Ladislas Faragó w swojej książce pt. *Wojna mózgów. Anatomia szpiegostwa i wywiadu*, mimo wszystko autor ten zwraca uwagę na przekształcenie znaczenia terminu. Warto jednak podkreślić, że saboty wykorzystywane były po prostu do zatrzymywania maszyn w sytuacji wystąpienia wypadku podczas pracy. W literaturze wskazuje się na bardziej prawdopodobne pochodzenie sensu słowa „sabotaż", które utożsamia się nie tyle z samymi drewnianymi butami, lecz ze sposobem chodzenia w nich – chodzeniem głośno. Tak mieli chodzić robotnicy, którzy przerywali swoją pracę, by strajkować. Wskazuje się więc, że zanim termin „sabotaż" oznaczał złośliwe niszczenie maszyn fabrycznych, używano go w kontekście wystąpienia sporu pracowniczego w ogóle[11]. W słowniku Émile'a Littrégo z 1873 r. termin „sabotaż" definiowany jest m.in. jako właśnie robienie hałasu albo robienie czegoś szybko i źle (w tym drugim przypadku podobnie do słowa *abloquer* ze słownika G.A.J. Hécarta z 1834 r.)[12].

---

[10] Por. E. Sobol (red.), *Słownik wyrazów obcych*, Warszawa 1995, s. 986.

[11] Ch.-L. D'Hautel, *Dictionnaire du bas-langage, ou, Des manières de parler usitées parmi le peuple*, Paris 1808, s. 325; L. Faragó, *Wojna mózgów. Anatomia szpiegostwa i wywiadu*, Warszawa 1961.

[12] G.A.J. Hécart, *Dictionnaire rouchi-français*, Paris 1834, s. 13; É. Littré, *Dictionnaire de la langue française: Tome 4*, Paris 1873, s. 1790.

Szczególnego rodzaju znaczenia termin „sabotaż" nabrał w odniesieniu do stosunków przemysłowych w okresie rozwoju kapitalizmu na przełomie XIX i XX w.[13] Abstrahując od etymologii tego terminu, należy zwrócić uwagę na okres początku drugiej dekady XIX w. w Anglii. Wtedy to rozwinął się ruch luddystyczny, którego jednym z celów było niszczenie maszyn tkackich jako forma walki o prawa robotnicze[14]. Skutkiem tych działań było wprowadzenie w Anglii w 1812 r. ustawy *Destruction of Stocking Frames*, określającej niszczenie krosien tkackich jako zbrodnię główną, za którą można było karać śmiercią[15]. Pokazuje to, w jaki sposób czynniki społeczne i polityczne wpływały i nadal wpływają na stosunek do przestępstw określanych mianem sabotażu. W dalszej kolejności sabotaż stał się częścią taktyki działań pracowniczych m.in. dzięki ruchom anarchistycznym i socjalistycznym. Wyrazem tego jest praktyka i teksty polityczne anarchistów, syndykalistów i socjalistów. Na przykład w 1898 r. francuski anarchista i syndykalista Émile Pouget pisze tekst pt. *Le Sabotage* (w późniejszym czasie opublikuje szerszy tekst o tym samym tytule), w którym przedstawia sabotaż jako instrument walki z wyzyskiem klasowym. Według É. Pougeta nie wystarczy, że strajkują ludzie – wraz z nimi mają strajkować narzędzia pracy, tylko to daje gwarancję skutecznego sabotażu. Co ciekawe, jednym z wielu przykładów, jakich użył É. Pouget w rozbudowanej wersji tekstu, był sektor elektroenergetyczny. Zwrócił on uwagę, że państwo stało się skuteczne w przeciwdziałaniu sabotażu w sektorze elektroenergetycznym ze względu na szybkie zastępowanie strajkujących wyszkolonymi technicznie w tej dziedzinie żołnierzami. Dlatego też sabotaż

[13] W swoim komentarzu do przepisów karnych M. Lityński pisze na temat działań robotników: „we Francji sabotaż przejawiał się w postaci przyśpieszonej, lecz niewydajnej pracy, we Włoszech w postaci pracy zwolnionej lub przeszkadzania w pracy (tzw. strajk włoski), wreszcie w Anglii przybierał formę skrupulatnego przestrzegania przestarzałych i drobiazgowych przepisów (*working to rule*), co w konsekwencji opóźniało działalność zakładów" (za: M. Lityński, *Przestępstwa przeciwko państwu ludowemu*, Łódź 1960, s. 74–121).

[14] F. Hozumi, *Some Notes on the Luddites*, „Kyoto University Economic Review", 1956, wol. 26, nr 2, s. 10–38; M.I. Thomis, *The Luddites: machine-breaking in regency England*, Newton Abbot 1970; K. Navickas, *The search for 'General Ludd': the mythology of Luddism*, „Social History", 2005, wol. 30, nr 3, s. 281–295.

[15] *Destruction of Stocking Frames, etc. Act 1812* (52 Geo 3 c. 16).

techniczny, np. infrastruktury energetycznej, powinien występować równolegle do prowadzonego strajku[16].

Niewątpliwie termin „sabotaż" stosowany jest dla oddania charakteru dwóch rodzajów czynności ludzkich – szczególnego rodzaju postępowania człowieka i niszczenia elementów infrastruktury. Znajduje to swoje odzwierciedlenie w historycznych już rozwiązaniach dotyczących penalizacji w polskim prawie karnym czynów określanych jako akty sabotażu. Przepisy określające odpowiedzialność karną za przestępstwo sabotażu i dywersji przewidywał zarówno dekret z 13 czerwca 1946 r. (tzw. mały kodeks karny), jak i przepisy wprowadzające nowy Kodeks karny z 1969 r.[17]

W przypadku dekretu z 1946 r. ustawodawca wprost posłużył się terminem sabotażu jako znamieniem czynu zabronionego (art. 3 dekretu). Dopuszczenie się aktów sabotażu przyjęło trzy główne formy[18]. Pierwsza to niszczenie lub czynienie niezdatnym do użytku zakładów i urządzeń (użyteczności

[16] É. Pouget, *Le Sabotage*, „Almanach du Père Peinard", 1898, s. 28–31; É. Pouget, *Le Sabotage*, Paris 1911, s. 3–66.

[17] *Dekret z dnia 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy państwa (Dz.U. 1946 Nr 30 poz. 192); ustawa z dnia 19 kwietnia 1969 r. Przepisy wprowadzające Kodeks karny (Dz.U. 1969 Nr 13 poz. 95).*

[18] Główna idea zakresu penalizacji sabotażu pochodzi z k.k. przyjętego w 1932 r. (jakkolwiek trzeba uwzględnić też wpływ ustawodawstwa ZSRR). W art. 217 tego k.k. spenalizowano przestępstwo uszkodzenia urządzeń użyteczności publicznej, a w art. 223 i 224 przestępstwa przeciwko urządzeniom użyteczności publicznej. Przepisy te znalazły się w dwóch odrębnych rozdziałach k.k. – art. 217 w rozdziale pt. *Sprowadzenie niebezpieczeństwa powszechnego*, a art. 223 i 224 w rozdziale pt. *Przestępstwa przeciwko urządzeniom użyteczności publicznej*. W tym miejscu warto zaznaczyć, że przepisem, który bezpośrednio dotyczył utrudniania dostępu do urządzeń dostarczających światło, ciepło lub energię, był art. 224. W sytuacji, gdy do wprowadzenia k.k. w 1969 r. obowiązywały przepisy k.k. z 1932 r. i dekretu z 1946 r., występowały dwie różne formy sabotażu – pierwszy o charakterze antypaństwowym czy „kontrrewolucyjnym" (art. 3 dekretu z 1946 roku) i bez tej przesłanki (art. 223 i 224 k.k. z 1932 roku). Mimo wszystko brak znamienia celowości działania antypaństwowego (kontrrewolucyjnego) w art. 3 dekretu z 1946 r. powodował, że i tak stanowił on przepis nadrzędny. Problemem było również to, że część doktryny nie odróżniała sabotażu politycznego od gospodarczego w ramach art. 3 dekretu z 1946 r., skutkiem czego było uznanie, że przestępstwo to można było popełnić z zamiarem bezpośrednim i ewentualnym, a pobudki tych działań były obojętne. Zob. szerzej: *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. – Kodeks karny (Dz.U. 1932 Nr 60 poz. 571)*; M. Siewierski, *Mały kodeks karny i postępowanie doraźne wraz z przepisami o Komisji Specjalnej do walki z nadużyciami i innymi dodatkowymi. Komentarz*, Łódź 1947, s. 29–32; J. Fajnberg, M. Leonieni (oprac.), *Kodeks karny z orzecznictwem okresu powojennego*, Łódź 1958; M. Siewierski, *Kodeks karny i prawo o wykroczeniach. Komentarz*, Warszawa 1958; M. Lityński, *Przestępstwa przeciwko państwu ludowemu…*, op. cit., s. 97–110.

publicznej, komunikacji publicznej, a także służących obronie państwa lub państwa sprzymierzonego). Druga forma sabotażu to uniemożliwienie lub utrudnienie prawidłowego działania zakładów lub urządzeń, które doprecyzowano w przypadku pierwszej formy. O ile w pierwszym przypadku położono nacisk na fizyczną ingerencję, o tyle w drugim ingerencja nie przybiera postaci fizycznego zniszczenia lub uszkodzenia. Z kolei trzecią formą przestępstwa sabotażu jest wytwarzanie wbrew warunkom umówionej dostawy dla wojska przedmiotów zupełnie lub w znacznym stopniu niezdatnych do użytku. Widać więc wyraźnie, że o ile w dwóch pierwszych przypadkach przestępstwa ukierunkowane są na szeroko rozumianą infrastrukturę użyteczności publicznej, o tyle trzeci przypadek wiąże się ze sferą działalności wojska. Ustawodawca nie wskazał przy tym, o jakie przedmioty chodzi, podkreślił jedynie, że stanowią one dostawy dla wojska, co powoduje, że przedmioty te nie muszą mieć bezpośredniego związku z ewentualnym prowadzeniem działań wojennych. Cechą charakterystyczną dekretu z 1946 r. jest jego duży stopień represyjności, co wyraża się np. w wysokich karach za omawiane przestępstwo sabotażu, ustawodawca przewidział za nie bowiem karę pozbawienia wolności na czas nie krótszy niż 3 lata, karę dożywotniego pozbawienia wolności lub karę śmierci[19].

Przepisy wprowadzające nowy Kodeks karny z 1969 r. zachowały ogólną strukturę przestępstwa sabotażu, jednakże ustawodawca nie użył wcześniejszego znamienia „dopuszcza się aktów sabotażu". W pewnym sensie zawęził stosowanie poprzednich przepisów karnych, wskazał bowiem na zamiar bezpośredni kierunkowy sprawcy. W nowej wersji przepisów niszczenie, uszkadzanie lub czynienie niezdatnym albo uniemożliwienie lub utrudnienie prawidłowego funkcjonowania określonej infrastruktury musi mieć cel w postaci chęci osłabienia władzy, wywołania zaburzeń lub nastrojów powszechnego niezadowolenia albo poważnych zakłóceń w funkcjonowaniu gospodarki narodowej. Nowy zapis miał na celu odróżnienie jakiegokolwiek sabotażu od tego, który ma podłoże polityczne. Warto zwrócić uwagę, że znamiona dookreślające zamiar sprawcy sabotażu przypominają obecne znamiona motywacyjne zawarte w definicji legalnej przestępstwa o charakterze terrorystycznym. Ustawodawca w art. 127 k.k. spenalizował omawiany

[19] M. Lityński, *Przestępstwa przeciwko państwu ludowemu*, op. cit.

sabotaż, a w art. 220 k.k. – tzw. mały sabotaż, czyli przestępstwo o podobnych znamionach czasownikowych, jednak bez wskazanego wcześniej zamiaru kierunkowego[20]. Oprócz znamion przepisy te różnią się zakresem odpowiedzialności karnej. Sam fakt szczególnego rodzaju strony podmiotowej i zachowania w przestępstwie sabotażu powoduje, że odpowiedzialność karna jest większa niż w przypadku małego sabotażu.

Warto zwrócić uwagę na rodzaj infrastruktury będącej przedmiotem ochrony w przepisie penalizującym sabotaż w Kodeksie karnym z 1969 r. O ile w przypadku dekretu z 1946 r. ustawodawca zawęził stronę przedmiotową do zakładów użyteczności publicznej albo komunikacji publicznej bądź urządzeń służących obronie państwa, o tyle w nowym kodeksie posłużył się kategoriami zakładów lub urządzeń albo innego mienia o poważnym znaczeniu dla państwa. Nie ma więc mowy jedynie o infrastrukturze o znaczeniu dla użyteczności publicznej i obronności. Oznacza to, że bez problemów doktrynalnych i wykładni przepisem objęto zakłady wydobywcze, a także zakłady, budowle oraz urządzenia przemysłowe. Ponadto ustawodawca objął ochroną mienie o poważnym znaczeniu dla państwa. W tym wypadku posłużył się zwrotem niedookreślonym i dającym różne możliwości interpretacji.

Z punktu widzenia doktrynalnego czyn, który scharakteryzowano w pkt 1 art. 3 dekretu z 1946 r. i pkt 1 art. 127 k.k. z 1969 r., przyjęło się określać mianem dywersji, natomiast odpowiednio czyn w pkt 2 i 3 art. 3 oraz pkt 2 art. 127 mianem sabotażu[21]. Chodzi więc o sformułowania, które są wieloznaczne w zależności od dziedziny, w jakiej są przedmiotem zainteresowania.

---

[20] A. Krukowski, *Przestępstwa przeciwko podstawowym interesom politycznym i gospodarczym PRL*, w: L. Lernell, A. Krukowski (red.), *Prawo karne. Część szczególna. Wybrane zagadnienia*, Warszawa 1969, s. 5–26; I. Andrejew, *Kodeks karny. Krótki komentarz*, Warszawa 1975, s. 100 i 186.

[21] Podział na przestępstwo dywersji i sabotażu funkcjonował również w ustawach ZSRR (obok nich wyodrębniono przestępstwo szkodnictwa), np. w *Ustawie o przestępstwach przeciwko państwu z 25 lutego 1927 r.* Jakkolwiek podział ten zmodyfikowano w ustawie o przestępstwach przeciwko państwu z 25 grudnia 1958 roku, w której wyodrębniono przestępstwo dywersji i szkodnictwa. W nawiązaniu do doktryny radzieckiej trójelementowy podział aktów sabotażu (art. 3 dekretu z 1946 r.) na dywersję, szkodnictwo i właściwy sabotaż próbował utrzymać polski Wojskowy Sąd Najwyższy, jednak rozróżnienie to należy uznać za dyskusyjne. Należy więc przyjąć, że we wspomnianym artykule mamy do czynienia z przestępstwem dywersji (art. 3 pkt 1 dekretu z 1946 r.) i dwoma rodzajami sabotażu właściwego (art. 3 pkt 2 i 3 dekretu z 1946 r.). Zob. M. Lityński, *Przestępstwa przeciwko państwu ludowemu…*, op. cit., s. 97–110.

Na przykład dywersja i sabotaż będą miały inne znaczenia dla służb specjalnych lub wojska. Szczególnie, gdy obie kategorie mogą być rozpatrywane zarówno w kontekście obronnym, jak i bezpieczeństwa informacji. Wspomniany już wcześniej węgierski autor L. Faragó wskazuje, że termin „sabotaż" w języku tajnych służb oznacza akcje specjalne, więc stanowi jedną z form walki wywrotowej. Działania tego typu przybierają najczęściej postać akcji fizycznych, np. wyrządzenia szkód w infrastrukturze transportowej, przemysłowej i wojskowej. Mimo wszystko należy zwrócić uwagę, że L. Faragó podając różne przykłady aktów sabotażu, nie odróżnia ich od aktów dywersji. Obok fizycznych form sabotażu autor ten wspomina o sabotażu psychologicznym, którego celem jest np. wywołanie zamieszek, strajków, paniki lub strachu[22]. Z kolei w kontekście zorganizowanego oddziaływania na zachowania psychiczne i społeczne ludzi Yuri Bezmenov (T.D. Schuman) używa pojęcia dywersji ideologicznej, która w celu ostatecznym ma doprowadzić do upadku lub przejęcia państwa. Jest to jednak dłuższy proces, który dokonuje się przez demoralizację, destabilizację i wywołanie kryzysu w państwie[23].

Niewątpliwie rozwój technologiczny w różnych sferach życia społecznego rozszerzył możliwości negatywnego oddziaływania przestępców. Wzrastający poziom uzależnienia od technologii informatycznych i energetycznych naturalnie dał możliwość do rozwoju nowych form przestępczości[24]. Dlatego też obok typowych przestępstw polegających na fizycznym niszczeniu lub czynieniu niezdatnym różnego rodzaju mienia albo też uniemożliwieniu lub utrudnieniu prawidłowego korzystania z niego należy zwrócić uwagę na przestępstwa przeciwko ochronie informacji. W kontekście rozwoju technologii inteligentnych sieci elektroenergetycznych, baz danych sieci elektroenergetycznych, systemów zarządzania energią, domów inteligentnych, systemów pomiarowych energii itd. cyberprzestępstwa powinny być przedmiotem głębszych analiz w celu prowadzenia bardziej efektywnej polityki kryminalnej.

---

[22] Zob. więcej w: L. Faragó, *Wojna mózgów…*, op. cit.

[23] Y. Bezmenov, *Soviet Subversion of the Free-World Press: A Conversation with Yuri Bezmenov* (materiał filmowy – wywiad G.E. Griffina z Y. Bezmenovem), American Media 1984.

[24] Por. L.A. Maglaras i in., *Cyber security of critical infrastructures*, „ICT Express" 2018, wol. 4, z. 1, s. 42–45.

4. Przestępstwo sabotażu komputerowego (informatycznego)

Cechą charakterystyczną przepisu penalizującego sabotaż komputerowy jest to, że stanowi on *lex specialis* dla kilku innych przepisów znajdujących się w rozdziale dotyczącym przestępstw przeciwko ochronie informacji w polskim k.k. Co więcej, ze względu na skutki, jakie mogą powstać w wyniku przestępstwa sabotażu, przepis ten umożliwia dokonanie kumulatywnej kwalifikacji np. z artykułem 165 k.k. (penalizującym przestępstwo sprowadzenia niebezpieczeństwa dla życia i zdrowia) i 174 k.k. (penalizującym przestępstwo sprowadzenia katastrofy komunikacyjnej)[25].

W ogólnym ujęciu przestępstwo sabotażu określone w art. 269 § 1 k.k. dotyczy ingerencji w dane informatyczne, które mają szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Pierwsza forma ingerencji w dane informatyczne może przybrać postać ich niszczenia, uszkodzenia, usuwania lub zmiany. Z kolei druga może polegać na uniemożliwieniu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Ponadto art. 269 § 2 k.k. przewiduje odpowiedzialność karną za sabotaż komputerowy, który może mieć dwa rodzaje skutków negatywnych. W pierwszym wypadku będzie to sabotaż wobec danych informatycznych, którego skutkiem jest niszczenie lub wymiana informatycznego nośnika danych, natomiast w drugim – z sabotaż, którego skutkiem jest uszkodzenie urządzenia do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych. Zatem art. 269 § 2 k.k. przewiduje ochronę danych informatycznych przed ingerencją o charakterze fizycznym.

Zakres ingerencji określony art. 269 k.k. § 1–2 dotyczy więc różnego rodzaju oddziaływania w stosunku do danych informatycznych, automatycznego przetwarzania danych, informatycznego nośnika i urządzenia służącego do automatycznego przetwarzania danych informatycznych. W pierwszym rzędzie należy wyjaśnić, czym są dane informatyczne, definicji legalnej tego terminu nie zawarto bowiem w ustawie karnej. Można ją jednak odnaleźć

[25] P. Kozłowska-Kalisz, *Przestępstwa przeciwko ochronie informacji*, w: M. Mozgawa i in. (red.), *Kodeks karny. Komentarz*, Warszawa 2017, s. 825–826.

w Konwencji Rady Europy o cyberprzestępczości z 2001 r. **Dane informatyczne** to „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny". Z kolei **system informatyczny** to według Konwencji „każde urządzenie lub grupa wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych"[26]. Natomiast za **informatyczny nośnik danych** należy uznać rzeczy lub urządzenia, które służą do przechowywania, zapisywania i odczytywania danych zarówno w postaci analogowej, jak i cyfrowej[27].

Przestępstwo sabotażu komputerowego ukierunkowane jest na dane informatyczne, które mają szczególne znaczenie w określonych sferach publicznych. Oznacza to, że w przeciwieństwie do przepisów bardziej ogólnych ma znaczenie rodzaj informacji i charakter związanych z nimi dóbr czy interesów. Mimo wszystko głównym dobrem chronionym w artykule penalizującym sabotaż komputerowy jest bezpieczeństwo informacji, natomiast dobrami pobocznymi są te, które charakteryzują zarazem przedmiot czynności wykonawczej przestępstwa[28]. Kwestią otwartą jest natomiast, czy każdy ze zwrotów, który służy dookreśleniu szczególnego znaczenia danych informatycznych, jest jednoznaczny. Przykładem może być znamię „szczególne znaczenie dla obronności kraju". Posłużono się w nim terminami, które stanowią wyznacznik strony podmiotowej przestępstw spenalizowanych w jednym z rozdziałów polskiego k.k. pt. *Przestępstwa przeciwko obronności*. Pytanie, czy ustawodawcy chodziło o ochronę dobra tożsamą z dobrem chronionym w rozdziale dotyczącym przestępstw przeciwko obronności państwa, czy może o bardziej kolokwialne rozumienie obronności, które można sprowadzić do bezpieczeństwa wewnętrznego lub zewnętrznego.

---

[26] *Konwencja Rady Europy o cyberprzestępczości*, sporządzona w Budapeszcie 23 listopada 2001 r. (Dz.U. 2015 poz. 728).

[27] P. Kozłowska-Kalisz, *Przestępstwa przeciwko ochronie informacji…*, op. cit., s. 823.

[28] F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom komputerowym*, Warszawa 2016, s. 322–327; R. Hałas, *Przestępstwa przeciwko ochronie informacji*, w: A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*, Warszawa 2019, s. 1326–1327.

Pytanie to jest zasadne ze względu na doktrynalne przyjęcie nazewnictwa przestępstwa określonego w art. 269 k.k. jako przestępstwa sabotażu komputerowego. Z punktu widzenia interpretacji historycznej należy przypomnieć, że niszczenie lub uszkadzanie określonej infrastruktury to akt dywersji, natomiast utrudnianie korzystania z infrastruktury, jej celowe złe wykorzystywanie albo zaniechanie obowiązków jej obsługi to akty sabotażu. Utrzymując perspektywę obronności rozumianej jako moc obronna i zdolność militarna do przeciwstawiania się agresji, przekształca się tym samym strukturę dobra chronionego. W kontekście zagrożeń hybrydowych pojawia się problem przesunięcia dobra pobocznego również w kierunku przestępstw przeciwko państwu i pokojowi.

Kolejną dosyć otwartą kwestią jest status informacji, tzn. ich szczególne znaczenie dla poszczególnych sfer – obronności, bezpieczeństwa komunikacji i funkcjonowania administracji rządowej i innego rzędu. Jacek W. Giezek wskazuje, że ocena taka powinna nastąpić za pomocą obiektywnego kryterium, nie istnieje bowiem kryterium subiektywne możliwe do efektywnego wykorzystania[29]. Mimo tej tezy wydaje się, że nie istnieje również obiektywne kryterium szczególnego znaczenia dla poszczególnych dziedzin. Dlatego trudno wskazać na takie kryterium w przypadku obronności, bezpieczeństwa komunikacji i funkcjonowania administracji w każdej sytuacji. Wydaje się, że w zależności od sytuacji konieczne będzie stosowanie kryterium mieszanego, czyli obiektywno-subiektywnego. Z podobnym, lecz nieidentycznym problemem, można zetknąć się w przepisach dotyczących ochrony informacji niejawnej w tym samym rozdziale k.k. (doktrynalna dyskusja na temat formalnej przesłanki statusu informacji niejawnej i materialnych kryteriów jej oceny)[30].

Konsekwencją braków w penalizacji czynów ukierunkowanych na zakłócenie pracy sieci informatycznych było dodanie do k.k. art. 269a. W literaturze

[29] J.W. Giezek (red.), *Przestępstwa przeciwko ochronie informacji*, w: *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014, s. 1001.

[30] Por. P. Kozłowska-Kalisz, *Przestępstwa przeciwko ochronie informacji…*, op. cit., s. 808–816; W. Wróbel, D. Zając, *Przestępstwa przeciwko ochronie informacji*, w: W. Wróbel, A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d*, Warszawa 2017, s. 606–642; B. Gadecki, *Kodeks karny. Część szczególna. Art. 252–316. Komentarz*, Warszawa 2017, s. 63–68; R. Hałas, *Przestępstwa przeciwko ochronie informacji*, w: A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*, op. cit., s. 1316–1322.

wskazuje się, że nowy przepis miał właściwie implementować zapisy art. 5 Konwencji Rady Europy o cyberprzestępczości z 2001 r.[31] Konwencja ta wymagała od sygnatariuszy penalizacji czynów „umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych"[32]. W obecnym stanie prawnym przestępstwo zakłócania pracy sieci określone art. 269a k.k. obejmuje istotne zakłócenie pracy systemów informatycznych, systemów i sieci teleinformatycznych. Istotne zakłócenie systemów lub sieci może być wynikiem transmisji, zniszczenia, usunięcia, uszkodzenia, utrudnienia lub zmiany danych informatycznych. Trzymając się kategorii historycznych, należy wskazać, że czyny te mają cechy zarówno sabotażu, jak i dywersji. Przepis ten ze względu na stosowanie podlega różnym interpretacjom, co wynika z faktu, że jego znamiona zbliżone są do zapisów w innych przepisach w rozdziale dotyczącym przestępstw przeciwko ochronie informacji. Uznaje się więc, że art. 269a k.k. stanowi *lex specialis* w stosunku do przepisów penalizujących utrudnianie zapoznania się z informacją (268 k.k.) i niszczenie danych informatycznych (268a k.k.).

Od zakłócenia funkcjonowania sieci i systemów ze względu na dane informatyczne należy odróżnić przestępstwo zakłócenia działania całości lub części sieci (wodociągowych, kanalizacyjnych, ciepłowniczych, elektroenergetycznych, gazowych i telekomunikacyjnych) albo linii (kolejowych, tramwajowych, trolejbusowych i metra), które określone zostało w art. 254a, przy czym zakłócenie to następuje wskutek zaboru, zniszczenia, uszkodzenia lub uczynienia niezdatnym do użytku elementu wchodzącego w skład wymienionych sieci lub linii[33]. Wśród wymienionej infrastruktury ustawodawca wyszczególnił infrastrukturę energetyczną i informatyczną. W przepisie tym

---

[31] F. Radoniewicz, *Odpowiedzialność karna za hacking…*, op. cit., s. 327–329.

[32] *Konwencja Rady Europy o cyberprzestępczości*, op. cit.

[33] R. Krajewski, *Przestępstwo zakłócenia działania sieci lub linii tworzących infrastrukturę techniczną*, „Wojskowy Przegląd Prawniczy", 2014, nr 2, s. 52–62; M. Mozgawa, *Przestępstwa przeciwko porządkowi publicznemu*, w: M. Mozgawa (red.) et al., *Kodeks karny. Komentarz…*, op. cit., s. 775–777; Z. Ćwiąkalski, *Przestępstwa przeciwko porządkowi publicznemu*, w: W. Wróbel, A. Zoll (red.), *Kodeks karny. Część szczególna…*, op. cit., s. 503–508.

de facto chodzi o penalizację aktów sabotażu infrastruktury użyteczności publicznej (zamachu na urządzenia infrastruktury).

Wydaje się, że przywiązywanie wagi w doktrynalnych ujęciach czynu spenalizowanego w art. 269 k.k. do kategorii sabotażu może skutkować potrzebą zmian w ramach zagadnień dotyczących przestępstw przeciwko ochronie informacji, ale i w innych częściach k.k. W pierwszym rzędzie przestępstwo sabotażu związane było z funkcją użyteczności publicznej określonych rodzajów infrastruktury. Świadczą o tym zapisy chociażby art. 217, 223 i 224 k.k. z 1932 r., a także art. 3 dekretu z 1946 r. Inną tradycją jest powiązanie sabotażu z trzema sferami, czyli polityczną (państwem), gospodarczą i militarną. Ze względu na coraz większą technicyzację sfer życia społecznego (m.in. za pomocą dematerializacji transportu i komunikacji), a także ze względu na wzrost zagrożeń zewnętrznych za pomocą konfliktów nowych generacji (np. działań hybrydowych) granice między tymi sferami dawno się zatarły. Widać to dobrze w sferze infrastruktury energetycznej, która podlega procesom wzmożonej informatyzacji. Obecnie bez infrastruktury wytwórczej, przesyłowej, dystrybucyjnej i magazynowej energii w zasadzie nie ma możliwości pomyślnego rozwoju państwa. Zatem przestępcza ingerencja w cyfrowe procesy zarządzania energią powinna być przedmiotem głębszej dyskusji na temat cyberprzestępczości w sferze energetyki. Wydaje się, że przestępstwa przeciwko ochronie informacji w kontekście nowych zagrożeń powinny być przedmiotem głębszego przemyślenia w ramach polityki karnej.

5. Przykłady sabotaży infrastruktury energetycznej i innego typu

Infrastruktura wytwórcza, przesyłowa i dystrybucyjna energii staje się przedmiotem zwiększonego ryzyka cyberataków, podobnie zresztą jak w przypadku innego rodzaju infrastruktury krytycznej i strategicznej[34]. Skutki negatywne tego rodzaju ataków mogą być trudne do przewidzenia, na pewno mogą

[34] Por. A. Zimba, Z. Wang, H. Chen, *Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems*, „ICT Express", 2018, wol. 4, z. 1, s. 14–18.

stanowić większe zagrożenie niż ataki na systemy informatyczne instytucji publicznych i finansowych przeprowadzone w Estonii w 2017 r.

Potencjalnym zagrożeniem mogą być rozległe awarie zasilania lub inne rodzaje zakłóceń zasilania, które w stopniu znacznym będą wpływać na funkcjonowanie społeczeństwa, gospodarki i państwa. Przykładem tego problemu może być jedna z największych awarii zasilania w USA i Kanadzie w 2003 r. Przywracanie systemu elektroenergetycznego trwało ponad 35 godzin, w zależności od obszaru braki dostaw energii trwały od jednego do trzech dni, a liczbę mieszkańców odciętych od energii elektrycznej szacowano na ponad 50 milionów. Skutkiem awarii było wyłączenie ponad 260 elektrowni (w tym 16 elektrowni jądrowych), paraliż komunikacyjny i problemy z realizacją innych usług aglomeracyjnych[35]. Mimo istnienia oficjalnych raportów na temat przyczyn tego zdarzenia, niektóre źródła prasowe wskazują, że administracja rządowa USA uwzględnia uczestnictwo chińskich hakerów w destabilizacji sieci elektroenergetycznej USA i Kanady w 2003 r. Co więcej, wskazuje się, że za braki dostaw energii wzdłuż wschodniego wybrzeża Florydy w 2008 r również odpowiadają hakerzy[36]. Przykładem zagrożeń w sektorze energetycznym może być też to, że w 2003 r. podczas szerszego ataku na świecie robak SQL Slammer przedostał się m.in. do systemu wyświetlania parametrów bezpieczeństwa i systemu monitorowania elektrowni jądrowej Davis-Besse w USA[37]. Z kolei w 2012 i 2013 r. za pomocą złośliwego oprogramowania rosyjscy hakerzy próbowali nielegalnie pozyskiwać informacje z amerykańskich spółek użyteczności publicznej (w tym ze spółek energetycznych)[38].

---

[35] *Blackout 2003: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force, 2004.

[36] S. Harris, *Chinese hackers pose serious danger to U.S. computer networks Hackers may be responsible for two major U.S. power blackouts*, https://www.govexec.com/defense/2008/05/chinese-hackers-pose-serious-danger-to-us-computer-networks/26971/ (dostęp: 12.09.2019).

[37] M. Wu, Y.B. Moon, *Taxonomy of Cross-Domain Attacks on CyberManufacturing System*, „Procedia Computer Science" 2017, no. 114, s. 367–374; J. Shin, H. Son, G. Heo, *Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET*, „Nuclear Engineering and Technology" 2017, wol. 49, z. 3, s. 517–524.

[38] G. Burke, J. Fahey, *Iranian hackers breached US power grid to engineer blackouts*, https://www.timesofisrael.com/iranian-hackers-breached-us-power-grid-to-engineer-blackouts/ (dostęp: 12.09.2019).

Kolejnym przykładem ataków cybernetycznych na infrastrukturę energetyczną może być awaria ukraińskiej elektrowni w Zaporożu w grudniu 2015 r. W różnych opracowaniach wykazuje się, że jest to przykład skutecznego ataku na obiekt wytwarzający energię, którego skutkiem było przerwanie dostaw energii elektrycznej do odbiorców. Ocenia się, że na skutek awarii przez kilka godzin ok. 0,7 miliona gospodarstw domowych nie miało dostępu do energii elektrycznej. Z kolei w 2017 r. rosyjscy hakerzy dokonali ataku na sieć energetyczną w okolicy Kijowa na Ukrainie. Wskazuje się, że zarówno w 2015, jak i w 2017 roku do przełamania systemu bezpieczeństwa wykorzystano te same narzędzia, tj. BlackEnergy i KillDisk[39].

Poza problematyką sabotażu infrastrukturalnego i informatycznego należy zwrócić uwagę na nowe wersje działań za pomocą technologii internetowych, które przybierają postać dywersji ideologicznej. Znajduje to swoje odzwierciedlenie w ingerencji np. Rosji w przebieg wyborów prezydenckich i parlamentarnych albo referenda w USA i Wielkiej Brytanii. Do szeroko rozumianego sabotażu politycznego dochodzi za pomocą tzw. farm trolli internetowych i ich kont w serwisach społecznościowych takich jak Facebook i Twitter[40]. Działania dezinformujące za pomocą farm trolli lub po prostu za pomocą skoordynowanych działań internetowych mogą też dotyczyć rozpowszechniania nieprawdziwych informacji na temat technologii energetycznych (zarówno konwencjonalnych, jak i niekonwencjonalnych). Mogą ponadto służyć kreowaniu braku zaufania społeczeństwa do władz w obliczu różnych incydentów związanych z infrastrukturą energetyczną lub wydobywczą (np. z eksploatacją elektrowni jądrowych lub szczelinowaniem gazu łupkowego).

---

[39] *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, E-ISAC, Washington 2016; M. Baezner, P. Robin, *Cyber and Information warfare in the Ukrainian conflict*, Zürich 2018.

[40] Por. *Background to „Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, Office of the Director of National Intelligence, Washington 2017; M. Field, M. Wright, *Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals*, https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/ (dostęp: 17.10.2018); R.S. Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, Washington 2019; *Report on the implementation of the Action Plan Against Disinformation*, European Commission /JOIN(2019) 12 final/, Brussels 2019; L. Sykulski, *Rosyjska geopolityka a wojna informacyjna*, Warszawa 2019, s. 80–130.

Z punktu widzenia polityki kryminalnej wydaje się, że należy w Polsce rozwijać wyspecjalizowane służby specjalne do zwalczania zagrożeń cybernetycznych, szczególnie w zakresie zagrożeń infrastruktury strategicznej i krytycznej. Ze względu na konieczność zapewnienia funkcjonowania systemu energetycznego trzeba odejść od rozwiązań ukierunkowanych na poszczególne podmioty energetyczne. Istnieje wyraźna potrzeba wzmocnienia bezpieczeństwa całego procesu dostaw energii, od wytwarzania po finalnego odbiorcę.

6. Zakończenie

Zakres przedmiotowy problemu badawczego zaprezentowanego w niniejszym tekście objął wybrane przestępstwa przeciwko ochronie informacji w kontekście bezpieczeństwa energetycznego. Zaprezentowana analiza skupiła się głównie na interpretacji historycznej, doktrynalnej i funkcjonalnej przestępstw sabotażu, sabotażu komputerowego i zakłócenia pracy w sieci. W celu uszczegółowienia problemu badawczego w tekście przedstawiono następujące pytania badawcze:

(1) Jakie powinny być kierunki zmian w zakresie penalizacji czynów określanych mianem sabotażu komputerowego (informatycznego) w ramach polityki karnej? Przyjmując szerokie rozumienie sabotażu, obejmujące też historyczną i doktrynalną kategorię prawną przestępstwa dywersji, należy wskazać, że konieczne jest wyeliminowanie trudności w interpretacji przepisów penalizujących czyny przeciwko ochronie informacji. Warto też rozważyć systemowe i metodyczne rozwiązania w zakresie penalizacji czynów określanych mianem sabotażu i dywersji ukierunkowanych na infrastrukturę użyteczności publicznej, strategiczną i krytyczną (w tym infrastrukturę energetyczną). Ponadto wraz ze wzrostem znaczenia technologii informatycznych w różnych sferach życia, szczególnie tych, które służą komunikacji, należy zastanowić się nad sposobami penalizacji czynów związanych z czymś, co określono w tekście jako nowe formy dywersji ideologicznej.

(2) Jaki wpływ na zmiany w zakresie penalizacji czynów określanych mianem sabotażu komputerowego (informatycznego) powinny mieć zagrożenia w zakresie bezpieczeństwa energetycznego?

Przykłady sabotażu i dywersji ukierunkowanych na destabilizację systemów energetycznych w USA i na Ukrainie wskazują na konieczność przemyślenia rozwiązań prawnych, które rozszerzyłyby odpowiedzialność karną za ten rodzaj czynów przestępczych. Biorąc pod uwagę, że nowy rodzaj konfliktów zewnętrznych, przyjmujących postać konfliktów hybrydowych, jest faktem, to uwzględnić należy potrzebę przesunięcia dobra chronionego z obszaru ochrony informacji w kierunku obronności i bezpieczeństwa państwa.

Z punktu widzenia zwalczania przestępczości należy rozważyć rozbudowę i wzmocnienie instytucji, których funkcją jest taktyka kryminalna w zakresie zwalczania przestępczości w sferze nowych technologii. Mimo już istniejących rozwiązań instytucjonalnych w zakresie zwalczania różnych form terroryzmu, w tym cyberterroryzmu, wydaje się, że bezpieczeństwo w tym zakresie trzeba przenieść na wyższy poziom specjalizacji. Warto jednak zwrócić uwagę, że instytucje same w sobie nie gwarantują bezpieczeństwa, konieczna jest bowiem równoległa praca nad kulturą bezpieczeństwa. Swoista kultura bezpieczeństwa powinna być wyznacznikiem funkcjonowania spółek zarządzających infrastrukturą strategiczną lub krytyczną (w tym wypadku również i infrastrukturą energetyczną). Wynika to z faktu, że czynnik ludzki jest jednym ze słabszych ogniw ochrony przed sabotażem i dywersją informatyczną.

Bibliografia

Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case, E-ISAC, Washington 2016.

Andrejew I., *Kodeks karny. Krótki komentarz*, Warszawa 1975.

Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, Office of the Director of National Intelligence, Washington 2017.

Bezmenov Y., *Soviet Subversion of the Free-World Press: A Conversation with Yuri Bezmenov* (materiał filmowy – wywiad G.E. Griffina z Y. Bezmenovem), American Media 1984.

Blackout 2003: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, U.S.-Canada Power System Outage Task Force, 2004.

Bojarski M. (red.), *Prawo karne materialne. Część ogólna i szczególna*, Warszawa 2017.

Burke G., Fahey J., *Iranian hackers breached US power grid to engineer blackouts*, https://www.timesofisrael.com/iranian-hackers-breached-us-power-grid-to-engineer-blackouts/ (dostęp: 12.09.2019).

Cherp A., Jewell J., *The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration*, "Current Opinion in Environmental Sustainability", 2011, wol. 3, nr 4, s. 202–212.

Ćwiąkalski Z., *Przestępstwa przeciwko porządkowi publicznemu,* w: W. Wróbel, A. Zoll, *red.*, *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017, s. 503–508.

Dekret z dnia 13 czerwca 1946 r. *o przestępstwach szczególnie niebezpiecznych w okresie odbudowy Państwa* (Dz.U. 1946 Nr 30 poz. 192).

Destruction of Stocking Frames, etc. Act 1812 (52 Geo 3 c. 16).

Dukiet-Nagórska T. (red.), *Prawo karne. Część ogólna, szczególna i wojskowa*, Warszawa 2018.

Fajnberg J., Leonieni M. (oprac.), *Kodeks karny z orzecznictwem okresu powojennego*, Łódź 1958.

Faragó L., *Wojna mózgów. Anatomia szpiegostwa i wywiadu*, Warszawa 1961.

Gadecki B., *Kodeks karny. Część szczególna: Art. 252-316. Komentarz*, Warszawa, 2017.

Gardocki L., *Prawo karne*, Warszawa 2002.

Giezek J.W. (red.), *Przestępstwa przeciwko ochronie informacji*, w: *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014, s. 976–1001.

Giezek J.W. (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014.

Giezek J.W., *Przedmiot prawnokarnej ochrony*, w: M. Bojarski (red.) *Prawo karne materialne. Część ogólna i szczególna*, Warszawa 2017, s. 101–108.

Grześkowiak A., Wiak K. (red.), *Kodeks karny. Komentarz*, Warszawa 2019.

Hałas R., *Przestępstwa przeciwko ochronie informacji*, w: A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*, Warszawa 2019, s. 1314–1330.

Harris S., *Chinese hackers pose serious danger to U.S. computer networks Hackers may be responsible for two major U.S. power blackouts*, https://www.govexec.com/defense/2008/05/chinese-hackers-pose-serious-danger-to-us-computer-networks/26971/ (dostęp: 12.09.2019).

Hécart G.A.J., *Dictionnaire rouchi-français*, Paris 1834.

Hozumi F., *Some Notes on the Luddites*, "Kyoto University Economic Review", 1956, wol. 26, nr 2, s. 10–38.

d'Hautel Ch.-L., *Dictionnaire du bas-langage, ou, Des manières de parler usitées parmi le peuple*, Paris 1808.

Kałążna K., Rosicki R., *Wymiary bezpieczeństwa energetycznego Unii Europejskiej*, Poznań 2010.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. 2015 poz. 728).

Kozłowska-Kalisz P., *Przestępstwa przeciwko ochronie informacji*, w: M. Mozgawa i in. (red.), *Kodeks karny. Komentarz*, Warszawa 2017, s. 807–829.

Krajewski R., *Przestępstwo zakłócenia działania sieci lub linii tworzących infrastrukturę techniczną*, „Wojskowy Przegląd Prawniczy", 2014, nr 2, s. 52–62.

Krukowski A., *Przestępstwa przeciwko podstawowym interesom politycznym i gospodarczym PRL*, w: L. Lernell, A. Krukowski (red.), *Prawo karne. Część Szczególna. Wybrane zagadnienia*, Warszawa 1969, s. 5–26.

Lernell L., Krukowski A. (red.), *Prawo karne. Część Szczególna. Wybrane zagadnienia*, Warszawa 1969.

Leszczyński T.Z. (red.), *Bezpieczeństwo energetyczne Polski w Unii Europejskiej – wizja czy rzeczywistość?*, Warszawa 2012.

Littré E., *Dictionnaire de la langue française: Tome 4*, Paris 1873.

Lityński M., *Przestępstwa przeciwko państwu ludowemu*, Łódź 1960.

Maglaras L.A. i in., *Cyber security of critical infrastructures*, „ICT Express", 2018, wol. 4, z. 1, s. 42–45.

Mozgawa M. i in. (red.), *Kodeks karny. Komentarz*, Warszawa 2017.

Mozgawa M., *Przestępstwa przeciwko porządkowi publicznemu*, w: M. Mozgawa i in. (red.), *Kodeks karny. Komentarz*, Warszawa 2017.

Mueller, R.S. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, Washington 2019.

Navickas K., *The search for 'General Ludd': the mythology of Luddism*, „Social History", 2005, wol. 30, nr 3, s. 281–295.

Pohl Ł., *Prawo karne. Wykład części ogólnej*, Warszawa 2019.

Pouget É., *Le Sabotage*, „Almanach du Père Peinard" 1898.

Pouget É., *Le Sabotage*, Paris 1911.

Radoniewicz F., *Odpowiedzialność karna hacking i inne przestępstwa przeciwko danym komputerowym i systemom komputerowym*, Warszawa 2016.

Report on the implementation of the Action Plan Against Disinformation, European Commission /JOIN(2019) 12 final/, Brussels 2019.

Rosicki R., *O pojęciu i istocie bezpieczeństwa*, „Przegląd Politologiczny", 2010, nr 3, s. 24–32.

Rosicki R., *Pojęcie i definicje bezpieczeństwa energetycznego*, w: T.Z. Leszczyński (red.), *Bezpieczeństwo energetyczne Polski w Unii Europejskiej – wizja czy rzeczywistość?*, Warszawa 2012, s. 35–65.

Rosicki R., *Kultury energetyczne Unii Europejskiej*, Poznań 2018.

Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. Kodeks karny (Dz.U. 1932 Nr 60 poz. 571).

Shin J., Son H., Heo G., *Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET*, „Nuclear Engineering and Technology", 2017, wol. 49, z. 3, s. 517–524.

Siewierski M., *Mały kodeks karny i postępowanie doraźne wraz z przepisami o Komisji Specjalnej do walki z nadużyciami i innymi dodatkowymi. Komentarz*, Łódź 1947.

Siewierski M., *Kodeks karny i prawo o wykroczeniach. Komentarz*, Warszawa 1958.

Sobol E. (red.), *Słownik wyrazów obcych*, Warszawa 1995.

Sykulski L., *Rosyjska geopolityka a wojna informacyjna*, Warszawa 2019.

Thomis M.I., *The Luddites: machine-breaking in regency England*, Newton Abbot 1970.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 Nr 88 poz. 553 ze zm.).

Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 1997 Nr 54 poz. 348 ze zm.).

Wróbel W., Zając D., *Przestępstwa przeciwko ochronie informacji*, w: W. Wróbel, A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017, s. 606–642.

Wu M., Moon Y.B., *Taxonomy of Cross-Domain Attacks on CyberManufacturing System*, „Procedia Computer Science", 2017, nr 114, s. 367–374.

Zimba A., Wang Z., Chen H., *Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems*, „ICT Express", 2018, wol. 4, z. 1, s. 14–18.

ROZDZIAŁ IV

Społeczna akceptacja popełniania przestępstw ubezpieczeniowych jako przesłanka sprzyjająca przestępczości na rynku ubezpieczeniowym

TOMASZ JEDYNAK[1]

1. Wprowadzenie

Oszustwa ubezpieczeniowe są równie stare jak funkcjonowanie samej metody ubezpieczeniowej, a udokumentowana historia przestępczości ubezpieczeniowej sięga początków rynku ubezpieczeń w starożytnym Rzymie. W zachowanych źródłach prawnicy rzymscy odnotowywali sytuacje, w których dochodziło do nadużyć na rynku ubezpieczeniowym. Wśród najczęstszych oszustw związanych z kontraktami ubezpieczeniowymi już dwa tysiące lat temu wymieniali oni zdarzenia, takie jak: sfingowane zatonięcia ubezpieczonych statków, napady na karawany, kradzież towarów czy pożary magazynów

[1] Adiunkt w Katedrze Zarządzania Ryzykiem i Ubezpieczeń Uniwersytetu Ekonomicznego w Krakowie. Absolwent kierunku Finanse i Rachunkowość. Od 2009 r. makler papierów wartościowych z uprawnieniami do czynności doradztwa inwestycyjnego. Ukończył studia podyplomowe na Wydziale Zarządzania UEK Zarządzanie projektami badawczymi i komercjalizacja wyników badań. W 2015 r. obronił na Wydziale Finansów UEK pracę doktorską pt. *Efektywność i ryzyko funduszy inwestycji społecznie odpowiedzialnych*, która zdobyła pierwsze miejsce w konkursie o Nagrodę Prezesa Zarządu GPW SA oraz została wyróżniona Nagrodą Rektora UEK. Uczestnik warsztatów NUS-Santander Doctorate Workshop on Advanced Financial Risk Management na Narodowym Uniwersytecie w Singapurze. W 2016 r. odbył półroczny staż naukowo-badawczy na Wydziale Zarządzania Uniwersytetu Warszawskiego. Wykładał gościnnie na Lwowskim Instytucie Bankowości Narodowego Banku Ukrainy, Politechnice Lwowskiej oraz Uniwersytecie Ekonomicznym w Pradze.

Autor i współautor kilkudziesięciu publikacji za zakresu ekonomii i finansów, współautor dwóch podręczników akademickich. Wykonawca i współwykonawca kilkunastu projektów naukowo-badawczych obejmujących zagadnienia z zakresu finansów, w tym w szczególności problematykę ubezpieczeń społecznych i funkcjonowania systemu emerytalnego. Wykładowca na studiach doktoranckich i podyplomowych prowadzonych w Uniwersytecie Ekonomicznym w Krakowie. Uczestnik wielu międzynarodowych i krajowych konferencji i seminariów naukowych.

mające na celu wyłudzenie nienależnego odszkodowania[2]. Rzecz jasna na przestrzeni kolejnych stuleci charakter i forma przestępstw ubezpieczeniowych ewoluowały. Niewątpliwie stosowane przez współczesnych sprawców przestępstw ubezpieczeniowych metody wyłudzania odszkodowań i świadczeń są bardziej wyrafinowane, a przez to trudniejsze do wykrycia. W coraz większym stopniu przestępczość ubezpieczeniowa staje się również domeną zorganizowanych grup przestępczych, w skład których wchodzą pracownicy różnych instytucji rynku ubezpieczeniowego (w tym także zakładów ubezpieczeń). Wydaje się jednak, że jedna kwestia związana z przestępczością ubezpieczeniową nie zmieniła się – głównym motywem działania ich sprawców była i jest chęć wzbogacenia się kosztem zakładu ubezpieczeń, a więc pośrednio również kosztem wszystkich jego klientów.

Mając na uwadze, że zjawisko przestępczości ubezpieczeniowej stanowi jedno z największych wyzwań dla współczesnego rynku ubezpieczeń, w ramach opracowania podjęto rozważania nad problemem przyczyn powstawania sytuacji, w których dochodzi do przestępstw na rynku ubezpieczeniowym, oraz podjęto próbę wskazania potencjalnych rozwiązań im zapobiegających w aspekcie koncepcji „Transforming People and Organizations". Tak określony problem badawczy jest niezwykle obszerny i nie sposób wyczerpująco go przeanalizować i przedstawić w formie jednej publikacji monograficznej, a tym bardziej syntetycznej ekspertyzy. Stąd też, uwzględniając ograniczone ramy opracowania, za główną tezą prowadzonych w nim rozważań przyjęto stwierdzenie, zgodnie z którym istotną przesłanką sprzyjającą przestępczości na rynku ubezpieczeniowym jest zjawisko społecznej akceptacji popełniania przestępstw ubezpieczeniowych. Wyprowadzeniu koncepcyjnemu powyższej tezy oraz jej uzasadnieniu poświęcone są kolejne punkty opracowania.

Opracowanie uwzględnia trojakie podejście do prowadzonych rozważań: prawne, technologiczne oraz gospodarcze, przy czym charakter podjętego problemu badawczego oraz przyjęta teza badawcza powodują, że główną oś rozważań stanowią kwestie gospodarcze i ekonomiczno-społeczne. Ponadto w opracowaniu, aczkolwiek nie wprost, uwzględniono dwa ujęcia problemu

[2] S. Stypułkowski, *Przestępstwa ubezpieczeniowe oraz działania podejmowane w celu ich ograniczenia,* „Prawo, Ubezpieczenia, Reasekuracja, Warszawa", 1999, nr 12 (36), s. 77.

przyczyn przestępczości na rynku ubezpieczeniowym –osobowe oraz instytucjonalne.

Aby umożliwić realizację głównego celu pracy, jakim jest uzasadnienie przyjętej tezy badawczej, określono następujące cele szczegółowe poszczególnych części opracowania:

1. charakterystyka pojęcia przestępstwa ubezpieczeniowego oraz sprawców przestępstw ubezpieczeniowych;
2. identyfikacja przyczyn powstawania sytuacji, w których dochodzi do przestępstw rynku ubezpieczeniowym oraz rozpoznanie typowych przestępstw ubezpieczeniowych, ze szczególnym uwzględnieniem kwestii związanych ze społeczną akceptacją przestępczości ubezpieczeniowej;
3. wskazanie potencjalnych metod i narzędzi przeciwdziałania przestępczości ubezpieczeniowej w kontekście przeprowadzonych rozważań.

Metody badawcze wykorzystane do realizacji poszczególnych celów pracy opierają się głównie na rozumowaniu dedukcyjnym. W pierwszej kolejności, na podstawie przeglądu piśmiennictwa przeprowadzono została analiza o charakterze teoretyczno-kompilacyjnym. Następnie, opierając się na wnioskach płynących z tych analiz, podjęto próbę krytyki wybranych koncepcji, dokonano syntezy zebranego materiału oraz sformułowano autorskie propozycje dotyczące przeciwdziałania przestępczości na rynku ubezpieczeniowym w analizowanym aspekcie.

Struktura opracowania odpowiada przyjętym celom szczegółowym i poza niniejszym wstępem obejmuje trzy części oraz podsumowanie. W **części pierwszej** nakreślono istotę pojęcia przestępstwa ubezpieczeniowego oraz przedstawiono klasyfikację przestępczości ubezpieczeniowej. W **części drugiej** wskazano i scharakteryzowano sprawców przestępstw ubezpieczeniowych i podano szacunkowe rozmiary przestępczości ubezpieczeniowej w Polsce. W **części trzeciej** szczegółowym analizom poddano przyczyny powstawania sytuacji, w których dochodzi do przestępstw na rynku ubezpieczeniowym, oraz w ogólnym ujęciu wskazano typowe przestępstwa ubezpieczeniowe. Zgodnie z postawioną wyżej tezą w rozdziale skoncentrowano się przede wszystkim na kwestiach związanych ze społeczną akceptacją przestępczości ubezpieczeniowej. **Część czwarta** obejmuje zagadnienia z zakresu zapobiegania przestępczości w obszarze ubezpieczeń. Całość opracowania

kończy **podsumowanie**, w którym sformułowano najważniejsze wnioski płynące z przeprowadzonych rozważań oraz wysunięto autorskie postulaty w zakresie innowacji mających na celu przeciwdziałanie przestępstwom ubezpieczeniowym.

2. Przestępstwo ubezpieczeniowe

Pojęcie przestępstwa ubezpieczeniowego w piśmiennictwie nie jest definiowane jednoznacznie. W szerokim ujęciu Tadeusza Rydzeka przestępstwo ubezpieczeniowe to każdy czyn karalny, który w sposób bezpośredni lub pośredni godzi w funkcjonowanie rynku ubezpieczeniowego bądź interesy firm i instytucji ubezpieczeniowych[3]. Nieco odmiennego zdania jest Waldemar Jaroch, który uważa, że przestępstwo ubezpieczeniowe to przestępstwo godzące w interesy towarzystw ubezpieczeniowych i rynku ubezpieczeń, wiążące się ze stosunkiem ubezpieczeniowym[4]. Podejmując się sformułowania formalno-prawnej definicji przestępstwa ubezpieczeniowego, Eugeniusz Kędra stwierdza natomiast, że jest to „społecznie szkodliwy, bezprawny, zawiniony, karalny zamach na majątkowe i niemajątkowe dobra ubezpieczone, czyniący w nich podlegające kompensacji szkodę, oraz zamach na wszelkie inne dobra prawne ubezpieczyciela"[5].

Europejski Komitet Ubezpieczeń (Comité Europeén des Assurances, obecnie Insurance Europe –CEA) przyjmując wąską perspektywę definiowania przestępstwa ubezpieczeniowego stoi na stanowisku, że jest to „żądanie odszkodowania lub otrzymanie takiego odszkodowania drogą oszustwa"[6]. Podobnie pojęcie przestępczości ubezpieczeniowej traktują Krystian Dąbek i Andrzej Kamiński, zdaniem których przestępczość ubezpieczeniowa to działania lub zaniechania, które mają doprowadzić do uzyskania nienależnego

[3] T. Rydzek, *Przestępczość ubezpieczeniowa w świetle teorii i praktyki*, „Prawo Asekuracyjne", 1996, nr 2, s. 70.

[4] W. Jaroch, *Przestępczość na rynku ubezpieczeń*, Poltext, Warszawa 2002, s. 36.

[5] Definicja E. Kędry, w: S. Stypułkowski, *Przestępstwa ubezpieczeniowe oraz działania podejmowane w celu ich ograniczenia,* „Prawo, Ubezpieczenia, Reasekuracja", Warszawa 1999, nr 12 (36), s. 77–78.

[6] W. Jaroch, *Przestępczość…*, op. cit., s. 6.

odszkodowania, skierowane przeciwko instytucjom finansowym bądź towarzystwom ubezpieczeniowym, w wyniku których generowane są straty po stronie towarzystw ubezpieczeniowych[7].

Analizując przytoczone definicje przestępstwa ubezpieczeniowego należy odnotować, że w literaturze przedmiotu ścierają się dwa stanowiska związane z definiowaniem pojęcia przestępstwa ubezpieczeniowego. Wąskie ujęcie (por. definicja Waldemara Jarocha) mówi, że wyznacznikiem kwalifikacji czynów przestępnych jako przestępstw ubezpieczeniowych jest wykorzystanie umowy ubezpieczeniowej i stosunku ubezpieczeniowego[8]. W ujęciu szerokim, nawiązującym do przytoczonej definicji Tadeusza Rydzeka, katalog przestępstw ubezpieczeniowych jest natomiast rozszerzany na wszystkie przestępstwa godzące bezpośrednio bądź pośrednio w interesy zakładów ubezpieczeń i rynku ubezpieczeniowego[9]. Warto również zauważyć, że przytoczone definicje akcentują głównie sytuacje, w których sprawcą przestępstwa ubezpieczeniowego jest ubezpieczający. Dotyczy to w szczególności definicji CEA. Pomijają one lub spychają na dalszy plan przestępstwa ubezpieczeniowe popełniane przez innych uczestników rynku ubezpieczeń: pracowników zakładów ubezpieczeń, pośredników ubezpieczeniowych (agentów i brokerów) oraz podmioty współpracujące z ubezpieczycielami.

Podobnie jak w piśmiennictwie z zakresu nauk ekonomicznych, również w polskim ustawodawstwie nie ma jednoznacznej definicji przestępstwa ubezpieczeniowego. Odwołując się do przepisów Kodeksu karnego, w kontekście przestępczości ubezpieczeniowej należy przytoczyć przede wszystkim art. 298 § 1: „Kto, w celu uzyskania odszkodowania z tytułu umowy ubezpieczenia, powoduje zdarzenie będące podstawą do wypłaty takiego odszkodowania, podlega karze pozbawienia wolności od 3 miesięcy do lat 5". Ponadto do części oszustw ubezpieczeniowych będzie miał również zastosowanie art. 286§ 1

---

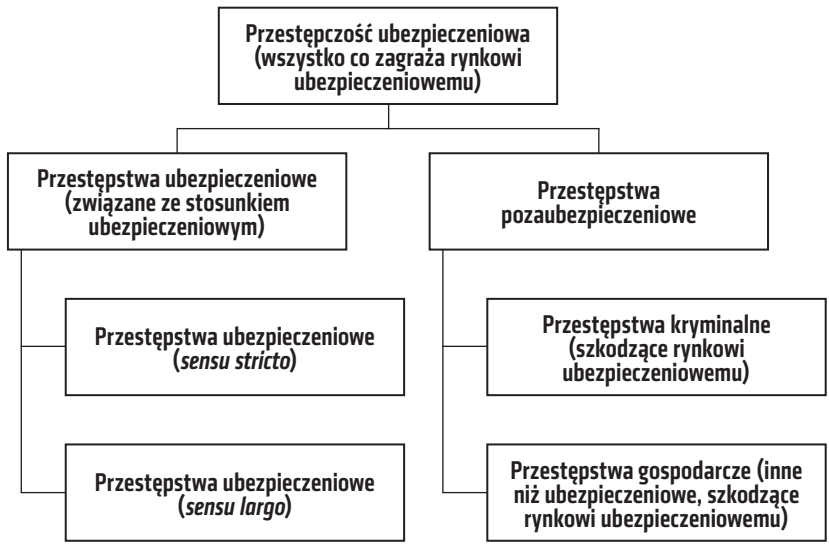
[7] K. Dąbek, A. Kamiński, *Analiza przestępczości ubezpieczeniowej w Polsce na przestrzeni lat 2012–2015*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 2017, nr 488, s. 12

[8] Np. Z. Brodecki, M. Serwach, *Prawo ubezpieczeń gospodarczych,* Zakamycze, Kraków 2005, s. 589.

[9] Szeroka dyskusja na temat pojęcia przestępstwa ubezpieczeniowego, wraz z odniesieniem się do występujących w literaturze dwóch stanowisk związanych z jego definiowaniem w: *Rynek ubezpieczeniowy – zapobieganie przyczynom przestępczości*, red. M. Płonka, B. Oręziak, M. Wielc, Warszawa 2019.

Kodeksu karnego, zgodnie z którym „Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8."

Rysunek 1. Podział przestępczości ubezpieczeniowej



Źródło: D. Miksiewicz, *Charakterystyka przestępczości ubezpieczeniowej w Polsce*, „Studenckie Zeszyty Naukowe", 2015, R. 18, z. 27, s. 45

Dla pełnego przedstawienia pojęcia przestępstwa ubezpieczeniowego zasadne jest odwołanie się w tym miejscu koncepcji do podziału przestępstw ubezpieczeniowych zaproponowanej przez T. Rydzeka, który wyróżnił przestępczość ubezpieczeniową zewnętrzną (oszustwa i wyłudzenia dokonywane przez klientów zakładów ubezpieczeń) i przestępczość ubezpieczeniową wewnętrzną (przestępstwa dokonywane w ramach branży ubezpieczeniowej, np. przywłaszczenie składek, fałszowanie dokumentów, *misseling*)[10]. Warto również przytoczyć kompleksowy podział przestępczości ubezpieczeniowej

[10] T. Rydzek, *Nowe patologie w ubezpieczeniach*, „Wiadomości Ubezpieczeniowe", 1998, nr 3–4, s. 7.

zaproponowany przez Dariusza Miksiewicza, w którym wyróżnia on przestępstwa ubezpieczeniowe oraz przestępstwa pozaubezpieczeniowe (por. rysunek 1). W ramach przestępczości ubezpieczeniowej *sensu stricto* autor wymienia oszustwa ubezpieczeniowe (wprowadzenie w błąd zakładu ubezpieczeń co do faktu zaistnienia zdarzenia ubezpieczeniowego, rozmiaru szkody lub istnienia związku przyczynowego między zdarzeniem a szkodą) i wyłudzenia odszkodowań (celowe spowodowanie zdarzenia ubezpieczeniowego).

3. Sprawcy przestępstw ubezpieczeniowych

Sprawcami przestępstw ubezpieczeniowych mogą być zarówno pojedynczy uczestnicy rynku ubezpieczeniowego, jak i zorganizowane, wyspecjalizowane w przestępczości gospodarczej podmioty i grupy przestępcze. Podobnie jak w przypadku innych przestępstw gospodarczych, głównym motywem działania przestępców ubezpieczeniowych jest chciwość i chęć uzyskania korzyści majątkowych. Wśród innych motywów sprawców przestępstw ubezpieczeniowych wskazuje się również na pewnego rodzaju ogólną awersję do zakładów ubezpieczeń, która powstaje na skutek (nieuzasadnionej w opinii ubezpieczonego) odmowy wypłaty świadczenia w przeszłości[11].

Szacuje się, że największą grupę – ok. 80% sprawców przestępstw ubezpieczeniowych – stanowią klienci zakładów ubezpieczeń[12]. Z reguły osoby takie nie działają w sposób zorganizowany, systematyczny i celowy. Zawierają one umowę ubezpieczenia w dobrej wierze i bez zamiaru popełnienia przestępstwa, a dopuszczając się czynu przestępnego (najczęściej wyłudzenia lub zawyżenia wysokości odszkodowania), korzystają z nadążającej się ku temu okazji. W klasycznej typologii kryminologicznej i klasyfikacji sprawców przestępstw gospodarczych osoby takie przyjęło się określać „przestępcami okazjonalnymi". Bywa, że uważają one swoje działania za zgodne z obowiązującymi normami społecznymi i twierdzą, że jedynie nieznacznie naruszają

[11] J.W. Wójcik, Wyłudzone odszkodowania, „Prawo i Życie", 1999, nr 9, s. 10, za: E. Otocka, *Przestępczość ubezpieczeniowa w Polsce. Formy wyłudzeń,* „Acta Universitatis Lodziensis. Folia Oeconomica", 2008, nr 222, s. 67.

[12] E. Otocka, *Przestępczość ubezpieczeniowa*…, op. cit., s. 67.

porządek prawny. U części przestępców okazjonalnych stwierdza się również brak świadomości łamania przepisów prawa[13].

Rafał Połeć i Marcin Lemańczyk twierdzą, że na rynku ubezpieczeń trudno wyróżnić typowego przestępcę okazjonalnego, gdyż w proceder ten angażują się osoby w różnym wieku, różnej płci i o różnym statusie społecznym i majątkowym[14]. Odnotowują oni również, że sprawcy przestępstw okazjonalnych w swoim postepowaniu kierują się często poczuciem niesprawiedliwości i nierówności w relacjach z ubezpieczycielem. W odczuciu sprawców wyłudzenie odszkodowania bywa postrzegane jako swoista rekompensata za zawyżone składki pobierane przez zakład ubezpieczeń lub w ogóle za całość dotychczas poniesionych kosztów ochrony ubezpieczeniowej (szczególnie w ubezpieczeniach obowiązkowych)[15]. W tym miejscu warto także zauważyć, że nie bez znaczenia dla przestępców okazjonalnych jest – będące główną osią rozważań w niniejszej ekspertyzie – stosunkowo wysokie przyzwolenie społeczne na tego typu działania. Zagadnienie to będzie przedmiotem szczegółowych rozważań w kolejnym punkcie opracowania.

Drugą grupą sprawców przestępstw ubezpieczeniowych są profesjonaliści z branży ubezpieczeniowej i jej bezpośredniego otoczenia. Osoby takie mogą być związane z zakładami ubezpieczeń (pracownicy zakładów ubezpieczeń, pośrednicy ubezpieczeniowi) lub działać niezależnie od nich (dealerzy firm samochodowych, pracownicy warsztatów naprawczych, niezależni rzeczoznawcy, celnicy, fałszerze dokumentów i in. [16]). Szacuje się, że przestępstwa popełniane przez pracowników zakładów ubezpieczeń stanowią ok. 2% ogółu nadużyć, a agenci i brokerzy odpowiadają za ok. 4% przestępstw ubezpieczeniowych[17]. Przestępstwa popełniane przez osoby profesjonalnie związane z branżą ubezpieczeniową są trudniejsze do wykrycia niż

---

[13] *Rynek ubezpieczeniowy – zapobieganie przyczynom przestępczości*, red. M. Płonka, B. Oręziak, M. Wielc, Warszawa 2019.

[14] R. Połeć, M. Lemańczyk, *Przeciwdziałanie przestępczości ubezpieczeniowej w aspekcie jej społecznej akceptacji*, „Studia Oecnomica Posnaniensia", 2015, nr 3 (110), s. 116

[15] Ibid.

[16] E. Czerwiec-Janus, *Wpływ przestępczości ubezpieczeniowej na rozwój rynku*, w: *Bariery rozwoju polskiego rynku ubezpieczeniowego*, red. W. Sułkowska, Wydawnictwo Zakamycze, Kraków 2000, s. 188.

[17] Ibid., s. 189

przestępstwa sprawców okazjonalnych i z reguły wiążą się one z większymi stratami finansowymi dla ubezpieczycieli.

Przestępstwa ubezpieczeniowe popełniane przez profesjonalistów związanych z rynkiem ubezpieczeń wiążą się na ogół z jednym z czterech obszarów[18]:

1. fałszowanie dokumentów (np. podrabianie podpisu, przerabianie dokumentu, wystawianie dokumentów poświadczających nieprawdę);
2. składanie fałszywych oświadczeń;
3. wyłudzanie odszkodowań;
4. *misselling* (proponowanie konsumentowi zakupu usług finansowych nieodpowiadających jego potrzebom lub proponowanie zakupu usług w sposób nieproporcjonalny do ich charakteru[19]).

Profesjonaliści działający na rynku ubezpieczeń coraz częściej dopuszczają się czynów przestępnych w ramach zorganizowanych grup przestępczych, dla których proceder przestępczy jest głównym źródłem dochodu. Bywa, że działania takich grup są bezwzględne i wiążą się z wymuszaniem określonych działań na innych osobach. Wspólny interes uczestników zorganizowanej grupy przestępczej oraz zaangażowanie w jej ramach osób pracujących w różnych podmiotach rynku ubezpieczeń (w tym również w samych zakładach ubezpieczeń) powoduje, że ich wykrycie jest niezwykle trudne i wymaga skoordynowanych działań zakładów ubezpieczeń, organów ścigania i organów nadzoru.

Osoby pracujące w branży ubezpieczeniowej niemal zawsze są świadome nielegalności swojego działania i łamania obowiązujących przepisów prawa. W kontekście tematyki opracowania trzeba podkreślić, że niezgodne z prawem działania tej grupy przestępców nie wiążą się z równie wysokim jak w przypadku sprawców przestępstw okazjonalnych przyzwoleniem społecznym. Podobnie jak w przypadku innych przestępstw gospodarczych trudno jednak w ich przypadku mówić o całkowitym i powszechnym braku akceptacji czy społecznym piętnowaniu sprawców.

Nie sposób dokładnie określić rozmiarów przestępczości ubezpieczeniowej w Polsce. Precyzyjne statystyki odnoszą się – ze zrozumiałych przyczyn – jedynie

---

[18] *Rynek ubezpieczeniowy…*, op. cit.

[19] Art. 24 pkt 2 ust 4. *ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2007 Nr 50 poz. 331).*

do przestępstw ujawnionych, których liczba jest zdecydowane niższa niż liczba przestępstw rzeczywiście popełnionych. Ogólne próby określenia rozmiarów przestępczości ubezpieczeniowej w Polsce można podjąć na podstawie przeciętnych wartości wyłudzeń szacowanych przez CEA – 3% składki przypisanej brutto oraz Insurance Europe – 10% wartości odszkodowań[20]. Opierając się na tych wartościach, można obliczyć, że w dużym przybliżeniu skala wyłudzeń w Polsce może wynosić nawet ok. 1,9–4 mld zł.

Obecnie najbardziej szczegółowe analizy zjawiska przestępczości ubezpieczeniowej na rynku polskim prowadzone są przez Komisję ds. Przeciwdziałania Przestępczości Ubezpieczeniowej działającą w ramach Polskiej Izby Ubezpieczeń. Komisja rokrocznie publikuje raport zawierający analizę ujawnionych przez członków PIU przestępstw ubezpieczeniowych. Najnowszy raport pt. *Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń* został opublikowany w 2018 r.[21] Zgodnie z informacjami zawartymi w raporcie w 2017 r. wartość ujawnionych przestępstw ubezpieczeniowych w Dziale I wynosiła 17,9 mln zł, a w dziale II – 195 mln zł. Wartości te w zestawieniu z szacunkowymi rozmiarami rzeczywistej skali wyłudzeń wskazują, że ujawniane jest jedno na dziesięć (lub przyjmując górną granicę szacunku – jedno na dwadzieścia) przestępstwo ubezpieczeniowe w Polsce.

4. Przyczyny powstawania sytuacji, w których dochodzi do przestępstw na rynku ubezpieczeniowym

Na gruncie teoriopoznawczym wskazuje się, że na występowanie przestępczości ubezpieczeniowej wpływa przede wszystkim zjawisko hazardu ubezpieczeniowego. Pojęcie to utożsamiane jest z zespołem warunków i okoliczności,

[20] D. Miksiewicz, *Charakterystyka przestępczości ubezpieczeniowej w Polsce*, „Studenckie Zeszyty Naukowe", 2015, R. 18, z. 27, s. 46–47.

[21] P. Majewski, *Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń,* Polska Izba Ubezpieczeń, Warszawa 2018.

które mają wpływ na rozmiary i nasilenie danego zdarzenia losowego[22]. Spośród trzech wyróżnianych w piśmiennictwie rodzajów hazardu (por. tabela 1), z perspektywy przestępczości ubezpieczeniowej oraz szczegółowych rozważań prowadzonych w tej części opracowania kluczowe znaczenie ma hazard moralny, określany również jako pokusa nadużycia. Za autorami opracowania *Rynek ubezpieczeniowy – Zapobieganie przyczynom przestępczości* trzeba bowiem wyraźnie podkreślić, że o ile wszystkie okoliczności i zachowania noszące znamiona hazardu są niekorzystne dla zakładów ubezpieczeń, gdyż powodują zwiększenie kosztów związanych z wypłatą odszkodowań i świadczeń, to nie wszystkie one są przejawem przestępczości ubezpieczeniowej[23].

Tabela 1. Rodzaje hazardu ubezpieczeniowego (pokusy nadużyć)

Rodzaj hazardu	Charakterystyka
Hazard fizyczny	Warunki zewnętrzne (o charakterze pozapodmiotowym) lub cechy fizyczne, które mają bezpośredni wpływ na nasilenie przyczyn strat
Hazard motywacyjny (duchowy)	Subiektywna reakcja ubezpieczonego wywołana świadomością istnienia ochrony ubezpieczeniowej, skutkująca postawami motywacyjnymi (np. zaniechanie zapobieganiu ryzyka, niedbałość, nieuwaga)
Hazard moralny	Zespół warunków podmiotowych danej osoby, wyrażających się w negatywnych tendencjach charakterologicznych czy osobowościowych, takich jak nieuczciwość lub skłonność do defraudacji

Źródło: opracowanie własne na podstawie T. Michalski, *Ryzyko…,* op.cit., s. 21–24

Zjawisko przestępczości ubezpieczeniowej – w jej wąskim rozumieniu – wynika przede wszystkim z istnienia hazardu moralnego, a więc z działań (zaniechań) ubezpieczającego, które mają charakter nadużyć umownych lub karnych wynikających ze stosunku ubezpieczenia[24]. Zaznaczyć trzeba jednak, że już samo dążenie do zawarcia umowy ubezpieczenia, jak również jej zawarcie, zmienia sposób zachowania ubezpieczonego (por. hazard motywacyjny). Zasadniczo od momentu zawarcia umowy ubezpieczenia (zaistnienia świadomości ochrony ubezpieczeniowej) ubezpieczający ulega – w różnym stopniu – pokusie nadużycia, kreując potencjalne obszary przestępczości ubezpieczeniowej.

[22] T. Michalski, *Ryzyko w działalności człowieka*, w: *Podstawy ubezpieczeń,* t. 1: *Mechanizmy i funkcje,* red. J. Monkiewicz, Poltext, Warszawa 2000, s. 19.

[23] *Rynek ubezpieczeniowy…*, op. cit.

[24] Ibid.

Na formę oraz rozmiary przestępczości ubezpieczeniowej wpływa wiele czynników o charakterze organizacyjno-prawnym, instytucjonalnym oraz kryminologicznym. W literaturze przedmiotu wskazuje się katalog kluczowych czynników determinujących rozwój i rozmiary przestępczości ubezpieczeniowej[25].

Po stronie ubezpieczycieli do czynników tych należą przede wszystkim:

1. jakość istniejącej infrastruktury informatycznej ubezpieczycieli i instytucji z otoczenia rynku ubezpieczeniowego (np. funkcjonowanie baz danych i systemów ewidencyjnych),
2. przygotowanie zakładów ubezpieczeń do skutecznej walki z przestępczością ubezpieczeniową w formie okazjonalnej i zorganizowanej (dotyczy przygotowania organizacyjnego, technicznego, taktycznego i szkoleniowego),
3. jakość współpracy i wymiany informacji między zakładami ubezpieczeń.

Ponadto w sposób pośredni od ubezpieczycieli zależy również poziom zaawansowania stosowanych fizycznych i teleinformatycznych metod zabezpieczenia i ochrony mienia. Z natury rzeczy kwestie te leżą co prawda po stronie ubezpieczających, jednak na etapie określania warunków przyjęcia do ubezpieczenia danego ryzyka oraz w ramach kształtowania taryfy składek zakłady ubezpieczeń mają istotny wpływ na stosowane w praktyce metody zabezpieczania i ochrony mienia.

Po stronie państwa – a więc m.in. ustawodawcy, organów nadzoru, organów ścigania i instytucji wymiaru sprawiedliwości – czynnikami determinującymi rozmiary przestępczości ubezpieczeniowej są przede wszystkim:

1. skuteczność działania organów śledczych i organów ścigania,
2. poziom dostosowania prawa karnego i procesowego do potrzeb skutecznej walki z przestępczością zorganizowaną.

Warto również nadmienić, że istotnym czynnikiem wpływającym na przestępczość ubezpieczeniową jest jakość i zakres współpracy ubezpieczycieli z organami ścigania.

W tabeli 2 przedstawiono tradycyjne ujęcie katalogu przestępstw ubezpieczeniowych, na które – w mniejszym lub większy stopniu – wpływają

[25] E. Czerwiec-Janus, *Wpływ przestępczości…*, op. cit., s. 186–187.

wskazane czynniki. Rzecz jasna przedstawiony katalog nie jest wyczerpujący, a postęp technologiczny i dynamiczny rozwój rynku ubezpieczeń przejawiający się m.in. powstawaniem nowych produktów ubezpieczeniowych i kanałów ich dystrybucji powodują, że z roku na rok wykrywane są nowe sposoby działania i obszary aktywności przestępców ubezpieczeniowych.

Tabela 2. Katalog typowych przestępstw ubezpieczeniowych

Rodzaj przestępstwa	Charakterystyka
Nadubezpieczenie	Celowe określenie sumy ubezpieczenia powyżej wartości ubezpieczonego mienia
Wielokrotne ubezpieczenie	Jednoczesne zawarcie umów ubezpieczenia z kilkoma zakładami ubezpieczeń w celu pobrania kilku odszkodowań za tę samą szkodę
Zatajenie informacji	Zatajenie istotnych informacji na etapie deklaracji ryzyka przez zawarciem umowy ubezpieczenia albo podanie nieprawdziwych informacji przy zgłaszaniu lub likwidacji szkody
Przekształcenie nieubezpieczonej szkody w roszczenie ubezpieczeniowe	Najczęściej polega na zawarciu umowy ubezpieczenia po powstaniu szkody
Fałszywe szkody	Zgłoszenie roszczenia w związku ze szkodą, która nie miała miejsca
Przestępstwa w trakcie likwidacji szkód	Zawyżenie wartości uszkodzonego lub skradzionego mienia
Umyślne spowodowanie szkody	Celowe uszkodzenie przedmiotu ubezpieczenia przez samego ubezpieczonego lub z wykorzystaniem osoby trzeciej

Źródło: E. Czerwiec-Janus, *Wpływ przestępczości…*, op. cit., s. 180; S. Stypułkowski, *Przestępstwa ubezpieczeniowe…*, op. cit., s. 77–78

W ostatnim czasie szeroką analizę zjawiska przestępczości ubezpieczeniowej, ze szczególnym uwzględnieniem trendów rozwoju zjawiska wyłudzeń, prowadzi organizacja Insurance Europe. W badaniach tej instytucji eksperci z różnych krajów europejskich są pytani o najbardziej popularne i najszybciej rozwijające się metody wyłudzeń w różnych rodzajach ubezpieczeń. Podobne badania – o charakterze pilotażowym – w Polsce przeprowadziła Komisji ds. Przeciwdziałania Przestępczości Ubezpieczeniowej PIU[26]. Syntetyczne podsumowanie najnowszych wyników badań Insurance Europe i PIU przedstawiono w tabeli 3.

[26] P. Majewski, *Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń,* Polska Izba Ubezpieczeń, Warszawa 2018.

Tabela 3. Najczęstsze i najszybciej rozwijające się przestępstwa ubezpieczeniowe w wybranych rodzajach ubezpieczeń

Rodzaj ubezpieczenia	Przestępstwa w Europie (Insurance Europe)	Przestępstwa w Polsce (PIU)
Ubezpieczenia komunikacyjne	**Najczęstsze**	
	• Celowe stłuczki • *Ghost brokers* (oferowanie fałszywych polis ubezpieczeniowych)	• Celowe stłuczki • Zgłaszanie tej samej szkody do różnych ubezpieczycieli
	Najszybciej się rozwijające	
	• Kradzieże aut z systemem bez kluczykowym (autentyczne lub fikcyjne) • Szkody transgraniczne (generowanie szkód komunikacyjnych przez samochody zarejestrowane za granicą)	• Wynajem pojazdu zastępczego (celowe zderzenie starych pojazdów i przedłużanie naprawy
Ubezpieczenia osobowe, NNW	**Najczęstsze**	
	• *Whiplash* (rzekomy, trudny do zdiagnozowania uraz odcinka szyjnego kręgosłupa na skutek wypadku) • Uszkodzenia zębów (nieprawdziwe okoliczności powstania urazu)	• Symulowana trauma powypadkowa, *whiplash* • fikcyjne szkody związane z dbaniem o chodnik przed nieruchomością • Wykorzystywanie kancelarii odszkodowawczych
	Najszybciej się rozwijające	
	• Symulowana trauma powypadkowa	• Roszczenia o utracone dochody na podstawie fałszywych dokumentów • Roszczenia o uszczerbek na zdrowie z podaniem nieprawdziwych okoliczności
Ubezpieczenia mieszkań, szkody majątkowe	**Najczęstsze**	
	• Celowe zalania i sfingowane kradzieże • Rzekoma utrata lub zniszczenie sprzętu elektronicznego, urządzeń mobilnych itp. • Zawyżanie strat	• Umyślne podpalenie • Zawarcie ubezpieczenia po wystąpieniu szkody • Celowe zawyżanie szkody lub zgłaszanie szkody niezwiązanej z wypadkiem ubezpieczeniowym • Fałszywe szkody przepięciowe
	Najszybciej się rozwijające	
	• Kradzieże rowerów (autentyczne)	• Zawyżanie wysokości szkód pożarowych i naprawy uszkodzonego mienia
	Najczęstsze	
	• Sfingowane kradzieże bagażu • Uszkodzenia ciała w fikcyjnych okolicznościach	• Sfingowane kradzieże bagażu
	Najszybciej się rozwijające	
	bd.	• Fałszerstwo dokumentów z wykorzystaniem kradzieży tożsamości

Rodzaj ubezpieczenia	Przestępstwa w Europie (Insurance Europe)	Przestępstwa w Polsce (PIU)
OC inne niż komunikacyjne	• Najszybciej się rozwijające • Wykorzystywanie OC w życiu prywatnym do zgłaszania roszczeń z tytułu szkód na mieniu lub osobie	bd.

Źródło: opracowanie własne na podstawie P. Majewski, *Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń,* Polska Izba Ubezpieczeń, Warszawa 2018

W kontekście rozważanego problemu badawczego warto odnotować, że przestępczość ubezpieczeniowa stanowi problem zarówno z prawnego, jak i z ekonomicznego punktu widzenia[27]. Przyjmując za główną oś rozważań aspekty ekonomiczne, trzeba zauważyć, że głównym motywem kierującym sprawcami przestępstw ubezpieczeniowych jest chęć szybkiego wzbogacenia się, do którego dochodzi kosztem zakładów ubezpieczeń. Rzecz jasna specyfika metody ubezpieczeniowej powoduje, że straty ponoszone na skutek oszustw ubezpieczeniowych przez zakłady ubezpieczeń są przenoszone na ich klientów (ubezpieczających), którzy w ostatecznym rozrachunku są zmuszeni płacić wyższe składki. Można by zatem wnioskować, że każdemu ubezpieczającemu powinno zależeć na maksymalnym ograniczeniu skali zjawiska przestępczości ubezpieczeniowej. Mniejsza skala oszustw przekłada się bowiem na niższy poziom składki płaconej przez uczciwego konsumenta usług ubezpieczeniowych. Wynika z tego, że klienci zakładów ubezpieczeń powinni chętnie zgłaszać zakładom ubezpieczeń oraz uprawnionym organom ścigania znane im przypadki, w których mogło dojść do oszustwa ubezpieczeniowego. Tymczasem w praktyce sytuacje takie rzadko kiedy mają miejsce[28].

Analiza zjawiska przestępczości ubezpieczeniowej w Polsce prowadzi do stwierdzenia, że w rzeczywistości społeczeństwo polskie zachowuje się dokładnie odwrotnie niż wskazuje przedstawione wyżej rozumowanie. Z reguły oszuści ubezpieczeniowi są bowiem kryci, a nawet zachęcani do popełniania przestępstw ubezpieczeniowych przez najbliższe im otocznie. Co więcej, w wielu przypadkach udane (tj. nieujawnione) przestępstwo ubezpieczeniowe cieszy się aprobatą i uznaniem części społeczeństwa. Trzeba

[27] K. Dąbek, A. Kamiński, *Analiza przestępczości…*, op. cit., s. 12
[28] Ibid.

jednak wyraźnie podkreślić, że ta swoista afirmacja przestępstw ubezpieczeniowych z reguły ogranicza się do sprawców okazjonalnych, będących klientami zakładów ubezpieczeń i nie obejmuje sprawców będących profesjonalistami z branży ubezpieczeniowej, a tym bardziej zorganizowanych grup przestępczych.

Próba odpowiedzi na pytanie o przyczyny omawianego fenomenu prowadzi do konstatacji, zgodnie z którą istnieje swoiste przyzwolenie społeczne na dokonywanie przestępstw ubezpieczeniowych. Zdaniem Krystiana Dąbka i Andrzeja Kamińskiego przyzwolenie to wynika z powszechnego przekonania, że zakłady ubezpieczeniowe same dopuszczają się nadużyć polegających na pobieraniu zawyżonych składek ubezpieczeniowych oraz podejmowaniu działań mających na celu jak największe zmniejszenie kwoty wypłacanego odszkodowania[29]. Przyjmując ten tok rozumowania, duża cześć społeczeństwa uważa, że w obliczu nieuczciwości samych zakładów ubezpieczeń oszustwa ubezpieczeniowe są usprawiedliwione. Według Rafała Połecia i Marecina Lemańczyka postawy takie znajdują wyraz w stwierdzeniach mówiących o „oszukiwaniu oszustów" lub „okradaniu złodziei". Przy czym owym „oszustem" i „złodziejem" jest tutaj rzecz jasna zakład ubezpieczeń[30]. Niezgodność z prawem tego typu działań przestępczych, a także ich ekonomiczne konsekwencje dla innych członków wspólnoty ubezpieczeniowej wydają się być w świadomości przeciętnego ubezpieczającego spychane na dalszy plan.

Rozważając kwestie związane ze społeczną akceptacją przestępczości ubezpieczeniowego, warto nadmienić, że zjawisko to w ostatnich latach wydaje się ewoluować. W początkowej fazie rozwoju polskiego rynku ubezpieczeń społeczne przyzwolenie dla sprawców przestępstw ubezpieczeniowych przejawiało się w biernej obojętności, cichym przyzwoleniu oraz braku sprzeciwu wobec popełnianych przez nich czynów przestępnych. Obecnie coraz częściej można spotkać się z afirmacją przestępstw ubezpieczeniowych, a społecznej przyzwolenie na nie przybiera postać aktywnego podżegania do popełnienia przestępstwa oraz pomocnictwa w popełnienie czynów przestępnych (*vide* działalność niektórych kancelarii odszkodowawczych)[31].

---

[29] Ibid., s. 12

[30] R. Połeć, M. Lemańczyk, *Przeciwdziałania przestępczości…*, op. cit., s. 114.

[31] Ibid., s. 115.

Prawdziwości formułowanych twierdzeń w zakresie wysokiego poziomu społecznej akceptacji przestępczości ubezpieczeniowej dowodzą wyniki licznych analiz empirycznych. Przykładowo z badań przeprowadzonych przez Elżbieta Żywucką-Kozłowską wynika, że znaczną szkodliwość społeczną przestępstw ubezpieczeniowych dostrzega zaledwie 10,7% badanych Polaków, 6,8% badanych dostrzega nieznaczną szkodliwość społeczną tego typu działań, a niemal trzy czwarte badanych (72,5%) uważa, że przestępstwa ubezpieczeniowe nie są szkodliwe społecznie[32]. Jeszcze bardziej zatrważające się wyniki badań Tomasza Gulla, w których 51,5% badanych twierdzi, że zna osobiście osobę, która wyłudziła odszkodowanie[33]. Co więcej, jedynie 18,2% z tych osób zadeklarowało, że powiadomiło jakąś instytucję o fakcie zaistnienia takiego zdarzenia. W tych samych badaniach niemal 19% osób twierdzi, że „operatywnym jest ten kto uzyskuje zawyżone odszkodowanie".

Podobnych wyników na temat poziomu społecznej akceptacji przestępczości ubezpieczeniowej dostarczają również badania przeprowadzone przez Marcina Kawińskiego, Piotra. Majewskiego i Damiana Walczaka[34]. Niemal 21% badanych przez ten zespół studentów (sic!) Uniwersytetu Mikołaja Kopernika i Wyższej Szkoły Bankowej w Toruniu uważa, że „przedsiębiorczym jest ten kto uzyskuje od ubezpieczyciela zawyżone lub nienależne odszkodowanie/świadczenie". W tych samych badaniach większość ankietowych stwierdziła, że osoby zgłaszające szkodę z ubezpieczenia rozszerzają jej zakres, aby uzyskać większe odszkodowanie (24% odpowiedzi „bardzo często" i 48% odpowiedzi „często"). Podobnie większość badanych uważa, że osoby zawierające umowę ubezpieczenia często podają nieprawdziwe dane o dotychczasowych szkodach w celu otrzymania korzystniejszej oferty (14% odpowiedzi „bardzo często" i 48% odpowiedzi „często").

---

[32] E. Żywucka-Kozłowska, *Społeczna ocena przestępczości ubezpieczeniowej*, w: *Materiały z polsko-ukraińskiej konferencji*, Lwów 2005, s. 111. Cyt. za: D. Miksiewicz, *Charakterystyka przestępczości…*, op. cit., s. 53. Przywołane badania przeprowadzone zostały na terenie województwa zachodniopomorskiego, pomorskiego i lubuskiego.

[33] T. Gulla, *Raport „Oszustwa ubezpieczeniowe – aspekty społeczne"*, cyt. za: D. Miksiewicz, *Charakterystyka przestępczości…*, op. cit., s. 54.

[34] P. Majewski, *Przyzwolenie społeczne jako istotna przyczyna wyłudzeń w sektorze ubezpieczeń,* materiały konferencyjne, Warszawa 2012, https://www.slideshare.net/SmithNovak/piotr-majewski-przyzwolenie-spoeczne-jako-istotna-przyczyna-wyudze-w-sektorze-ubezpiecze (dostęp: 10.09.2019).

Niezwykle interesujących wyników na temat społecznej postawy Polaków wobec przestępstw na rynku ubezpieczeniowym dostarcza badanie Moralność Finansowa Polaków 2018[35]. W badaniu tym, na pytanie „Czy można usprawiedliwić, gdy ktoś zawyża wartość poniesionych szkód, by uzyskać nienależne odszkodowanie?", ponad jedna piąta ankietowanych odpowiedziała twierdząco (0,6% odpowiedzi „zawsze", 2,5% odpowiedzi „często" oraz 17,6% odpowiedzi „czasem"). W dalszej części badania jako powody usprawiedliwiania wyłudzeń odszkodowań respondenci wskazywali przede wszystkim brak uczciwości ubezpieczycieli (71% badanych), konieczność życiową (16% badanych) oraz standard społeczny (13% badanych). Spośród osób, które w pierwszym pytaniu w żadnym wypadku nie usprawiedliwiały zawyżania wartość poniesionych szkód w celu uzyskania nienależnego odszkodowania, ponad 42% jako przyczynę takiej postawy wskazywało niemoralność takich działań, 49,6% – brak zgodności z prawem, a 8,3% twierdziło, że ryzyko wykrycia takiego przestępstwa jest zbyt duże.

Jako dopełnienie przytaczanych badań warto wskazać jeszcze na analizę poziomu zaufania do zakładów ubezpieczeń przeprowadzoną w ramach Diagnozy Społecznej[36]. W raporcie z 2015 r. 31,8% badanych stwierdziło, że nie ma zaufania do zakładów ubezpieczeń na życie. Jednocześnie 33,5% badanych zadeklarowało umiarkowane zaufanie, a jedynie 1,9% badanych stwierdziło, że ufa zakładom ubezpieczeń (pozostali badani nie mieli zdania). Niemal identyczne wyniki uzyskano w przypadku zakładów ubezpieczeń majątkowych: 31,7% badanych im nie ufa, umiarkowane zaufanie wyraża 29,4% badanych, a zaufanie deklaruje zaledwie 1,6% badanych. Warto jednak odnotować, że na przestrzeni minionych kilkunastu lat (od pierwszego badania w ramach Diagnozy Społecznej) zaufanie Polaków do zakładów ubezpieczeń nieznacznie wzrosło[37].

---

[35] A. Lewicka-Strzałecka, *Moralność finansowa Polaków – raport z badania*, Konferencja Przedsiębiorstw Finansowych w Polsce, Warszawa 2018.

[36] *Diagnoza Społeczna 2015: Warunki i jakość życia Polaków*, red. J. Czapiński, T. Panek, Warszawa, Rada Monitoringu Społecznego 2015, s. 85

[37] Szczegółową analizę zaufania Polaków do zakładów ubezpieczeń prezentuje T. Szumlicz w: *Wzrost zaufania do ZU w świetle Diagnozy Społecznej 2015*, „Wiadomości Ubezpieczeniowe", 2015, nr 3.

Reasumując tę część rozważań, należy stwierdzić, że u podstaw wysokiego poziomu społecznej akceptacji przestępczości ubezpieczeniowej w Polsce leżą trzy główne przesłanki. W pierwszej kolejności jest to niski poziom ogólnej uczciwości Polaków w sferze finansów, będący zarówno pochodną zaszłości historycznych (okres PRL), jak i swoistej moralności społeczeństwa polskiego w sferze gospodarczej. Po drugie, do wysokiego poziomu społecznej akceptacji przestępczości ubezpieczeniowej przyczynia się niski poziom świadomości ubezpieczeniowej będący konsekwencją braku podstawowej wiedzy na temat funkcjonowania rynku ubezpieczeniowego. W efekcie klienci zakładów ubezpieczeń afirmujący przestępstwa ubezpieczeniowe często nie zdają sobie sprawy, że okradanie ubezpieczyciela to tak naprawdę okradanie ich samych i innych klientów (poprzez wzrost składek). Po trzecie, przyczyn wysokiej społecznej akceptacji przestępstw ubezpieczeniowych można się również doszukiwać w stosunkowo niskim zaufaniu Polaków do zakładów ubezpieczeń. Podmioty te są postrzegane jako nieuczciwe, gdyż pobierają zbyt wysokie składki, a następnie zaniżają wypłacane odszkodowania lub odmawiają wypłat odszkodowań itp. W tej sytuacji wspomniane „oszukiwanie oszusta", czy „okradanie złodzieja" w społecznym odbiorze traci znamiona nieuczciwości.

5. Wybrane aspekty zapobiegania przestępczości w obszarze ubezpieczeń

Problematyka przeciwdziałania przestępczości ubezpieczeniowej może być – podobnie jak samo pojęcie przestępczości ubezpieczeniowej – traktowana szeroko lub wąsko. W szerokim ujęciu przeciwdziałanie przestępczości ubezpieczeniowej oznacza zapobieganie wszystkim rodzajom przestępstw godzących w interesy zakładów ubezpieczeń. W ujęciu tym zakres przedmiotowy przeciwdziałania przestępczości ubezpieczeniowej obejmuje zatem działania, takie jak np. zapobieganie kradzieży, zniszczenie mienia czy wypadki komunikacyjne. Przyjęte w dalszej części opracowania wąskie rozumienie problematyki zapobiegania przestępczości ubezpieczeniowej oznacza zawężenie katalogu rozważanych przestępstw ubezpieczeniowych do sytuacji, w których zakłady ubezpieczeń lub inne instytucje rynku ubezpieczeniowego mają realne możliwości ograniczania ich występowania.

W piśmiennictwie wskazuje się, że zapobieganie przestępczości ubezpieczeniowej ma dwojaki charakter: z jednej strony są to działania zmierzające do ograniczania występowania czynów przestępnych (prewencja ubezpieczeniowa), z drugiej strony polega ono natomiast na skutecznym wykrywaniu i ściganiu popełnionych przestępstw[38]. Ramy formalne dla zapobiegnia przestępczości ubezpieczeniowej dają działania legislacyjne państwa w zakresie stanowienia skutecznego prawa prewencyjnego oraz egzekwowanie tego prawa przez stosowne organy. Poprzez stanowienie ogólnych warunków ubezpieczeń istotny wpływ na działania prewencyjne mają również zakłady ubezpieczeń[39].

W klasycznym ujęciu za prewencję ubezpieczeniową uważa się ogół technicznych, ekonomicznych i prawnych środków oddziaływania, których celem jest ograniczanie rozmiarów oraz zmniejszanie prawdopodobieństwa wystąpienia szkód losowych[40]. W ramach tak rozumianej działalności prewencyjnej wymienia się dwie sfery działań: prewencję normatywną oraz prewencję gospodarczą. Prewencja normatywna polega na stosowaniu środków techniczno-ubezpieczeniowych i prewencyjnych w oddziaływaniu na postępowanie ubezpieczającego. W jej ramach wyróżnia się dwie kategorie: 1) zapisy umowy ubezpieczenia (np. zakres odpowiedzialności zakładu ubezpieczeń, instytucja regresu ubezpieczeniowego); 2) środki określające normy postępowania stron umowy ubezpieczenia (np. obowiązki prewencyjne nakładane na ubezpieczającego). Prewencja gospodarcza przejawia się z kolei we wpływie organizacyjnym i finansowym zakładu ubezpieczeń na działalność gospodarczą i operatywną ubezpieczonego. Do najbardziej typowych środków prewencji ekonomicznej zalicza się udział własny, franszyzę redukcyjną i integralną, a także konstrukcję taryfy składek w systemie bonus-malus[41].

---

[38] K. Dąbek, A. Kamiński, *Analiza przestępczości…*, op. cit., s. 13.

[39] W. Jaroch, *Przestępczość…*, op. cit., s. 111.

[40] B. Hadyniak, *Ubezpieczenia jak narzędzie gospodarcze*, w: *Podstawy ubezpieczeń, Mechanizmy i funkcje*, red. J. Monkiewicz, Poltext, Warszawa 2000, s. 66.

[41] Szerzej o ekonomicznych instrumentach przeciwdziałania przestępczości ubezpieczeniowej np. P. Błażejewska, K. Łyda, *Analiza prawnych, ekonomicznych i społecznych aspektów przestępczości ubezpieczeniowej w Polsce*, w: *Ubezpieczenia gospodarcze i społeczne w dobie przemian*, Przegląd Ubezpieczeń 2017, red. M. Cycoń, T. Jedynak, G. Strupczewski, Fundacja Uniwersytetu Ekonomicznego w Krakowie, Kraków.

Współcześnie w związku z dynamicznym rozwojem nowych technologii wydaje się, że do klasycznej klasyfikacji uwzględniającej prawne i ekonomiczne metody przeciwdziałania przestępczości ubezpieczeniowej należy dodać również aspekt technologiczny. Techniczne metody prewencji w rozumieniu autora obejmują ogół rozwiązań teleinformatycznych stosowanych przez ubezpieczycieli w celu ograniczania i wykrywania zjawiska przestępczości ubezpieczeniowej. Należą do nich w szczególności działania, takie jak: cyfrowa analiza zdjęć (zarówno typowych zdjęć zaistniałych szkód, jak i zdjęć satelitarnych), wykorzystanie danych z nowych źródeł (np. Internet rzeczy, telemetria), analiza zbiorów typu big data w celu wykrycia nieprawidłowości, zastosowanie *machine learning* do analizy danych itp.

W innym wymiarze metody przeciwdziałania przestępczości ubezpieczeniowej mogą być również rozpatrywane w ujęciu osobowym i instytucjonalnym. Ujęcie osobowe oznacza koncentrację działań prewencyjnych na pojedynczych osobach – uczestnikach rynku ubezpieczeń. Ujęcie instytucjonalne sprowadza się z kolei do przeciwdziałania przestępczości ubezpieczeniowej w aspekcie organizacyjnym, polega ono na tworzeniu takich ram funkcjonowania instytucji rynku ubezpieczeniowego, które uniemożliwiają lub znacznie ograniczają pole działania przestępców ubezpieczeniowych.

Biorąc pod uwagę podejście produktowe, warto zaznaczyć, że zarysowane powyżej metody prewencji ubezpieczeniowej są na tyle ogólne, że z powodzeniem można je odnieść do większości produktów ubezpieczeniowych. Wspomniane metody prewencji w dużej mierze stanowią również postulaty adresowane do uczestników rynku ubezpieczeniowego. W praktyce na obecnym poziomie rozwoju rynku ubezpieczeniowego zapobiegnie przestępczości ubezpieczeniowej w ramach poszczególnych grup produktowych wymaga jednak wdrożenia specjalistycznych rozwiązań mających na celu przeciwdziałanie lub wykrywanie niepożądanych działań. Nakreślony we wstępie charakter opracowania skłania jednak autora do zaniechania w tym miejscu szczegółowych rozważań produktowych[42]. W ich miejsce zaproponowano syntetyczne zestawienie najczęściej formułowanych postulatów w zakresie wprowadzania metod zapobiegania przestępczości ubezpieczeniowej:

[42] Zainteresowanych tą problematyką odsyłam do innych rozdziałów monografii, a także do publikacji *Rynek ubezpieczeniowy…*, op.cit.

- wprowadzanie przez zakłady ubezpieczeń najnowocześniejszych rozwiązań informatycznych (InsurtTechy, analiza zbiorów big data, sztuczna inteligencja, *machine learning* itp.);
- doskonalenie technik weryfikacji zgłoszonych roszczeń z zewnętrznymi bazami danych (np. bazy NFZ, UFG)[43];
- udoskonalanie procedur wewnętrznych w zakładach ubezpieczeń mających na celu wyeliminowanie przestępstw popełnianych przez pracowników;
- zacieśnianie współpracy zakładów ubezpieczeń z organami ścigania (wymiana informacji);
- korzystanie przez zakłady ubezpieczeń z oferty wyspecjalizowanych firm detektywistycznych;
- doskonalenie systemów bonus-malus oraz szerokie stosowanie franszyz i udziałów własnych.

6. Podsumowanie

We wprowadzeniu do niniejszego opracowania postawiono, a w dalszej części opracowania uzasadniono tezę, zgodnie z którą istotną przesłanką sprzyjającą przestępczości na rynku ubezpieczeniowym jest zjawisko społecznej akceptacji popełniania przestępstw ubezpieczeniowych. W kontekście zapobiegania przestępczości w obszarze ubezpieczeń przyjęcie prawdziwości tak sformułowanej tezy rodzi potrzebę zdefiniowania katalogu działań prowadzących do istotnego zmniejszenia stopnia społecznej akceptacji popełniania przestępstw ubezpieczeniowych.

W przekonaniu autora przeciwdziałanie społecznej akceptacji dla przestępstw ubezpieczeniowych wymaga w pierwszej kolejności szeroko zakrojonej akcji profilaktycznej. Przez profilaktykę rozumie się tutaj przede wszystkim działania edukacyjne mające na celu poprawę świadomości ubezpieczeniowej, rozpowszechnianie wiedzy w zakresie zachowań zgodnych z przepisami

[43] Warto w tym miejscu wskazać na szansę na poprawę wykrywalność przestępstw ubezpieczeniowych w ubezpieczeniach na życie jaką niesie ze sobą planowane pełne uruchomienie Bazy Danych Ubezpieczeniowych UFG.

prawa oraz promowanie postawy braku tolerancji dla sprawców czynów przestępstw ubezpieczeniowych. Istotne jest również informowanie ubezpieczających o ekonomicznych skutkach przestępczości ubezpieczeniowej (wzrost składki). W postulowaną profilaktykę powinny być zaanagażowane wszystkie podmioty rynku ubezpieczeniowego – zarówno same zakłady ubezpieczeń, jak i instytucje rynku ubezpieczeniowego (UFG, PIU, KNF).

Ważnym elementem postulowanej kampanii przeciwko społecznej akcepcji przestępczości ubezpieczeniowej powinny być również szkolenia adresowane nie tylko do zatrudnionych w zakładach ubezpieczeń czy pośredników ubezpieczeniowych, ale również pracowników organów ścigania. Szkolenia te powinny mieć na celu z jednej strony zwiększenie wykrywalności przestępstw ubezpieczeniowych, a z drugiej strony być ukierunkowane na efektywne gromadzenie wartościowego materiału dowodowego na potrzeby postępowań w związku z popełnieniem przestępstwa ubezpieczeniowego.

Skalę społecznej akceptacji dla przestępstw ubezpieczeniowych może ograniczyć również skuteczne działanie wymiaru sprawiedliwości przekładające się na społeczną świadomość dotyczącą nieuchronnej karalności przestępstw ubezpieczeniowych. Co istotne, spełnienie tego postulatu nie ciąży wyłącznie na ustawodawcy, który – co oczywiste – powinien doskonalić istniejące w tym obszarze ramy formalne, ale również na zakładach ubezpieczeń. Jak wskazują Rafał Połeć i Marcin Lemańczyk, w przypadku podejrzenia wyłudzenia lub usiłowania wyłudzenia odszkodowania zakład ubezpieczeń powinien bezwzględnie kierować zawiadomienie o możliwości popełnienia przestępstwa do organów ścigania[44]. Zaniechanie takiego działania i kończenie postępowania w ramach wewnętrznych procedur ubezpieczyciela rodzi bowiem przeświadczenie o bezkarności, a może i nawet zgodności z prawem przestępstw ubezpieczeniowych. Trzeba wyraźnie podkreślić, że konsekwencje prawnokarne, w przypadku przestępczości ubezpieczeniowej w sposób szczególny, powinny pełnić nie tylko funkcje represyjne czy kompensacyjne, ale przede wszystkim wychowawcze[45].

Na zakończenie warto nadmienić, że obok formułowanych wyżej postulatów istotnym elementem przeciwdziałającym społecznej akceptacji dla

[44] R. Połeć, M. Lemańczyk, op. cit., s. 119.
[45] Ibid.

przestępstw ubezpieczeniowych jest propagowanie poszanowania przez zakłady ubezpieczeń norm etycznych i dbałość o dobry wizerunek całego rynku ubezpieczeń. Trzeba przy tym pamiętać, że pojęcie norm etycznych wykracza poza przepisy prawa i obejmuje zarówno stosunki na linii ubezpieczyciel–ubezpieczony, jak również wzajemną konkurencję zakładów ubezpieczeń. Ubezpieczyciele w swojej działalności biznesowej muszą więc pamiętać o uwzględnianiu długiego horyzontu czasowego, mając na uwadze, że poziom zaufania społeczeństwa do rynku ubezpieczeń znajduje bezpośrednie odzwierciedlenie w społecznej akceptacji przestępczości ubezpieczeniowej.

Bibliografia

Brodecki Z., Serwach M., *Prawo ubezpieczeń gospodarczych,* Zakamycze, Kraków 2005.

Czerwiec-Janus E., *Wpływ przestępczości ubezpieczeniowej na rozwój rynku*, w: *Bariery rozwoju polskiego rynku ubezpieczeniowego*, red. W. Sułkowska, Wydawnictwo Zakamycze, Kraków 2000, s. 188.

Dąbek K., Kamiński A., *Analiza przestępczości ubezpieczeniowej w Polsce na przestrzeni lat 2012–2015*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 2017, nr 488, s. 11–20.

Diagnoza Społeczna 2015: Warunki i jakość życia Polaków, red. J. Czapiński, T. Panek, Warszawa, Rada Monitoringu Społecznego 2015.

Hadyniak B., *Ubezpieczenia jak narzędzie gospodarcze*, w: *Podstawy ubezpieczeń, Mechanizmy i funkcje*, red. J. Monkiewicz, Poltext, Warszawa 2000, s. 66.

Jaroch W., *Przestępczość na rynku ubezpieczeń,* Poltext, Warszawa 2002.

Lewicka-Strzałecka A., *Moralność finansowa Polaków – raport z badania*, Konferencja Przedsiębiorstw Finansowych w Polsce, Warszawa 2018.

Majewski P., *Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń,* Polska Izba Ubezpieczeń, Warszawa 2018.

Majewski P., *Przyzwolenie społeczne jako istotna przyczyna wyłudzeń w sektorze ubezpieczeń*, materiały konferencyjne, Warszawa 2012, https://www.slideshare.net/SmithNovak/piotr-majewski-przyzwolenie-spoeczne-jako-istotna-przyczyna-wyudze-w-sektorze-ubezpiecze (dostęp: 10.09.2019).

Michalski T., *Ryzyko w działalności człowieka*, w: *Podstawy ubezpieczeń,* t. 1: – *Mechanizmy i funkcje,* red. J. Monkiewicz, Poltext, Warszawa 2000, s. 19.

Miksiewicz D., Charakterystyka przestępczości ubezpieczeniowej w Polsce, „Studenckie Zeszyty Naukowe", 2015, R. 18, z. 27, s. 42–58.

Otocka E., *Przestępczość ubezpieczeniowa w Polsce. Formy wyłudzeń,* „Acta Universitatis Lodziensis. Folia Oeconomica", 2008, nr 222, s. 63–74.

Połeć R., Lemańczyk M., *Przeciwdziałanie przestępczości ubezpieczeniowej w aspekcie jej społecznej akceptacji*, „Studia Oecnomica Posnaniensia", 2015, nr 3(110), s. 111–121.

Rydzek T., *Nowe patologie w ubezpieczeniach*, „Wiadomości Ubezpieczeniowe", 1998, nr 3–4, s. 7.

Rydzek T., *Przestępczość ubezpieczeniowa w świetle teorii i praktyki*, „Prawo Asekuracyjne" 1996, nr 2, s. 70.

Rynek ubezpieczeniowy – zapobieganie przyczynom przestępczości, red. M. Płonka, B. Oręziak, M. Wielc, Warszawa 2019.

Stypułkowski S., *Przestępstwa ubezpieczeniowe oraz działania podejmowane w celu ich ograniczenia,* „Prawo, Ubezpieczenia, Reasekuracja", Warszawa 1999, nr 12(36), s. 77–78.

Szumlicz T., *Wzrost zaufania do ZU w świetle Diagnozy Społecznej 2015*, „Wiadomości Ubezpieczeniowe", 2015, nr 3, s. 3–19.

Ubezpieczenia gospodarcze i społeczne w dobie przemian, Przegląd Ubezpieczeń 2017, red. M. Cycoń, T. Jedynak, G. Strupczewski, Fundacja Uniwersytetu Ekonomicznego w Krakowie, Kraków.

Wójcik J.W., *Wyłudzone odszkodowania*, „Prawo i Życie", 1999, nr 9.

Żywucka-Kozłowska E., *Społeczna ocena przestępczości ubezpieczeniowej*, w: Materiały z polsko-ukraińskiej konferencji, Lwów 2005.

ROZDZIAŁ V

Metody i instrumenty zapobiegania przestępczości w organizacji realizującej zadanie kontroli ruchu drogowego

ARTUR MEZGLEWSKI[1]

1. Wprowadzenie

Zarówno prawo, jak i technologia mogą w znacznym stopniu przyczynić się do zapobiegania przyczynom przestępczości. W niniejszym opracowaniu zostaną przedstawione propozycje rozwiązań prawnych oraz technologicznych, które mogą posłużyć do zapobiegania przyczynom przestępczości w specyficznej organizacji, jaką jest policja. Proponowane rozwiązanie technologiczne dotyczyć będzie wprowadzenia obowiązku nagrywania interwencji drogowych za pomocą kamer samochodowych oraz kamer nasobnych. Samo wprowadzenie powyższego rozwiązania technologicznego nie usprawni organizacji w działaniu. Konieczne jest ponadto wprowadzenie odpowiednich ram organizacyjnych związanych ze stosowaniem proponowanych urządzeń, a także zmiana otoczenia prawnego poprzez nowelizację obowiązujących przepisów administracyjnych oraz karnych.

W tym celu w rozdziale pierwszym ukazano model zarządzania tego rodzaju instytucją, a także jego mankamenty. W rozdziale drugim przedstawiono efekty badań aktowych. Przedmiotem kwerendy było poszukiwanie nieprawidłowości w pracy przedmiotowej instytucji oraz analiza ich przyczyn. W rozdziale trzecim zaprezentowanno wątki komparatystyczne, w rozdziałach czwartym i piątym zaś sformułowano wnioski *de lege lata* oraz *de lege ferenda*.

[1] Profesor nauk prawnych. Afiliacja: Akademia Sztuki Wojennej w Warszawie.

2. Model zarządzania w policji oraz jego mankamenty

Jedną z istotniejszych kwestii w zarządzaniu ludźmi w organizacji są zadania związane z kierowaniem i kontrolą. W teorii zarządzania oraz w nauce administracji wyróżnia się różne style kierowania. Współcześnie podkreśla się, że styl kooperatywny zwiększa efektywność działania i lepiej motywuje urzędnika. Styl ten zakłada, że dobrze przygotowani oraz wykształceni urzędnicy mają świadomość odpowiedzialności oraz zdolność do samokontroli[2]. Niezależnie jednak od stopnia wykształcenia i przygotowania kadry urzędniczej działalność zespołu ludzkiego wchodzącego w skład organizacji poddawana jest kontroli. Aby kontrola odniosła swój skutek w postaci oceny i porównania tego, co jest z tym, co powinno być, najpierw musi być zapewniony sprawnie działający mechanizm informacyjny[3].

W nauce administracji zakłada się określony model administrowania polegający na tym, że w procesie przygotowywania decyzji uczestniczy wiele podmiotów, jednakże formalnie decyzje, mające wpływ na prawa i obowiązki obywateli, podejmowane są przez osobę piastującą funkcję organu administracji lub inny podmiot posiadający kompetencje (upoważnienie)[4]. W ten sposób działa administracja publiczna w sferze prawa administracyjnego. Istnieją jednak organy administracji wyposażone we władztwo publiczne wykraczające po sferę prawa administracyjnego, w których każdy urzędnik (funkcjonariusz) podejmuje decyzje[5] – czyniąc to w porozumieniu lub nawet bez porozumienia z kadrą kierowniczą organizacji. Do takich organów należy m.in. Policja. Policja jest organem administracji publicznej, a Komendant Główny Policji jest centralnym organem administracji rządowej, właściwym w sprawach ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa

[2] Zob. E. Knossala, *Zarys nauki administracji*, Zakamycze 2006, s. 155.

[3] Jak stwierdził E. Knossala, „rdzeniem systemu kontrolnego jest mechanizm informacyjny". Ibid., s. 232.

[4] Ibid., s. 160. Przez kompetencje należy rozumieć „prawo do wiążącego ustalania czyichś zachowań w sferze publicznej". Zob.W. Góralczyk jr, *Kierownictwo w prawie administracyjnym*, Warszawa 2016, s. 54.

[5] Chodzi o decyzje w szerokim tego słowa znaczeniu, polegające na wyborze określonej alternatywy.

i porządku publicznego[6]. Jednocześnie jednak Policja jest organem porządku publicznego, posiadającym prerogatywy w zakresie ścigania, zapobiegania oraz zwalczania wykroczeń oraz przestępstw oraz ścigania ich sprawców[7].

Funkcjonariusze Policji – w szczególności działając w obszarze ruchu drogowego – podejmują decyzje na miejscu zdarzeń drogowych o zastosowaniu określonych sankcji wobec uczestników ruchu drogowego, a podstawy prawne tych interwencji zostały określone w przepisach postępowania w sprawach o wykroczenia oraz w przepisach postępowania karnego – rzadziej w przepisach o charakterze administracyjnym.

Rzetelność interwencji policjantów na miejscu zdarzeń drogowych stanowi przedmiot badań naukowych. Wykazują one, że interwencje te mogą nosić cechy niedopełnienia obowiązków lub przekroczenia uprawnień. W związku z procedurą przeprowadzania kontroli drogowej nieprawidłowości te mogą polegać na:

- odstąpieniu od wykonywania czynności służbowych, które obowiązany był wykonać w związku ze stwierdzeniem popełnienia wykroczenia drogowego (np. odstąpienie od zatrzymania prawa jazdy);
- przyjęciu korzyści majątkowej w związku z odstąpieniem od ukarania mandatem karnym za wykroczenie drogowe;
- przyjęciu korzyści majątkowej w zamian za odstąpienie od wykonywania prawnych czynności służbowych (np. odstąpienie od badania na zawartość alkoholu w organizmie);
- nakłanianiu;
- poświadczeniu nieprawdy w mandacie karnym w zakresie kwalifikacji prawnej wykroczenia;
- przerobieniu mandatu karnego (np. poprzez obniżenie kwoty);
- bezzasadnym ukaraniu mandatem karnym;
- niewydaniu ukaranemu mandatu karnego,
- poświadczeniu nieprawdy w dokumentacji związanej ze zdarzeniem drogowym;

---

[6] Zob. S. Pieprzny, *Administracja bezpieczeństwa i porządku publicznego*, Rzeszów 2012, s. 99.

[7] Art. 1 ust. 2 pkt 4 *ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jedn.: Dz.U. 2019 poz. 161 ze zm.);* art. 17 § 1 *ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2019 poz. 1120 ze zm.)*

- podżeganieu do poświadczenia nieprawdy w protokole użycia alkomatu;
- działaniach w celu osiągnięcia korzyści majątkowej i wprowadzenia w błąd co do ważności posiadania polisy ubezpieczeniowej OC i wyłudzenia kwoty majątkowej;
- fałszywym zapewnieniu o możliwości uregulowania należności za kredytowany mandat w drodze bezpośredniej zapłaty;
- przywłaszczeniu na własne cele kwoty uzyskanej z mandatu karnego gotówkowego;
- niedopełnieniu obowiązku w zakresie prowadzenia bloczka mandatów karnych;
- kradzieży podczas kontroli drogowej;
- podżeganiu innych funkcjonariuszy do wspólnego zaboru pieniędzy podczas kontroli drogowej;
- bezzasadnym lub nadmiernym użyciu środków przymusu bezpośredniego;
- pobiciu lub (i) spowodowaniu uszczerbku na zdrowiu;
- nierzetelnej obsłudze zdarzenia drogowego (niedokonanie wszystkich czynności na miejscu wypadku drogowego);
- niewłaściwym zachowaniu (arogancja);
- bezzasadnym przeprowadzeniu kontroli drogowej[8].

Powyższe badania objęły wszystkie sprawy (893) dotyczące przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy Policji w latach 1999–2006. Dają one pewną wiedzę o rzeczywistości, jednakże jest to wiedza jednostronna. Na podstawie badań aktowych oraz aktywności w zakresie monitorowania procesów stosowania prawa przez organy władzy publicznej należy stwierdzić, iż postępowania przygotowawcze przeciwko funkcjonariuszom Policji wszczynane są zasadniczo tylko w przypadkach, gdy przestępcza działalność funkcjonariusza prowadzona była na szkodę państwa albo też narażała państwo na uszczerbek finansowy. Natomiast w przypadkach zgłaszanych przez obywateli naruszeń, które dokonywane były

[8] Za D. Mocarska, *Przekroczenie uprawnień lub niedopełnienie obowiązków przez funkcjonariuszy policji w reakcji na wykroczenie drogowe – prezentacja badań kryminologicznych*, w: *Współdziałanie organów bezpieczeństwa i porządku publicznego w zakresie zapobiegania i zwalczania wykroczeń*, red. I. Nowicka, A. Sadło-Nowak, A. Tunia, Lublin 2012, s. 257–270.

na szkodę uczestników ruchu postępowania, zasadniczo nie są wszczynane lub są wszczynane i umarzane w fazie *in rem*[9]. Dlatego też zasadna jest analiza akt postępowań karnych i wykroczeniowych pod kątem oceny praworządności i legalności prowadzonych kontroli ruchu drogowego.

3. Wyniki kwerendy aktowej

W wyniku przeprowadzonej kwerendy aktowej oraz analizy kilkudziesięciu postępowań karnych i wykroczeniowych dostrzeżono następujące uprawdopodobnione delikty funkcjonariuszy Policji w związku z przeprowadzaniem przez nich kontroli ruchu drogowego. Stwierdzono ponadto, że w zakresie kontroli prędkości w ruchu drogowym – ze względu na brak zastosowania bardziej zaawansowanych technologicznie urządzeń pomiarowych, które posiadałyby funkcję rejestracji pomiaru, stan faktyczny ustalany jest jednie na podstawie „relacji" funkcjonariuszy Policji dokonywanych najczęściej po upływie kilku miesięcy od dokonania czynu.

3.1. Sprawa II W 236/15 (Sąd Rejonowy w Oświęcimiu)

Funkcjonariusze Komendy Powiatowej Policji w Oświęcimiu zatrzymali do kontroli drogowej znanego im osobiście kierującego samochodem osobowym i poinformowali go, że popełnił on w ciągu siedmiu minut sześć wykroczeń (sześć niesygnalizowanych kierunkowskazem zmian kierunku jazdy). Wspominane manewry miał on rzekomo wykonywać w dniu 13 grudnia 2014 r.

[9] Jako przykłady można wskazać zawiadomienia kierowane do organów ścigania przez Stowarzyszenie Prawo na Drodze: w sprawie 2 Ds 1300.2018 w Prokuraturze Rejonowej w Kraśniku o czyny z art. 231 § 1 k.k., 271 § 1 k.k., 239 § 1 k.k., w sprawie 2 Ds 366.2019 w Prokuraturze Rejonowej w Puławach o czyny z art. 231 § 1 k.k., 233 § 1 k.k., w sprawie RSOW 2879/17 w Komendzie Miejskiej Policji w Olsztynie o czyn z art. 97 k.w., w sprawie RSOW-34-13 RKP w Komendzie Powiatowej Policji w Kraśniku o czyny z art. 86 § 1 k.w. oraz art. 92a k.w., sprawa DS 1544/15 w Prokuraturze Rejonowej w Myśliborzu o czyn z art. 231 § 1 k.k., w sprawie PR Ds 40/16 w Prokuraturze Rejonowej w Pyrzycach o czyn a art. 231 § 1k.k., w sprawie PR Ds 282.2016 w Prokuraturze w Białogardzie o czyn z art. 231 § 1 kk., w sprawie PR Ds 730.2017 w Prokuraturze Rejonowej w Kolbuszowej o czyny z art. 228 § 3 k.k. oraz 229 § 3 k.k.

na ul. Rynek w miejscowości Zator. Jeden z funkcjonariuszy zaproponował kierowcy sześć mandatów karnych na łączną kwotę 1000 zł. Kierujący odmówił przyjęcia mandatów, oświadczając, że żadnego wykroczenia nie popełnił.

Jeszcze tego samego dnia funkcjonariusz Policji sporządził obszerną notatkę urzędową, w której opisał jedenaście (a nie sześć) wykroczeń popełnionych rzekomo przez kierującego – a wśród nich m.in. niezastosowanie się do poleceń osoby kierującej ruchem w celu uniknięcia kontroli oraz niezatrzymywanie się na znaku STOP (kilkukrotnie). Ponadto w ramach przeprowadzonych czynności wyjaśniających o sygnaturze RSOW-235/2014/Z przesłuchano w charakterze świadków policjantów, którzy dokonywali kontroli drogowej. Policjanci ci fałszywie potwierdzili popełnienie zarzucanych kierującemu czynów oraz to, że nie proponowano obwinionemu żadnego mandatu karnego.

W dniu 11 lutego 2015 r. został skierowany wniosek o ukaranie do Sądu Rejonowego w Oświęcimiu, a w dniu 25 marca 2015 r. (sygn. akt II W 236/15) sąd ten wydał wyrok nakazowy uznający kierującego za winnego popełnienia wszystkich jedenastu wykroczeń, orzekając karę 2000 zł grzywny oraz zakaz prowadzenia wszelkich pojazdów mechanicznych na okres 6 miesięcy za stworzenie realnego zagrożenia w ruchu drogowym[10].

Przebieg przedmiotowej kontroli drogowej został nagrany przez kierującego na nośniku zainstalowanym w telefonie komórkowym. Z nagrania wynika, że policjant nałożył na kierującego sześć mandatów karnych za sześć, a nie za jedenaście wykroczeń – przy czym kierujący kwestionował popełnienie jakiegokolwiek wykroczenia[11]. Nagranie zdecydowanie zaprzecza wersji policjantów, którzy twierdzili, że mandaty karne nie były proponowane. Policjanci z KPP w Oświęcimiu zastosowali zatem retorsję za asertywną postawę kierującego w postaci obwinienia go za pięć dodatkowych wykroczeń, w tym za niestosowanie się do poleceń osoby kierującej ruchem w celu uniknięcia kontroli – co zaskutkowało wydaniem przez Sąd Rejonowy zakazu prowadzenia pojazdów. Autor opracowania ustalił ponadto, iż w momencie dokonywania kontroli drogowej istniał konflikt pomiędzy policją a kierującym.

[10] Zob. akta sprawy o sygnaturze II W 236/15 prowadzonej przez Sąd Rejonowy w Oświęcimiu.

[11] Kopia nagrania jest w posiadaniu autora niniejszego opracowania. Autor był też na miejscu zdarzenia i przeanalizował wersję zdarzenia prezentowaną przez policjantów w zeznaniach i notatce. Wersja ta jest z pewnością niewiarygodna.

W związku z powyższym jest wysoce prawdopodobne (prawdopodobieństwo graniczące z pewnością), że funkcjonariusz Policji z Komisariatu Policji w Zatorze popełnił przestępstwo z art. 231 § 1 Kodeksu karnego[12] (dalej k.k.), a także szereg przestępstw przeciwko Wymiarowi Sprawiedliwości.

3.2. Sprawa VI W 135/19 (Sąd Rejonowy w Lesku)

Przedmiotowa sprawa jest jeszcze w toku na etapie rozpatrywania apelacji. Przedmiotem postępowania są zarzuty dotyczące znacznego przekroczenia prędkości w obszarze zabudowanym (art. 92a k.w.) oraz niezastosowania się do sygnału do zatrzymania wydanego przez funkcjonariuszy patrolu statycznego z KPP w Ustrzykach Dolnych (art. 92 § 1 k.w.[13]). W sprawie istotne jest przede wszystkim to, iż kierujący pojazdem w momencie zdarzenia znajdował się w poważnym konflikcie z funkcjonariuszem dokonującym kontroli – a wielu świadków potwierdziło fakt, że funkcjonariusz ten publicznie odgrażał się wcześniej, że zatrzyma obwinionemu prawo jazdy. I faktycznie tak się stało.

Analizując akta, nie da się – bez przeprowadzenia określonych dowodów – stwierdzić, czy i ewentualnie o ile kilometrów na godzinę kierujący przekroczył prędkość. Z materiału dowodowego wynika, że funkcjonariusz nie posiadał szkoleń w zakresie obsługi urządzenia pomiarowego oraz że pomiar został wykonany w sposób niezgodny z zasadami dotyczącymi używania urządzeń celowniczych (w pozycji siedzącej, na fotelu kierowcy, bez użycia statywu i lunety kierujący trafił z odległości ponad 160 m w tablice rejestracyjną pędzącego auta i bez minimalnego nawet wzruszenia ręką przytrzymał pomiar – do czasu, aż urządzenie na podstawie kilkudziesięciu pomiarów odległości obliczy średnią prędkość pojazdu na mierzonym odcinku). Da się ponadto stwierdzić, że w podanych przez funkcjonariuszy okolicznościach nie mogło dojść do wydania prawidłowego sygnału do zatrzymania, a tym samym o popełnieniu wykroczeniu z art. 92 § 1 k.w. nie mogło być mowy. A zatem – także i w tym przypadku – z duża dozą prawdopodobieństwa można

[12] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn.: Dz.U. 2018 poz. 1600 ze zm.).*
[13] *Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (tekst jedn.: Dz.U. 2019 poz. 821 ze zm.).*

twierdzić, że funkcjonariusze popełnili przestępstwa z art. 231§ 1 k.k. oraz szereg przestępstw przeciwko Wymiarowi Sprawiedliwości.

3.3. Sprawa II W 210/18 (Sąd Rejonowy w Kraśniku)

Sprawa dotyczyła sprawstwa kolizji, której uczestnikami byli kierujący pojazdem osobowym oraz ciągnikiem rolniczym. Kierujący ciągnikiem rolniczym marki T-25 (od którego wyraźnie czuć było alkohol), włączając się do ruchu, wyjechał z drogi gruntowej na drogę powiatową, nie ustępując pierwszeństwa przejeżdżającemu samochodowi osobowemu marki Opel Astra – czym spowodował zagrożenie w ruchu drogowym, gdyż kierujący Oplem Astrą w celu uniknięcia zderzenia z ciągnikiem został zmuszony do wykonania gwałtownego manewru obronnego (skrętu na lewy pas jezdni) i z tego powodu stracił panowanie nad pojazdem i uderzył w ogrodzenie.

Funkcjonariusze KPP w Kraśniku, którzy przybyli na miejsce zdarzenia, nie zabezpieczyli śladów zdarzenia (a jeden z nich wręcz je zamazywał nogą) i oskarżyli niewinnego uczestnika ruchu – co później zostało potwierdzone procesowo wyrokiem. W dodatku funkcjonariusze ci przekroczyli swoje uprawnienia poprzez przeprowadzenie badania trzeźwości uczestnika kolizji bez udziału świadków, w ukryciu (za pojazdem służbowym) – w sytuacji gdy istniało uzasadnione podejrzenie, że ów uczestnik prowadził po drodze publicznej pojazd, będąc w stanie nietrzeźwości – popełniając tym samym przestępstwo z art. 178a § 1 k.k – w szczególności, że przeprowadzenia badania żądali inni uczestnicy zdarzenia drogowego, którzy zauważyli, że kierujący jest nietrzeźwy. Funkcjonariusze jednocześnie nie dopełnili swoich obowiązków poprzez zaniechanie przeprowadzenia badania trzeźwości w sposób określony w art. 47 ust. 1 i 2 ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi[14] oraz przepisami Rozporządzenia Ministra Zdrowia z dnia 11 grudnia 2015 r. w sprawie badań na zawartość alkoholu w organizmie[15], określającymi sposób przeprowadzania badań trzeźwości dla celów dowodowych – w efekcie

[14] *(Tekst jedn.: Dz.U. 2018 poz. 2137).*
[15] (*Dz.U. poz. 2153*).

czego – pomimo uzasadnionego podejrzenia – nie została ustalona dla celów postępowania dowodowego zawartość alkoholu w organizmie kierującego ciągnikiem rolniczym.

Popełnienie powyższych czynów jest bezdyskusyjne, natomiast różnoraka ocena prawna może wynikać z faktu, iż przepisy wykonawcze wydane przez Komendanta Głównego Policji w przedmiocie obowiązku wykonywania badań trzeźwości urządzeniami dowodowymi nie respektują wymogów prawa powszechnie obowiązującego[16].

3.4. Sprawa II W 35718 (Sąd Rejonowy w Kraśniku)

Podczas kontroli drogowej w dniu 18 lutego 2018 r. funkcjonariusz KMP w Lublinie zarzucił kierującemu przekroczenie dozwolonej prędkości o 45 km/h. Tego samego dnia funkcjonariusz ten, będąc przesłuchiwany w Komendzie Miejskiej Policji (czynności wyjaśniające o sygnaturze RSOW-526/18) w charakterze świadka i pouczony o odpowiedzialności karnej za składanie fałszywych zeznań, zeznał, że „W dniu 18 lutego 2018 r. (…) dokonałem pomiaru prędkości pojazdu Kia Ceed (…). Pomiaru dokonałem z odległości 242,9 m. (…) nadmieniam, iż pojazd kierującego był jedynym pojazdem na drodze podczas wykonywania pomiaru. Z obu kierunków podczas pomiarów nie jechały żadne pojazdy". Policjant powyższe zeznania przeczytał, podpisał oraz nie wniósł do nich żadnych uzupełnień lub poprawek.

W dniu 26 czerwca 2018 r. funkcjonariusz ten, będąc ponownie przesłuchiwany w Sądzie Rejonowym w Kraśniku podczas rozprawy w sprawie o sygnaturze II W 357/18 (karta 2) w charakterze świadka, zeznał, że „Kierujący jechał z pasażerką – chyba matką (…) Podczas pomiaru ani przed kierującym, ani za kierującym nie było innych pojazdów. Z nikim się też nie wymijał. W czasie dokonywania pomiaru jechał sam". Tego samego dnia i na tej samej rozprawie (karta 8), odpowiadając na pytanie obwinionego, świadek ten, że „(…) w tym przypadku nie było żadnych innych pojazdów,

[16] Zob. *Zarządzenie nr 30 Komendanta Głównego Policji z dnia 22 września 2017 r. w sprawie pełnienia służby na drogach (Dz. Urz. KGP, poz. 64)*.

pan znajdował się sam na drodze.(…) w tym przypadku na drodze znajdował się tylko jeden pojazd obwinionego".

Po wypowiedzeniu przez świadka powyższych słów, obrońca obwinionego złożył do akt postępowania fotograficzny materiał dowodowy, z którego wynika, że w momencie dokonywania pomiaru po przeciwległym pasie ruchu jechały cztery samochody – jeden za drugim, które musiały utrudnić lub uniemożliwić pomiar. Z załączonego materiału wynika w sposób niezbity, że funkcjonariusz zeznał nieprawdę co do okoliczności mających znaczenie dla sprawy.

3.5. Sprawy o przekroczenie dozwolonej prędkości z art. 92a k.w.

W ramach przeprowadzonej kwerendy akt postępowań wykroczeniowych ustalono znaczną liczbę spraw bliźniaczo do siebie podobnych, o jednorodnym przedmiocie postępowania (zarzut przekroczenia dozwolonej prędkości w ruchu drogowym) oraz o zbliżonym do siebie przebiegu postępowania. Są to sprawy: II W 3994/16 w Sądzie Rejonowym w Tomaszowie Lubelskim, V W 576/16 w Sądzie Rejonowym dla Warszawy Woli w Warszawie, VI W 384/17 w Sądzie Rejonowym w Tarnowskich Górach (Wydział Zamiejscowy w Piekarach Śląskich), II W 234/17 w Sądzie Rejonowym w Łukowie, II W 319/17 w Sądzie Rejonowym w Nidzicy, II 45/16 w Sądzie Rejonowym w Zambrowie, II W 758/15 w Sądzie Rejonowym w Gorlicach, II W 398/16 w Sądzie Rejonowym w Gostyniu, XII W 3021 w Sądzie Rejonowym w Toruniu, II W 731/15 w Sądzie Rejonowym w Kościanie, IV 185/16 w Sądzie Rejonowym w Częstochowie, II 736/16 w Sądzie Rejonowym w Kozienicach, II W 256/16 w Sądzie Rejonowym w Lubartowie, II W 1680/15 w Sądzie Rejonowym w Łęczycy, II W 783/17 w Sądzie Rejonowym w Kozienicach, II W 691/15 w Sądzie Rejonowym w Myśliborzu, II W 555/17 w Sądzie Rejonowym w Gryficach, II W 621/15 w Sądzie Rejonowym w Zambrowie, II 490/16 w Sądzie Rejonowym w Pile, VII W 961/17 w Sądzie Rejonowym w Piotrkowie Trybunalskim, II W 497/17 w Sądzie Rejonowym w Lesznie, II W 327/17 w Sądzie Rejonowym w Pułtusku, II W 1016/17 w Sądzie Rejonowym w Legionowie, III W 1540/16 w Sądzie Rejonowym Lublin-Zachód w Lublinie, II W 943/17 w Sądzie Rejonowym w Gliwicach, II W 1083/17

w Sądzie Rejonowym w Dębicy, II W 501/18 w Sądzie Rejonowym w Kielcach, II 311/17 w Sądzie Rejonowym w Białogardzie, II W 556/16 w Sądzie Rejonowym w Staszowie, II W 369/16 w Sądzie Rejonowym w Miechowie, II W 715/17 w Sądzie Rejonowym w Tarnobrzegu, II W 546/16 w Sądzie Rejonowym w Wągrowcu.

Pośród nich można wyodrębnić te, w których narzędziem, którym dokonano pomiaru prędkości, był ręczny (radarowy lub lidarowy) miernik prędkości oraz te, w których do mierzenia prędkości zastosowano prędkościomierz kontrolny (tzw. wideorejestrator). W przypadku tych pierwszych sądy pozbawione były szans na obiektywne rozpatrzenie sprawy poprzez dotarcie do prawdy materialnej – i albo ograniczały postępowanie dowodowe do źródeł osobowych, albo powoływały biegłego z zakresu pomiarów prędkości. Należy jednak zauważyć, iż wywołanie dowodu z opinii biegłego w przypadku braku zabezpieczonego zapisu bądź nagrania pomiaru miało się z celem. W takich przypadkach opinie ograniczały się bowiem do ogólnikowych stwierdzeń i hipotetycznych założeń. Inaczej rzecz się miała z pomiarami dokonanymi przy użyciu prędkościomierza kontrolnego. Wprawdzie prędkościomierz kontrolny nie dokonuje pomiaru prędkości pojazdu kontrolowanego, jednakże na podstawie zarejestrowanego na cyfrowym nośniku przebiegu zdarzenia, powołany był w stanie „na piechotę" obliczyć jego prędkość.

Wspólną cechą wszystkich tych spraw był brak rzetelnie udokumentowanego przez oskarżyciela publicznego zarzucanego czynu. W efekcie wydłużało to proces i generowało koszty. Należy zauważyć, iż nawet dołączenie do wniosku o ukaranie nagrania z kamerki samochodowej znacznie ułatwiałoby sprawę, gdyż większość urządzeń tego typu posiada wszystkie elementy potrzebne do rejestracji służby policji, np. podświetlanie podczerwone do nagrywania zdarzeń w nocy, wykrywanie ruchu, aby ograniczyć zużycie pamięci, nagrywanie prędkości pojazdu itp.

4. Ujęcie komparatystyczne

Stosowanie w ramach służby drogowej przez funkcjonariuszy Policji kamer samochodowych oraz kamer nasobnych testowane jest w wielu krajach. Do masowego użytku kamerki te weszły w Stanach Zjednoczonych Ameryki

Północnej, Wielkiej Brytanii, Francji oraz we Włoszech. Z prawnego punktu widzenia istotne są nie tyle kwestie techniczne czy technologiczne, a raczej kwestie organizacyjne oraz prawne określające zasady ich użytkowania. W Wielkiej Brytanii realizowany jest model znacznej władzy dyskrecjonalnej policjanta. To policjant decyduje, kiedy włączyć kamerę, a kiedy nie. „*College of Policing* – centralny ośrodek szkoleniowo-edukacyjny dla jednostek policji w Anglii i Walii potwierdził wcześniejsze rządowe dyrektywy orzekając, że decyzja o tym, czy nagrywać lub nie nagrywać należy do użytkowników sprzętu, a więc policjantów, którzy nie mogą bezkrytycznie rejestrować całego przebiegu służby. Jednakże powinni oni utrwalać incydenty w każdej sytuacji, gdy powołują się na swoje uprawnienia policyjne”[17]. Także większość jednostek Policji w USA daje funkcjonariuszom swobodę w zakresie decydowania, kiedy włączyć kamerę, a kiedy nie, jednakże w jednostkach Policji operujących w aglomeracja miejskich stosuje się „ograniczony uznaniowy model stosowania władzy” (*limiteddiscretion model*), co oznacza, że funkcjonariusze są zobowiązani nagrywać określone działania policyjne, ale mają pozostawioną swobodę decyzji w pozostałych przypadkach. W praktyce zdecydowana większość dużych jednostek policji miejskiej w USA nakazuje rejestrować takie działania policyjne jak: kontrole drogowe, przeszukania, zatrzymania, aresztowania, pościgi samochodowe lub piesze[18].

Istnieje jednak wiele środowisk opiniotwórczych, które postulują, aby rejestrowana była każda interwencja policjanta. M.in. Stowarzyszenie Prokuratorów Okręgowych Karoliny Północnej postuluje, „aby rejestrować każdą interakcję policjanta z obywatelem oraz wszystkie interwencje funkcjonariuszy, odpowiadających na telefoniczne wezwanie o pomoc”, i aby wyłączać kamery można tylko wtedy, gdy policjanci mają przerwę, nie wykonują oficjalnych obowiązków służbowych lub gdy konieczne jest skorzystanie z toalety”. „Środowisko prokuratorskie argumentuje, że funkcjonariusze stosując się do tego rodzaju procedur unikną zarzutu selektywnego nagrywania zdarzeń, aby ukryć zachowania niegodne z prawem lub regulaminem”[19].

[17] R. Wasiak, *Kryminalistyczno-prawna problematyka wprowadzenia do użytku nasobnych kamer video w Policji – w ujęciu porównawczym*, Warszawa 2019, s. 74.

[18] Ibid., s. 74–75.

[19] Ibid., s. 78.

5. Wnioski *de lege lata*

Interwencje Policji w zakresie kontroli ruchu drogowego wzbudzają spore kontrowersje. Na wokandy sądowe trafia spora liczba spraw, w których osoby obwinione kwestionują zasadność podnoszonych zarzutów oraz wykazują nierzetelność podejmowanych przez Policję działań. Kontrowersje te w postępowaniach sądowych rozstrzygane są z zasady na niekorzyść podsądnych, gdyż Policja nie zabezpiecza obiektywnego materiału dowodowego, który mógłby podważyć stanowiska prezentowane przez policyjne źródła dowodowe, a sądy ślepo dają wiarę zeznaniom nierzetelnych funkcjonariuszy.

Od kilku lat w Polskiej Policji rozważana jest kwestia wyposażenia funkcjonariuszy w kamerki nasobne. Pierwsze programy pilotażowe z zastosowaniem tego rodzaju sprzętu przeprowadzono w latach 2015–2016 w Komendach Miejskich Policji w Krakowie oraz w Gorzowie Wielkopolskim – w tym zastosowano je podczas Światowych Dni Młodzieży[20]. W 2017 r. kamerki nasobne zaczęto regularnie stosować w katowickim Oddziale Prewencji[21]. Pod koniec 2017 r. został rozstrzygnięty przetarg na zakup 180 nasobnych kamer video na zamówienie Komendy Głównej Policji. Zakupione kamery zostały przeznaczone do programu pilotażowego, który realizowany był w Komendzie Stołecznej Policji oraz w Komendach Wojewódzkich w Białymstoku i Wrocławiu[22]. W grudniu 2018 r. zakończyło się policyjne postępowanie przetargowe w tej sprawie, które wygrała amerykańska firma „Axon", oferując nasobne kamery video typu „Axon Body". Zgodnie z planami w 2019 r. sprzęt trafił do ponad 31 jednostek polskiej policji we wszystkich województwach. 1191 kamer video przeznaczono dla policjantów ruchu drogowego, a 919 kamer dla funkcjonariuszy służby patrolowej[23]. Docelowo – zgodnie z Programem Modernizacji Służb Mundurowych na lata 2017–2020 – wszystkie komendy miejskie i powiatowe w całym kraju zostaną objęte tym systemem.

---

[20] J. Nowak, Dowódca Oddziału Prewencji Policji w Krakowie, *Opinia dotycząca kamer nasobnych, użyczonych do testowania policji*, Kraków 20.12.2016.

[21] Zob. P. Drabek, *Policjanci jeżdżą już na akcje z kamerkami*, „Dziennik Zachodni 30.05.2017.

[22] P. Słowik, *Policjanci dostaną kamery. Na razie tylko do testów*, „Dziennik Gazeta Prawna" 29.06.2017.

[23] Główny Sztab Policji KGP, *Informacje nt. procedury przetargowej, dotyczącej zakupu nasobnych kamer video na potrzeby polskiej policji*, Warszawa, 20.11.2018.

Pomimo powyższych programów pilotażowych oraz faktu, iż Policja jest już w posiadaniu ponad 2 tysięcy kamer nasobnych, w przedmiocie postępowań wykroczeniowych z zakresu ruchu drogowego na razie nic się nie zmienia. A nie zmienia się dlatego, iż:

- kamery wykorzystywane są tylko w sytuacjach, gdy funkcjonariusz dysponujący urządzeniem uruchomi go;
- nagranie z kamery nie jest obligatoryjnym dowodem procesowym.

Badania aktowe oraz monitoring postępowań sądowych na razie nie wychwyciły ani jednego przypadku, w którym nagranie z kamery stanowiłoby dowód w postępowaniu sądowym.

Aby kamery nasobne – a także kamery samochodowe – spełniły swoją rolę, ich użycie podczas kontroli drogowej musi być obligatoryjne – a ich wyłączenie oraz edytowanie zapisu przez funkcjonariusza musi być uniemożliwione. Ponadto dowodem w sprawie musi być zapis całej interwencji, a nie wybranych fragmentów. A taka opcja wykorzystania tych urządzeń – na razie – nie jest przez Policję brana pod uwagę.

6. Wnioski *de lege ferenda*

Należy ucywilizować postępowania związane z naruszeniami przepisów ruchu drogowego i urzeczywistnić zasadę prawdy obiektywnej w tym obszarze. Będą temu służyć przede wszystkim dwie wzajemnie uzupełniające się regulacje:

- podstawą obwinienia kierujących o bezskutkowe wykroczenie drogowe (a wiec nie dotyczy to kolizji i wypadków drogowych) będzie stanowić jedynie dowód materialny w postaci nagrania lub zapisu pomiaru zarejestrowanego przez urządzenie rejestrujące lub przyrząd kontrolno-pomiarowy (w tym nagranie dokonane zwykłą kamerą osobistą lub samochodową);
- osoby pełniące funkcje organu mandatowego nie będą mogły być przesłuchiwane w charakterze świadków. Rozwiązanie to wymusi na Policji prowadzenie postępowań według standardów stosowanych w demokratycznych państwach prawa. Zeznania policjanta nie będą mogły być dowodem w sprawie, dlatego też policjant będzie musiał takie dowody zdobyć.

Powyższe standardy powinny być wprowadzone poprzez dokonanie następującej nowelizacji obowiązujących przepisów:

- w art. 130 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym dodaje się ustęp 1b w następującym brzmieniu: „1b. Do ewidencji wpisuje się jedynie te naruszenia formalne, które zostały zarejestrowane przez urządzenie rejestrujące, przyrząd kontrolno-pomiarowy lub inne urządzenia rejestrujące obraz i dźwięk";
- w art. 57 ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia dodaje się § 3a w następującym brzmieniu: „§ 3a Wniosek o ukaranie w sprawie o wykroczenie formalne popełnione przez kierującego w ruchu drogowym oprócz danych, o których mowa w § 2 zawiera: 1) informację o dokonaniu wpisu wykroczenia do ewidencji kierowców, 2) wyciąg z ewidencji kierowców zawierający naruszenia przepisów ruchu drogowego, które nie uległy zatarciu";
- do ustawy z dnia z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego do art. 178 dodaje się punkt 3 w brzmieniu: „3) funkcjonariusza organu uprawnionego do nakładania mandatów karnych co do faktów dotyczących zarzutów stanowiących przedmiot postępowania mandatowego".

W celu zrealizowania powyższych zmian wszystkie pojazdy służbowe „Policji drogowej" będą wyposażone w kamery, które będą rejestrować zdarzenia na drodze, a nagrania te będą służyć jako dowód w sprawie. Ponadto każdy policjant ruchu drogowego będzie wyposażony w kamerę osobistą, którą będzie nagrywać wszystkie interwencje. Respektowanie tego wymogu wzmocni zasadę jawności procedur podejmowanych przez organy demokratycznego państwa prawnego, urzeczywistni zasadę prawdy obiektywnej oraz ograniczy lub nawet wyeliminuje przypadki nadużywania uprawnień przez funkcjonariuszy w stosunku do kierujących pojazdami.

Proponowane zmiany wymagają zabezpieczenia odpowiednich środków finansowych na zakup sprzętu multimedialnego, lecz nie muszą to być środki zbyt wielkie. Sprzęt ten jest obecnie powszechnie dostępny i stosunkowo tani. Gdy chodzi o kamery wewnątrzsamochodowe, to niemal każda dostępna na rynku kamera samochodowa posiada wszystkie elementy potrzebne do rejestracji służby policji. Jako wystarczający na wskazane potrzeby należy uznać sprzęt w rozdzielczości HD HD (1920x1080 pikseli). Koszt jednej takiej

kamery nie powinien przekroczyć 300 zł[24]. Również kamery namundurowe (*body cameras*) są tak zaprojektowane, aby można je było wygodnie nosić na klapie munduru czy nawet kieszonki koszuli. Podobnie jak kamery samochodowe są one dzisiaj powszechnie dostępne i też dość tanie. Koszt jednej kamery nie powinien przekroczyć 700 zł[25]. W przypadku kamer kupowanych przed jednostki Policji – z jakiegoś powodu – te koszty są jednak większe. Koszt kamer, w jakie wyposażani są policjanci w USA, oscyluje w granicach 350–700 dolarów[26]. Również w Polsce pierwsze zakupione przez Policję kamery okazały się znacznie droższe.

W aktualnie obowiązującym stanie do ewidencji kierowców wpisywane są wykroczenia, których popełnienie niekoniecznie zostało w jakikolwiek sposób udokumentowane. Niniejszy projekt wprowadza natomiast zasadę, że do ewidencji będą wpisywane jedynie te naruszenia formalne, które zostały zarejestrowane przez urządzenie rejestrujące, przyrząd kontrolno-pomiarowy bądź kamerę personalną lub samochodową. Także w postępowaniu sądowym powyższe środki dowodowe uzyskują priorytet – kosztem środków osobowych.

Proponowane zmiany uproszczą oraz znacznie przyspieszą postępowania sądowe w sprawach z zakresu ruchu drogowego. Wprowadzenie zasady obligatoryjnego rejestrowania wykroczeń przy użyciu urządzeń rejestrujących oraz kamer sprawi, że zdecydowana większość spraw w ogóle nie trafi do sądu, gdyż fakt popełnienia wykroczenia nie będzie kwestionowany przez sprawców – a zatem sprawy będą się kończyć w postępowaniu mandatowym, ewentualnie w postępowaniu nakazowym (w przypadkach, gdy postępowanie mandatowe będzie niedopuszczalne).

[24] Należy też zauważyć, że niemal wszystkie takie kamery są wyposażone w sensor przyspieszenia, za pomocą którego można szacować prędkość samochodu, a niektóre, jak ta powyżej, są także wyposażone w odbiornik GPS, który pozwala kalibrować pomiar przyspieszenia, co pozawala na dokładniejszy pomiar prędkości radiowozu niż ten który stosuje dzisiaj policja w polskich radiowozach. Pogląd za: S. Janczewski, *Krótka analiza kosztów kamer dla Policji* (w posiadaniu autora).

[25] Ibid.

[26] Źródło prasowe.

Bibliografia

Akta czynności wyjaśniających RSOW 2879/17 w Komendzie Miejskiej Policji w Olsztynie.

Akta czynności wyjaśniających RSOW-34-13 RKP w Komendzie Powiatowej Policji w Kraśniku.

Akta postępowania przygotowawczego 2 Ds 1300.2018 w Prokuraturze Rejonowej w Kraśniku.

Akta postępowania przygotowawczego 2 Ds 366.2019 w Prokuraturze Rejonowej w Puławach.

Akta postępowania przygotowawczego DS 1544/15 w Prokuraturze Rejonowej w Myśliborzu.

Akta postępowania przygotowawczego PR Ds 40/16 w Prokuraturze Rejonowej w Pyrzycach.

Akta postępowania przygotowawczego PR Ds 282.2016 w Prokuraturze Rejonowej w Białogardzie.

Akta postępowania przygotowawczego PR Ds 730.2017 w Prokuraturze Rejonowej w Kolbuszowej.

Akta sprawy II W 236/15 w Sądzie Rejonowym w Oświęcimiu.

Akta sprawy VI W 135/19 w Sądzie Rejonowym w Lesku.

Akta sprawy II W 210/18 w Sądzie Rejonowym w Kraśniku.

Akta sprawy II W 357/18 w Sądzie Rejonowym w Kraśniku.

Drabek P., *Policjanci jeżdżą już na akcje z kamerkami,* „Dziennik Zachodni" 30.05.2017, https://dziennikzachodni.pl/policjanci-jezdza-juz-na-akcje-z-kamerkami/ar/12127264.

Główny Sztab Policji KGP, *Informacje nt. procedury przetargowej, dotyczącej zakupu nasobnych kamer video na potrzeby polskiej policji*, Warszawa, 20.11.2018,

Góralczyk W., *Kierownictwo w prawie administracyjnym,* Warszawa 2016.

Janczewski S., *Krótka analiza kosztów kamer dla Policji.*

Knossala E., *Zarys nauki administracji*, Zakamycze 2006.

Mocarska D., *Przekroczenie uprawnień lub niedopełnienie obowiązków przez funkcjonariuszy policji w reakcji na wykroczenie drogowe – prezentacja badań kryminologicznych*, w: *Współdziałanie organów bezpieczeństwa i porządku publicznego w zakresie zapobiegania i zwalczania wykroczeń*, red. I. Nowicka, A. Sadło-Nowak, A. Tunia, Lublin 2012, s. 257–270.

Nowak J., Dowódca Oddziału Prewencji Policji w Krakowie, *Opinia dotycząca kamer nasobnych, użyczonych do testowania policji*, Kraków 20.12.2016.

Pieprzny S., *Administracja bezpieczeństwa i porządku publicznego,* Rzeszów 2012.

Rozporządzenie Ministra Zdrowia z dnia 11 grudnia 2015 r. w sprawie badań na zawartość alkoholu w organizmie (Dz.U. poz. 2153).

Słowik P., *Policjanci dostaną kamery. Na razie tylko do testów,* „Dziennik Gazeta Prawna", 29.06.2017, https://prawo.gazetaprawna.pl/artykuly/1054110,policjanci-kamery-w-mundurach.htm.

Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (tekst jedn.: Dz.U. 2018 poz. 2137).

Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (tekst jedn.: Dz.U. 2019 poz. 821 ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn.: Dz.U. 2019 poz. 161 ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (tekst jedn.: Dz.U. 2018 poz. 1600 ze zm.).

Ustawa z dnia z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jedn.: Dz.U. 2018 poz.1600 ze zm).

Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2019 poz. 1120 ze zm.).

Wasiak R., *Kryminalistyczno-prawna problematyka wprowadzenia do użytku nasobnych kamer video w Policji – w ujęciu porównawczym,* Warszawa 2019.

Zarządzenie nr 30 Komendanta Głównego Policji z dnia 22 września 2017 r. w sprawie pełnienia służby na drogach (Dz. Urz. KGP poz. 64).