METODY ZAPOBIEGANIA PRZESTĘPCZOŚCI

AUTORZY:

Adrian DONE, London Business School
Bartosz JANASZEK, Executive Education Center
Marcin KIELISZCZYK, Executive Education Center
Jeff KLABEN, SRI International
Radosław KOSZEWSKI, Executive Education Center
Stuart MADNICK, Massachusetts Institute of Technology
Marcin MROWIEC, Bank Polska Kasa Opieki SA

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
Łukasz WOJCIESZAK, Politechnika Świętokrzyska
Jolanta STANIENDA, Uniwersytet Ekonomiczny w Krakowie
Marek BIELECKI, Akademia Sztuki Wojennej

METODY ZAPOBIEGANIA PRZESTĘPCZOŚCI

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 978-83-66344-35-8

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

CZĘŚĆ DRUGA. ZESPÓŁ IMPLEMENTACYJNY

Słowo wstępne

Niniejszy raport jest podsumowaniem prac badawczych przeprowadzonych w ramach drugiego modułu projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" Instytutu Wymiaru Sprawiedliwości. To druga praca z cyklu poświęconego zagadnieniu przeciwdziałania przestępczości w kluczowych obszarach polskiej gospodarki. Badania wpisują się w nurt działań wspierających zwalczanie przyczyn przestępczości i ograniczanie czynników ryzyka jej występowania.

Pierwsza część niniejszej publikacji (raport) jest podsumowaniem przeprowadzonej krytycznej analizy dotyczącej metodologii zarządzania operacyjnego wykorzystywanej w działaniach podejmowanych w celu zapobiegania i przeciwdziałania przestępczości. Zakres jej stosowania i skuteczności został określony. Wypracowano również podstawy decyzyjne dla krytycznej analizy wyboru optymalnych metod przeciwdziałania przestępczości. Wskazano przy tym podstawowe kryteria, które należy uwzględnić przy wyborze właściwej metody. Jednym z nich jest zastosowanie metod stosownie do specyfiki działalności organizacji w Polsce – zarówno instytucji administracji publicznej, jak również strategicznych podmiotów gospodarczych funkcjonujących w sektorach finansowym, ubezpieczeniowym i energetycznym. Szczególną uwagę poświęcono obszarowi zarządzania ludźmi w organizacjach. W raporcie analizowane są elementy metod zapobiegania przestępczości zaproponowane przez zaproszonych ekspertów.

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 Improving Performance. 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 metod zapobiegania przestępczości.

CZĘŚĆ PIERWSZA
RAPORT

AUTORZY:

Adrian DONE, London Business School
Bartosz JANASZEK, Executive Education Center
Marcin KIELISZCZYK, Executive Education Center
Jeff KLABEN, SRI International
Radosław KOSZEWSKI, Politechnika Warszawska
Stuart MADNICK, Massachusetts Institute of Technology
Marcin MROWIEC, Bank Polska Kasa Opieki SA

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 w ramach pierwszego etapu seminariów skupiły się na przyczynach przestępczości w wybranych obszarach gospodarki i identyfikacji tych wektorów zagrożeń, które niosą największe ryzyko powstania szkód materialnych i wizerunkowych dla organizacji funkcjonujących w sektorze ubezpieczeniowym, finansowym, energetycznym oraz dla obszaru zarządzania ludźmi w organizacjach. Badania przeprowadzone w ramach drugiego etapu seminariów, których wyniki zostały podsumowane w niniejszym raporcie, dotyczyły metod zapobiegania przestępczości z wykorzystaniem metod zarządzania operacyjnego, które w szczególny sposób adresują wektory zagrożeń zidentyfikowane w pierwszym etapie seminariów.

Metody zapobiegania przestępczości można sklasyfikować według strategii kreatywnej lub destruktywnej[1]. Zgodnie z podejściem destruktywnym zjawiska przestępcze[2] są nieuniknione. Dlatego należy podejmować kroki uprzedzające ich wystąpienie. Pośród nich postuluje się następujące działania:

- uniemożliwiające bądź utrudniające podejmowanie określonych działań przestępczych bądź szkodliwych (1),
- sankcjonujące te przypadki działań szkodliwych, co do których istnieje podejrzenie, że powtórzą się w przyszłości lub będą się nasilać; stosuje

[1] B. Hołyst, *Kryminologia*, Wolters Kluwer, Warszawa 2016.

[2] „Przestępczy" należy rozumieć w szerokim kontekście, jako każdy przejaw działalności, który godzi w uprawnione interesy osób i organizacji lub jest rażąco niezgodny z ich wartościami (kulturą organizacji) lub przyjętym kodeksem postępowania (ang. *code of conduct*). W szczególności termin ten należy odróżnić od terminu „przestępny" stosowanego w przepisach Kodeksu karnego jako określenie tych czynów, które wyczerpują znamiona przestępstwa zapisane w prawie.

się sankcje zarówno formalne (prawne), jak i nieformalne, takie jak poddanie ostracyzmowi lokalnej społeczności czy podjęcie decyzji personalnych związanych z zatrudnieniem (2), oraz
- zagrażające nałożeniem sankcji w przypadku potencjalnego dopuszczenia się czynu szkodliwego (3).

Jedna z głównych tez badań przeprowadzonych w ramach seminariów wskazuje, że metody określane zbiorczym terminem zarządzania operacyjnego stosowane w kontekście przeciwdziałania przestępczości realizują pierwszy z postulatów właściwych dla grupy strategii destruktywnych poprzez optymalizację wykorzystania zasobów organizacji. Służą one ograniczaniu zmienności (niepewności) w działalności operacyjnej, skutecznie redukując bądź zapobiegając nadużyciom. W efekcie dochodzi do wytworzenia odporności organizacji (ang. *resiliency*) na zewnętrzne i wewnętrzne działania destabilizujące. Ponadto wzmocnione zostają mechanizmy kontroli zasobów, co pozytywnie rzutuje na ogólną produktywność organizacji.

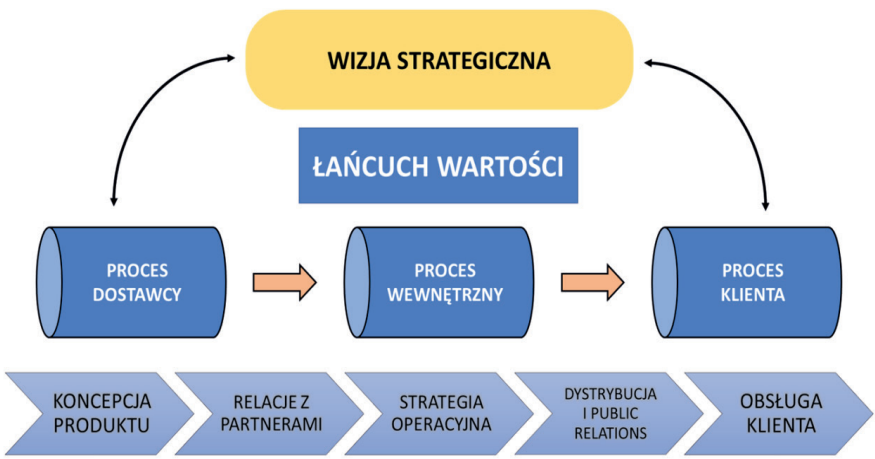
Jednocześnie należy wyjść z założenia, że zabezpieczenie organizacji przed każdym potencjalnym atakiem nie jest możliwe. Zatem, na gruncie podejścia ekonomicznego, każdą strategię destruktywną należy rozumieć jako taką, która powoduje, że pewne działania podjęte przeciwko organizacji będą nieopłacalne w perspektywie potencjalnych korzyści płynących z ich powodzenia, a przez to wykazujące niski priorytet w ramach przyjętej strategii bezpieczeństwa.

Proces uzyskiwania odporności rozpoczyna się od poznania i zrozumienia tzw. łańcucha wartości organizacji (ang. *value chain*), czyli następstwa działań, które prowadzą do pomyślnego wytworzenia i dostarczenia produktu oferowanego przez daną organizację w drodze zwiększania jego wartości w kolejnych etapach procesu biznesowego[3]. Pełna interpretacja łańcucha wartości, oprócz wewnętrznych procesów biznesowych organizacji, uwzględnia jej interakcję z dostawcami (surowców, półproduktów), nabywcami (odbiorcami) oraz dystrybutorami stanowiącymi istotne elementy ekosystemu, w którym funkcjonuje (zob. rysunek 1).

[3] M.E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance*, Free Press, Riverside 2008.

Na potrzeby niniejszego projektu badawczego niepewność powiązaną z przebiegiem procesów operacyjnych uznano za podstawową metrykę fenomenu, który autorzy określili mianem *powierzchni ataku na organizację*. Terminem tym, zapożyczonym z nauk informatycznych[4], określono zespół czynników będący podzespołem tych elementów łańcucha wartości, które mogą w istotny sposób zagrozić przebiegowi zasadniczych procesów operacyjnych, jeśli zostaną wykorzystane przez agresora. Sam atak należy rozumieć jako każde działanie skutkujące zaburzeniem funkcjonowania łańcucha wartości organizacji. Powyższa definicja opiera się na założeniu, zgodnie z którym każdy potencjalny atak wymierzony przeciwko organizacji odbywa się przy wykorzystaniu jej własnych zasobów bądź elementów jej ekosystemu.

Rysunek 1. Schemat zewnętrznego (pełnego) łańcucha wartości z uwzględnieniem procesów dostawców i klientów (odbiorców)



Źródło: opracowanie własne

Na tym gruncie wszelkie odstępstwa od optymalnego przebiegu procesu biznesowego rzutują na jego niepewność. Stanowią zagrożenie dla funkcjonowania organizacji (w tym graniczny przypadek całkowitej utraty zdolności organizacji do realizacji działań operacyjnych) znajdujące odzwierciedlenie

[4] P.K. Manadhata, *An Attack Surface Metric*, Carnegie Mellon University 2008, http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf#page=45&zoom=100,0,382

w spadku wartości miar efektywności (produktywności). Należy pamiętać, że mamy tu do czynienia z relacją zwrotną, gdzie spadek miar efektywności można powiązać z możliwością realizowanego, bądź pomyślnie zakończonego, ataku wymierzonego przeciwko danej organizacji. W tym kontekście metody wykorzystywane w zarządzaniu operacyjnym zastosowane zostały także do oszacowania maksymalnego potencjału wytwórczego organizacji. Jest to ten element wypracowanej metodologii zapobiegania przestępczości w organizacjach, który wyznacza warunki początkowe i brzegowe dla analizy niepewności procesów operacyjnych odpowiadające odpowiednio ocenie bieżącego stanu procesów, określonego przy pomocy przyjętych miar efektywności oraz stanu optymalnego, preferowanego w świetle wizji strategicznej przyjętej przez organizację.

Wyniki badań stanowią element kompleksowego szkieletu metodologicznego B^3 (ang. *Be Lean, Be a Team, Be Ready*) na rzecz zapobiegania przestępczości w organizacjach, który został kompleksowo zaprezentowany w ramach ostatniego z cyklu raportów podsumowujących badania.

2. Seminarium jako narzędzie badawcze

Członkowie najwyższej kadry kierowniczej zwykle nie mają okazji ani warsztatu pozwalających na prowadzenie badań z zachowaniem rygoru naukowego. Posiadają jednak cenną wiedzę. Dzięki zastosowaniu seminarium jako narzędzia badawczego w projekcie „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" możliwe było wykorzystanie tej wiedzy dla potrzeb naukowych. Metodyka badawcza, gdzie stosowane jest seminarium, została opisana w raporcie „Identyfikacja przyczyn przestępczości w wybranych obszarach w Polsce i na świecie". Kluczowe w wybranej metodyce były studia przypadku. Stanowiły instrument wprowadzający istotne pojęcia i zagadnienia, aby zaangażować uczestników w dyskusje poświęcone metodom zapobiegania przestępczości.

Tematyka seminariów przeprowadzonych w październiku 2018 roku dotyczyła możliwości wykorzystania elementów zarządzania operacyjnego na rzecz przeciwdziałania przestępczości. Głównym celem był rozwój umiejętności w zakresie zarządzania operacyjnego w kontekście przeciwdziałania przestępczości. Z uwagi na sformułowany cel, zakres problemowy seminariów miał charakter uniwersalny, istotny z punktu widzenia możliwości wykorzystania wiedzy i doświadczenia przedstawicieli organizacji należących do każdego z reprezentowanych sektorów.

Kolejne części niniejszego rozdziału zawierają opis przeprowadzonych prac badawczych wraz z wyszczególnieniem poszczególnych faz oraz podziałem na etapy, zgodnie z założeniami projektu (zob. rozdziały 2.1–2.3). Dalej przedstawiono również tematykę poruszoną w ramach każdego z paneli seminaryjnych, opis kompetencji zaproszonych ekspertów oraz ocenę treści merytorycznych wystąpień i strony organizacyjnej seminarium, dokonaną

przez uczestników. Szczegółowe informacje dotyczące metodologii prac badawczych zostały przedstawione w pierwszym raporcie tego cyklu zatytułowanym „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".

2.1. Faza wstępna

Właściwe zaplanowanie i przeprowadzenie prac w fazie wstępnej miało decydujące znaczenie dla powodzenia projektu. Dzięki wieloletniemu doświadczeniu dyrektora naukowego projektu, prof. Michaela Rosenberga z IESE Business School, treści seminariów zostały dobrane w taki sposób, aby spotkały się z zainteresowaniem uczestników, a dyskusje tworzyły warunki do pozyskania od nich wiedzy na temat analizowanych zagadnień.

Same seminaria były poprzedzone samodzielną pracą uczestników w zakresie metod zapobiegania przestępczości. Dokonali oni indywidualnej analizy udostępnionych materiałów, zgodnie z instrukcją dotyczącą zakresu i metody ich opracowania.

2.1.1. Wybór studium przypadku

Pierwszym etapem fazy wstępnej był wybór studiów przypadków odpowiednio do potrzeb prac badawczych prowadzonych podczas seminariów. W drodze krytycznej analizy zaproszeni eksperci wyróżnili dwa studia przypadków, jako najwłaściwsze dla tego etapu projektu. Opracowania zatytułowane *Kristen's Cookie*[5] oraz *Benihana of Tokio*[6] to sztandarowe przykłady wykorzystania metodyki zarządzania operacjami. Zostały wybrane z uwagi na swój uniwersalny charakter. Poruszają problematykę łańcucha wartości jako elementu niezbędnego dla zrozumienia potencjalnych zagrożeń

[5] R.E. Bohn, *Kristen's Cookie*, *Harvard Business School Case Collection*, 1986, nr 686093-PDF-ENG.

[6] W.E. Sasser, *Benihana of Tokyo*, *Harvard Business School Case Collection*, 1972, nr 673–057.

związanych z prowadzeniem działalności przez organizację w kontekście możliwości wystąpienia nadużyć. Dodatkowo wskazują na istotę identyfikacji tzw. wąskich gardeł, będących krytycznymi elementami działalności operacyjnej. Wybór takich studiów przypadków pozwolił stworzyć odpowiedni kontekst do wprowadzenia tematyki zarządzania operacjami, co bezpośrednio nawiązuje do celu tego etapu projektu, tj. rozwoju umiejętności uczestników seminariów w zakresie zarządzania operacjami mającymi na celu przeciwdziałanie przestępczości. Kolejnym założeniem przyjętym przez ekspertów przy selekcji studiów przypadków była ich przydatność pod kątem analizy ukierunkowanej na zrozumienie metod przeciwdziałania przestępczości w Polsce i na świecie oraz identyfikacji ogólnych mechanizmów znajdujących zastosowanie w zapobieganiu przestępczości. Wybrane przez ekspertów studia przypadków dla grup złożonych z przedstawicieli poszczególnych sektorów zostały przedstawione 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	• *Kristen's Cookie* • *Benihana of Tokyo*
SEKTOR UBEZPIECZEŃ	
SEKTOR ENERGETYKI	
ZARZĄDZANIE LUDŹMI W ORGANIZACJACH	

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

2.1.2. Indywidualna analiza studium przypadku

W ramach przygotowania do udziału w seminariach uczestnicy przeprowadzili indywidualną analizę studiów przypadków *Kristen's Cookie* oraz *Benihana of Tokyo*, zgodnie z wytycznymi sformułowanymi przez organizatorów. Zasadniczym elementem zastosowanej metody badawczej było wykorzystanie potencjału intelektualnego i doświadczenia uczestników, zatem głównym

celem pracy indywidualnej było odpowiednie przygotowanie uczestników do pracy w grupie.

Analizując schematy organizacyjne przedsiębiorstw, sprawozdania finansowe, strategie marketingowe oraz statystyki rynkowe, uczestnicy mogli wstępnie zapoznać się z zagadnieniami z zakresu zarządzania operacyjnego w organizacjach będących przedmiotem późniejszych rozważań.

Na tym etapie każdy z uczestników sformułował opinię w zakresie aktualnych bądź potencjalnych przyczyn niewydolności operacyjnej organizacji opisanych w studiach przypadków. Aby właściwie ukierunkować uwagę uczestników oraz dyskusje prowadzone w trakcie seminariów, zaproszeni eksperci sporządzili listę pytań pomocniczych do wybranych studiów przypadków. Dodatkowym zaleceniem było przeprowadzenie szczegółowej analizy ilościowej opisanych historii z uwzględnieniem narzędzi typowych dla metodyki zarządzania operacyjnego, w tym harmonogramu Adamieckiego.

Przedmiotem prac badawczych była również analiza studiów przypadków z zakresu metodyki działalności grup przestępczych wykorzystujących zaawansowane narzędzia technologiczne. Z uwagi na złożoność i techniczną naturę zagadnienia, w ramach przygotowania indywidualnego, prof. Stuart Madnick zalecił uczestnikom zapoznanie się z wybranymi publikacjami prasowymi dotyczącymi cyberprzestępczości. Pozostałe wytyczne znalazły się w pierwszym raporcie cyklu zatytułowanym „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".

2.2. Seminaria

Zgodnie z przyjętą metodyką badawczą dyskusje przeprowadzone w ramach seminariów stanowiły kluczowy element analizy, a co za tym idzie, prac badawczych październikowego etapu projektu. Dzięki kompleksowemu przygotowaniu uczestników i ich bogatym doświadczeniom zawodowym, a także właściwemu ukierunkowaniu dyskusji seminaryjnych przez ekspertów, możliwa była analiza o rygorze naukowym, wykorzystująca specjalistyczną wiedzę uczestników w zakresie działalności poszczególnych sektorów gospodarki.

Niniejszy podrozdział zawiera dalszy opis prac badawczych, ze szczególnym uwzględnieniem założeń organizacyjnych i przebiegu seminariów będących podstawą sformułowania wniosków oraz zaleceń dotyczących metod przeciwdziałania przestępczości. Treści zawarte w tym rozdziale obejmują etapy i cele analiz uczestników (zob. rozdziały 2.2.1–2.2.3), zakres tematyczny seminariów z uwzględnieniem poszczególnych paneli (zob. rozdział 2.2.4) oraz biogramy i opis kompetencji zaproszonych ekspertów (zob. rozdział 2.2.5).

2.2.1. Praca w grupach

Praca w grupach miała pomóc uczestnikom stworzyć społeczność naukową posługującą się spójnym zestawem pojęciowym i wspólnie dążącą do wypracowania oryginalnych wniosków w zakresie metod przeciwdziałania przestępczości w wybranych sektorach gospodarki. Na tym etapie uczestnicy mieli okazję poznać opinie pozostałych osób sformułowane podczas indywidualnej analizy otrzymanych materiałów. Dzięki temu wszyscy mogli lepiej zrozumieć argumentację, intencje i styl komunikacji pozostałych członków grupy, tym samym zwiększając wzajemne zaufanie. To pozwoliło na stworzenie warunków sprzyjających dzieleniu się własnymi przemyśleniami z innymi. Analizę grupową poprzedziło wprowadzenie prof. Adriana Done'a dotyczące zarządzania operacyjnego wraz z zarysowaniem możliwości jego wykorzystania w kontekście przeciwdziałania przestępczości. Istotnym elementem było tu zagadnienie zmienności (niepewności) w działalności operacyjnej organizacji oraz związanych z nią zagrożeń w odniesieniu do potencjalnych nadużyć. Głównym celem wprowadzenia tematyki był rozwój umiejętności uczestników w zakresie posługiwania się pojęciami z zakresu zarządzania operacjami tak, aby możliwe było optymalne wykorzystanie potencjału intelektualnego oraz doświadczeń każdego z uczestników na potrzeby identyfikacji ogólnych mechanizmów działania metod zapobiegania przestępczości.

2.2.2. Praca w grupach nad studium przypadku

Praca nad studiami przypadków miała podobny charakter do poprzedzającej ją pracy grupowej.

W zespołach liczących od pięciu do dziewięciu osób uczestnicy mogli przedstawić swoje przemyślenia związane z problematyką studiów przypadków. Małe grupy sprzyjały poczuciu komfortu i pozwalały na swobodną wymianę poglądów. Ten etap miał szczególne znaczenie dla dalszych prac badawczych z uwagi na zróżnicowane kompetencje i doświadczenia uczestników, co pozwoliło na przeprowadzenie uporządkowanej i dokładnej analizy podczas dyskusji plenarnych. Istotnym elementem prac było wzbogacenie samodzielnych analiz o pojęciowy warsztat wypracowany w ramach wcześniejszych etapów oraz narzędzia analityczne zaproponowane przez prof. Done'a.

Warto pokreślić, że celem dyskusji przeprowadzonej w ramach tego etapu nie było sformułowanie wspólnego stanowiska na temat właściwego sposobu zaradzenia problemom przedstawionym w studiach przypadku. Był to etap przygotowujący do analizy przeprowadzonej w ramach dyskusji plenarnej.

2.2.3. Praca w grupach plenarnych

Połączenie różnorodnych doświadczeń i spostrzeżeń uczestników ze wszystkich grup pozwoliło na kompleksową analizę złożonych zagadnień z zakresu metod przeciwdziałania przestępczości. Nie byłoby to możliwe bez uprzedniego przygotowania uczestników w ramach poprzednich etapów pracy grupowej.

Dyskusje plenarne były końcowym etapem poprzednich analiz, w tym analizy indywidualnej oraz pracy grupowej. W tej części, skoncentrowanej na analizie studiów przypadków, zaproszeni eksperci pełnili rolę moderatorów prac badawczych i służyli swoją wiedzą ekspercką w zakresie wykorzystania innowacyjnych metod przeciwdziałania przestępczości stosowanych na świecie. Rezultatem przeprowadzonej analizy były wnioski i zalecenia końcowe dotyczące metod zapobiegania przestępczości, które podsumowano w kolejnych rozdziałach niniejszego raportu (zob. rozdziały 2.3.3 i 3).

2.2.4. Dyskusja panelowa

Kolejnym elementem przeprowadzonych seminariów była dyskusja panelowa. Jej celem było zaznajomienie uczestników z koncepcją wykorzystania elementów zarządzania operacyjnego w kontekście przeciwdziałania przestępczości w Polsce. Pierwszy etap przeprowadzonych prelekcji miał za zadanie wprowadzić tematykę zarządzania operacyjnego i sposobów zabezpieczania łańcucha wartości, jako kluczowych elementów ochrony działalności operacyjnej organizacji. Aby uzyskać lepszy wgląd w metodykę zarządzania operacyjnego, przedstawione zagadnienia zostały omówione na przykładzie wybranych studiów przypadku, tj., *Benihana of Tokyo*[7] oraz *Kristen's Cookie*[8]. Drugi etap panelu dyskusyjnego był poświęcony analizie skutecznego zastosowania metodyki zarządzania operacyjnego w kontekście uwarunkowań każdego z rozważanych sektorów polskiej gospodarki. W trakcie dyskusji poruszono również kwestię uwarunkowań ekonomicznych dla przestępstw popełnianych w Polsce, wskazano czynniki ekonomiczne wpływające na skłonność do podejmowania nielegalnych działań i obszary o podwyższonym ryzyku operacyjnym. Uczestnicy zadawali pytania panelistom, co pozwoliło na pogłębienie ich wiedzy na dany temat, analizę niejasnych kwestii, a także, poprzez wspólną dyskusję ekspertów i uczestników, analizę przyjętego modelu podejmowania decyzji pod kątem zapobiegania przyczynom przestępczości.

2.2.5. Profile prelegentów

W niniejszym rozdziale przedstawiono sylwetki zaproszonych ekspertów, ze szczególnym uwzględnieniem ich kompetencji i doświadczenia, w tym udokumentowanego dorobku naukowego. Do udziału zaproszeni zostali wybitni światowi eksperci specjalizujący się w różnych dziedzinach, zarówno w obszarze nauki jak i praktyki gospodarczej. Wywodzą się z IESE Business School, Massachusetts Institute of Technology, SRI International i Akademii

[7] W.E. Sasser, *Benihana of Tokyo…* op. cit.
[8] R.E. Bohn, *Kristen's Cookie…* op. cit.

Ekonomicznej w Krakowie. Ich dokonania są powszechnie znane i cenione. Wszyscy pracowali na rzecz rządów lub międzynarodowych koncernów.

Poniżej przedstawiono ich biogramy i skrócone opisy kompetencji. Opis szczegółowy, wraz z listami wybranych publikacji, znaleźć można w załączniku do niniejszego raportu (zob. załącznik A).

Adrian Done

Prof. Adrian Done jest cenionym autorytetem w obszarze kształcenia wyższej kadry kierowniczej, doradztwa strategicznego i biznesowego. Pełnił stanowisko pracownika naukowego w London Business School oraz profesora w IESE Business School. Zdobył szerokie uznanie jako autor licznych kursów dla programów MBA, *Executive Education* oraz studiów doktorskich. Za swoją pracę badawczą w Advanced Institute of Management (AIM) Research London Business School otrzymał szereg nagród od instytucji takich jak European Foundation for Management Development i Decision Sciences Institute.

Prof. Done uzyskał stopień doktora w dziedzinie operacji i zarządzania łańcuchem dostaw na London Business School w Wielkiej Brytanii. Ponadto ukończył dwujęzyczne studia MBA w IESE Business School. Zdobył tytuł inżyniera na angielskim Loughborough University. Karierę rozpoczął w sektorze motoryzacyjnym, w Ford Motor Company, na stanowisku inżyniera projektu.

Jeff Klaben

Jeff Klaben jest głównym inspektorem ds. bezpieczeństwa informacji w SRI International (zajmuje stanowisko Chief Information Security Officer, CIO). Jest również wykładowcą (ang. *Adjunct Professor*) w College of Engineering w Santa Clara University. Zdobywał doświadczenie zawodowe piastując stanowiska kierownicze w przedsiębiorstwach takich jak SanDisk, Cadence Design Systems czy Accenture.

Przewodniczył panelowi doradczemu San Francisco Bay Area InfraGard, za co został uhonorowany dwoma nagrodami Departamentu Sprawiedliwości Stanów Zjednoczonych, za specjalną służbę (ang. *Dedicated Service*) oraz wybitne zasługi dla interesu publicznego (ang. *Exceptional Service in the Public Interest*). Jest współautorem przewodnika po strategiach tworzenia planu reagowania na incydenty bezpieczeństwa infrastruktury informatycznej

pt. *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk*. Brał udział we wdrażaniu strategii bezpieczeństwa cybernetycznego Stanów Zjednoczonych (ang. National Strategy to Secure Cyberspace) w charakterze moderatora konsultacji społecznych. Ponadto występował na licznych międzynarodowych konferencjach poświęconych bezpieczeństwu informacyjnemu.

Uzyskał tytuł MBA w Santa Clara University oraz tytuł BS w dziedzinie systemów informacyjnych w Wright State University. Posiada uprawnienia Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) oraz Certified Information Systems Auditor (CISA).

Stuart Madnick

Prof. Stuart Madnick od ponad 20 lat pełni funkcję dyrektora Grupy Technologii Informacyjnej w MIT. W tym czasie jego zespół nieustannie zdobywał pierwsze miejsca w konkursach programów informatycznych dla szkół biznesu organizowanych w Stanach Zjednoczonych. Prof. Madnick jest autorem i współautorem ponad 380 artykułów, raportów technicznych i książek, w tym podręczników akademickich. W toku kariery zawodowej był kierownikiem licznych projektów badawczych oraz wdrożeniowych, w tym kierownikiem projektu Contex Interchange, którego celem było rozwinięcie technologii wspomagających współpracę między organizacjami, w zakresie zarówno koordynacji, jak i zwiększania efektywności.

Do wybitnych osiągnięć prof. Madnicka należy zaliczyć udział, w charakterze głównego projektanta, w pracach nad stworzeniem systemu operacyjnego VM/370 firmy IBM przeznaczonego dla komputerów klasy *mainframe* oraz systemu informacyjno-wyszukiwawczego DIALOG firmy Lockheed Martin Corporation.

Do bieżących zainteresowań prof. Madnicka należą m.in. komunikacja w rozproszonych systemach informacyjnych, technologia baz danych, zarządzanie projektowaniem oprogramowania oraz strategiczne wykorzystanie technologii informacyjnych.

Marcin Mrowiec

Dr Marcin Mrowiec pełni funkcję Głównego Ekonomisty Banku PKO SA (od 2008 roku), zdobywając liczne wyróżnienia za najbardziej trafne prognozy makroekonomiczne i rynkowe. Studia na kierunku Finanse i Bankowość ukończył z wyróżnieniem w krakowskiej Akademii Ekonomicznej. W roku 2000 rozpoczął pracę w sektorze finansowym, w Dziale Badań Rynków Międzynarodowych monachijskiego Bayerische HypoVereinsbank (HVB). Karierę kontynuował w Banku BPH jako ekonomista, a następnie starszy ekonomista.

2.2.6. Zakres tematyczny seminariów

An introduction to operations management (OM): Benihana case

Celem tego panelu był rozwój umiejętności uczestników w zakresie zarządzania operacjami w obszarze przeciwdziałania przestępczości. Przeprowadzone prace wpisywały się w szerszy kontekst przedstawionej metodyki dedykowanej zwiększaniu efektywności operacji na rzecz zapobiegania przestępczości. Panel poprowadził Adrian Done, uznany specjalista w zakresie zarządzania operacyjnego w organizacjach.

W ramach pierwszej części warsztatów ekspert wprowadził problematykę stosowania zarządzania operacyjnego jako narzędzia zabezpieczającego działalność operacyjną organizacji wywodzących się z dowolnego sektora. Warsztaty objęły również koncepcję łańcucha wartości (ang. *value chain*), jako zestawu następujących po sobie działań związanych z wytwarzaniem produktu (dobra materialnego bądź usługi). Zagadnienie zostało przedstawione jako element niezbędny dla zrozumienia ryzyka prowadzenia działalności przez organizację w kontekście możliwości zaistnienia nadużyć zarówno ze strony sprawców wewnętrznych, jak też tych z bezpośredniego otoczenia organizacji (pracowników, kontrahentów, klientów, dostawców itd.). Wskazano na konieczność pełnego zrozumienia procesów zachodzących w organizacji, umożliwiającego identyfikację zagrożeń i ich eliminację w drodze ciągłego doskonalenia procesów.

Drugą część panelu poświęcono dyskusji grupowej na temat studium przypadku *Benihana of Tokyo*[9]. Historia dotyczy sukcesu Hiroakiego Aokiego, twórcy tytułowej sieci restauracji. Wybrane studium przypadku skupia się na strategii rozwoju i działalności operacyjnej sieci restauracji w oparciu o starannie opracowany model biznesowy w nietypowy sposób wykorzystujący elementy zarządzania operacyjnego. To studium przypadku zostało wybrane z uwagi na niekonwencjonalne zastosowanie zarządzania operacyjnego w sektorze usług, zwykle wykorzystywanego w sektorze produkcyjnym, aby zilustrować uczestnikom uniwersalność proponowanej metodyki. Kolejnym ważnym elementem wprowadzonym przez moderatora była analiza istotności zabezpieczenia łańcucha wartości, jako metody ograniczania nieprzewidywalności w działalności operacyjnej. Interesująca jest również analiza przebiegu kariery założyciela sieci restauracji. Hiroaki Aoki zoptymalizował zarządzanie operacyjne swojej organizacji w niespotykany sposób. Jednocześnie, działając nieetycznie, wykorzystywał dostępne informacje do prowadzenia gry na giełdzie papierów wartościowych. W konsekwencji został skazany na karę pozbawienia wolności, a sieć jego restauracji, pomimo doskonałych rezultatów w zarządzaniu operacyjnym, popadła w problemy finansowe.

Na podstawie przeprowadzonych dyskusji uczestnicy sformułowali następujące wnioski:

- zarządzanie operacyjne może być wykorzystane jako metoda zwiększająca efektywność w działalności operacyjnej organizacji dowolnego typu, ze szczególnym uwzględnieniem procesów dedykowanych przeciwdziałaniu przestępczości,
- zarządzanie operacyjne może być również wykorzystane jako metoda zabezpieczenia działalności operacyjnej przed nadużyciami i nieprawidłowościami, tym samym redukując ryzyko zaistnienia przestępstwa,
- kluczowym elementem zarządzania operacyjnego w kontekście przeciwdziałania przestępczości jest kompleksowe zabezpieczenie łańcucha wartości w działalności organizacji,
- elementy zarządzania operacyjnego są możliwe do zastosowania wprost w organizacjach należących do sektora produkcyjnego, natomiast

[9] W.E. Sasser, *Benihana of Tokyo*…, op. cit.

adaptacja rozważanej metodyki do innych obszarów może przynieść nadzwyczajne korzyści w zakresie zwiększenia efektywności,
- ustalenie transparentnych warunków zarządzania operacjami zniechęca potencjalnych przestępców do podejmowania prób wyłudzeń, kradzieży, nadużyć itp.

Controlling processes: Kristen's Cookie case

Ten etap był bezpośrednią kontynuacją tematyki zarządzania operacyjnego na rzecz przeciwdziałania przestępczości w organizacjach, co zostało zilustrowane podczas ćwiczenia symulacyjnego opartego na scenariuszu *Kristen's Cookie*[10]. Głównym założeniem panelu było pogłębienie analizy w zakresie zarządzania operacjami, ze szczególnym uwzględnieniem procesów dedykowanych przeciwdziałaniu przestępczości.

W pierwszej części panelu wprowadzono pojęcie analizy wydajności operacyjnej organizacji (ang. *capacity analysis*), rozumianej jako proces modelowania interakcji czynności (ang. *activities*) i zasobów (ang. *resources*) mający na celu określenie maksymalnej zdolności wytwórczej organizacji oraz identyfikację tzw. wąskich gardeł (ang. *bottlenecks*) jako tych zasobów, które w sposób zasadniczy ograniczają wydajność. W tym celu wykorzystano harmonogram Adamieckiego (znany także jako diagram Gantta). Wąskie gardło zostało wskazane jako ten przedmiot kontroli procesów biznesowych, który wymaga szczególnej uwagi, w tym także odpowiedniego zabezpieczenia.

Podczas drugiej części panelu moderator poprosił uczestników o przeprowadzenie analizy scenariusza zawartego w opracowaniu *Kristen's Cookie* pod kątem zastosowania zarządzania operacyjnego. Symulacja poprzez przykładowe wykorzystanie działalności opartej na prostych operacjach miała na celu kreatywne zastosowanie elementów zarządzania operacyjnego, w tym metodyki harmonogramu Adamieckiego i identyfikację wąskich gardeł. Szczególny nacisk został położony na wykorzystanie ww. elementów metodyki w kontekście zabezpieczania działalności operacyjnej organizacji przed przestępstwami, a także zwiększania efektywności operacji mających na celu przeciwdziałanie przestępczości.

[10] R.E. Bohn, *Kristen's Cookie*…, op. cit.

W ramach niniejszego panelu uczestnicy sformułowali następujące wnioski:

- identyfikacja wąskich gardeł stanowi kluczowy element rozpoznania najbardziej krytycznych obszarów działalności operacyjnej organizacji,
- odpowiednie zastosowanie zarządzania operacyjnego pozwala na ograniczenie zużycia zasobów i zwiększenie efektywności, co jest szczególnie istotne w kontekście działań krytycznych dla funkcjonowania organizacji,
- kluczowym elementem zarządzania operacyjnego mającego na celu kompleksowe zabezpieczenie łańcucha wartości jest nieustająca adaptacja do zmieniającego się środowiska organizacji.

Lecture & workshop: using OM to combat crime in (1) finance, (2) managing people, (3) energy and (4) insurance

Warsztat służył pogłębieniu wiedzy uczestników na temat zagadnień wprowadzonych podczas paneli *Introduction to operations management (OM): Benihana case* i *Controlling processes: Kristen's Cookie case* oraz wykazaniu zależności pomiędzy nimi. Ważnym wynikiem prac było ujawnienie zależności pomiędzy szeroko pojmowaną zmiennością (niepewnością), a ryzykiem wystąpienia niekorzystnych zdarzeń w prowadzeniu operacji (model Sześć Sigma). Stwierdzono występowanie relacji zwrotnej pomiędzy nieefektywnymi operacjami a zagrożeniem zjawiskami przestępczymi. Podczas dyskusji plenarnej poruszono również problematykę niepewności procesowej i metod jej redukcji w kontekście niwelowania czynników sprzyjających zaistnieniu zjawiska przestępczości oraz sformułowano następujące wnioski:

- stopień zmienności w działalności operacyjnej organizacji może stanowić o jej podatności na nieprawidłowości oraz nadużycia, zatem w kontekście przeciwdziałania przestępczości celowe jest ograniczanie tego zjawiska,
- wdrażając metodykę zarządzania operacyjnego w organizacji, należy pamiętać, że większa efektywność zużycia zasobów wiąże się z ograniczeniem dostępności operacji,
- redukcja zmienności w działalności operacyjnej może być metodą pozwalającą na znaczną redukcję występujących nieprawidłowości.

Cybersecurity and technology risk management

Panel posłużył jako wprowadzenie do zagadnień cyberbezpieczeństwa i zarządzania ryzykiem z perspektywy osoby zarządzającej organizacją. Omówiono warstwowy model dekompozycji problemu bezpieczeństwa jako podstawowy element metodologii tworzenia strategii bezpieczeństwa. Za punkt wyjścia przyjęto tezę, że postęp technologii zabezpieczeń jest pochodną rozwoju metod ataków. Na tym gruncie postulowano, aby strategie bezpieczeństwa w szczególności uwzględniały sposoby reakcji na incydenty, w wyniku których doszło już do naruszenia bezpieczeństwa. W kontekście metodologii działania grup cyberprzestępczych opartej na podejściu ekonomicznym (gdzie atak jest rozumiany jako przedsięwzięcie wymagające poświecenia czasu i zasobów, aby uzyskać maksymalne korzyści), dokonano szeregu obserwacji, które pozwalają ukierunkować działania zmierzające do zapewnienia odporności organizacji na ataki i zaradzić skutkom pomyślnie przeprowadzonych ataków.

What every manager should know about cybersecurity: popular myths and misunderstandings exposed

W trakcie panelu przedyskutowano szereg zagadnień związanych z cyberprzestępczością, w tym (1) model biznesowy przestępstw dokonywanych przy wykorzystaniu sieci Dark Web, (2) zjawisko fałszywego poczucia bezpieczeństwa, którego źródłem są ramowe programy bezpieczeństwa publikowane przez agendy rządowe, a także (3) metody odkrywania luk w zabezpieczeniach infrastruktury informatycznej organizacji. Szczególną uwagę zwrócono na problem powszechnych błędnych przekonań na temat cyberbezpieczeństwa rzutujących na uchybienia w polityce bezpieczeństwa, a także zakresu odpowiedzialności osób zarządzających organizacjami za kwestie bezpieczeństwa informatycznego.

Cybercrime ecosystem: the Dark Web and Cybercrime-as-a-service

Dobór zagadnień w ramach tego panelu miał na celu przedstawienie uczestnikom nieformalnej struktury sieci Internet, w ramach której można wyróżnić trzy warstwy: Surface Web (przestrzeń publiczna), Deep Web (przestrzeń prywatna) i Dark Web (warstwa ukryta, dostępna jedynie za pośrednictwem specjalnej infrastruktury). Warstwa Dark Web jest źródłem nielegalnych materiałów oraz dóbr (ang. *Dream Market*), programów służących do

przeprowadzania ataków na systemy informatyczne, a także rynkiem usług hackerskich (ang. *Cyberattack-as-a-Service*). Wprowadzona została metodologia budowania profilu osobowego atakującego, jako jedno z narzędzi zapobiegania incydentom bezpieczeństwa. Ponadto ekspert przedstawił swoje przewidywania co do zakresu możliwych nadużyć w przyszłości w obszarze bezpieczeństwa cybernetycznego. W ramach drugiej części panelu, prof. Stuart Madnick zaprezentował koncepcję *Cybercrime-as-a-Service*, czyli modelu działania społeczności cyberprzestępców jako sprawnie funkcjonującej organizacji, a także potencjalne zagrożenia i korzyści wynikające z tego zjawiska.

Conflict between data privacy and security

Podczas panelu dyskutowano o konflikcie etycznym odnoszącym się do problemu kompromisu pomiędzy uzyskaniem pożądanego poziomu bezpieczeństwa ogólnego a zachowaniem poufności danych wrażliwych, takich jak dane osobowe. Panel ten, prowadzony przez dra Jeffa Klabena z SRI International, opierał się na przykładach prawdziwych zdarzeń, które wymagały rozwiązania tego rodzaju konfliktów. Dyskusji poddano również szereg dylematów etycznych, których źródłem jest wykorzystywanie najnowszych technologii, np. do celów autonomicznego sterowania pojazdami, w obszarze cywilnym i wojskowym. W trakcie dyskusji uczestnicy stwierdzili, że zakres dostępu do danych prywatnych służący zwiększonemu bezpieczeństwu powinien być świadomym wyborem każdego bezpośredniego i pośredniego użytkownika. Wdrażając tego typu rozwiązania, należy więc rozważyć i zaadresować zróżnicowane preferencje użytkowników końcowych, co usprawni sam proces wdrożenia. W odniesieniu do obszaru zarządzania ludźmi w organizacjach uczestnicy seminarium zwrócili również uwagę, że decyzja dotycząca prywatności użytkownika jest zależna od wielu różnych czynników, w tym bieżących okoliczności i stanu emocjonalnego jednostki. Aby uzyskać jak najwyższy poziom bezpieczeństwa, kluczowe jest zatem stworzenie poczucia realności zagrożeń. Można tego dokonać, wprowadzając odpowiednie programy i inicjatywy edukacyjne.

Trustworthy technologies and innovation: the human factor

W trakcie panelu poprowadzonego przez dra Jeffa Klabena przedstawiono czynnik ludzki jako krytyczny element procesu analizy zagrożeń oraz

budowania strategii bezpieczeństwa organizacji. Wskazano elementy sprzyjające budowaniu kultury bezpieczeństwa organizacji. Zaprezentowano także zestaw prognoz odnoszących się do kierunku rozwoju ekosystemu bezpieczeństwa cybernetycznego stanowiących zestaw kluczowych zaleceń, które należy uwzględniać w procesie budowania oraz utrzymania strategii bezpieczeństwa organizacji.

Do najistotniejszych wniosków uczestników panelu należy zaliczyć stwierdzenie, że zastosowanie tzw. wirtualnych asystentów może stanowić znaczące wsparcie dla systemu bezpieczeństwa organizacji w zakresie ograniczania potencjalnie destruktywnego wpływu tzw. czynnika ludzkiego. W wyniku dyskusji sformułowano tezę, zgodnie z którą wirtualni asystenci mogą przyczynić się do skrócenia czasu reakcji pracowników na incydenty bezpieczeństwa bądź inne istotne zdarzenia biznesowe.

Trustworthy technologies and innovation in the insurance sector

W ramach panelu uczestnicy zapoznali się z najnowszymi osiągnięciami technologicznymi w zakresie wspomagania działalności operacyjnej organizacji sektora ubezpieczeniowego, a także związanymi z nimi potencjalnymi zagrożeniami i wyzwaniami. Zagadnienia wchodzące w zakres tego panelu wpisywały się bezpośrednio w tematykę metod zapobiegania przestępczości. Szczególną uwagę uczestników seminarium dla sektora ubezpieczeniowego zwróciła możliwość wykorzystania innowacyjnych narzędzi bazujących na sztucznej inteligencji pozwalających na ocenę wiarygodności zgłoszonej szkody i identyfikację prób oszustwa poprzez analizę stanu emocjonalnego zgłaszającego i uwzględnienie okoliczności. W wyniku dyskusji uczestnicy wyróżnili kluczowe cechy tego typu narzędzia, włączając w to konieczność zwiększenia jakości obsługi klienta poprzez przyspieszenie procesu rozpatrywania zgłoszeń, a także adaptacje mechanizmów analitycznych narzędzi pod kątem uwarunkowań regionalnych, w tym niuansów fonetyczno-językowych ekspresji emocjonalnej.

Ludzie i kapitał. Perspektywy gospodarki Polski w kontekście wyzwań demograficznych

W ramach panelu zaprezentowano i przedyskutowano czynniki kształtujące wzrost gospodarczy w Polsce i na świecie w kontekście globalnego cyklu koniunkturalnego i zagrożeń niesionych przez jego wahania. Na gruncie

przyjętego szkieletu metodologicznego seminariów panel uzupełnił tematykę prac w zakresie kreowania gotowości do świadomego reagowania w obliczu bieżących wyzwań i zagrożeń (ang. *Be Ready*). Podniesiono także problem przestępczości jako zjawiska ekonomicznego będącego pochodną analizy kosztów i korzyści wynikających z działalności przestępczej w stosunku do legalnych alternatyw. Wskazano czynniki ekonomiczne, które wpływają na skłonność do podejmowania nielegalnych działań, jak również wykazano zależność oddziaływania przestępczości na poziom wzrostu gospodarczego.

Czym jest pieniądz? Zarys historii systemów monetarnych w kontekście bieżących wyzwań i propozycji reform

W ramach panelu, poprzedzonego wprowadzeniem do historii systemów monetarnych, odbyła się dyskusja na temat wyzwań i zagrożeń niesionych przez stosowanie alternatywnych środków płatniczych i korzyści płynących z zastąpienia pieniądza papierowego elektronicznym. Wyjaśniono szereg wątpliwości uczestników dotyczących przestrzeni regulacyjnej wokół kryptowalut, ich roli w systemie płatniczym oraz zagrożeń związanych z ich obrotem. W czasie dyskusji analizowano również zależności pomiędzy przestępczością a rozwojem gospodarczym.

Uczestnicy zgodzili się, że szybki rozwój gospodarczy wpływa znacząco na obniżenie poziomu przestępczości. Wynika to m.in. ze spadku stopy bezrobocia oraz zmniejszania się atrakcyjności działalności przestępczej w stosunku do legalnych alternatyw. Istotna jest również wyrównana dystrybucja majątku narodowego: im mniejsze różnice w dochodach mieszkańców, tym niższy poziom przestępczości. W państwach Unii Europejskiej, w których osiągnięto wysoki poziom rozwoju gospodarczego, obserwuje się stosunkowo niski wpływ przestępczości na życie gospodarcze. Wyjątek stanowią tu niektóre regiony Włoch.

Podkreślono również, że wysoki poziom poczucia bezpieczeństwa mieszkańców jest związany z nakładami na wymiar sprawiedliwości i organy ścigania. W Polsce środki przeznaczane na ten cel są średnio nieco wyższe niż w innych państwach UE, o ile wydatki te są liczone jako udział w PKB. W przypadku kwot nominalnych jest to poniżej średniej unijnej. Oprócz wartości środków przeznaczonych na zwalczanie przestępczości istotna jest również ich alokacja, a więc przeznaczenie na określone cele i działania. W związku

z postępem technologicznym coraz szybciej rośnie zagrożenie ze strony cyberprzestępców, a łatwiej jest ograniczać poziom przestępstw tradycyjnych (chociażby poprzez monitoring). Jednak coraz bardziej wyrafinowane przestępstwa związane np. z kradzieżą danych, kradzieżą środków na rachunkach bankowych itp. wymagają przeznaczania na ich zwalczanie coraz większych kwot. Zjawisko to jest obserwowane w krajach rozwiniętych, np. w Stanach Zjednoczonych, gdzie – pomimo wysokich nakładów na zapewnienie bezpieczeństwa – wzrasta zakres i wartość cyberprzestępstw. Uczestnicy seminariów podkreślali znaczenie zarządzania operacyjnego i podnoszenia poziomu efektywności operacyjnej, dzięki którym środki przeznaczone na zwalczanie przestępczości przynoszą pożądane rezultaty.

2.3. Faza podsumowania

Niniejszy rozdział jest podsumowaniem prac badawczych przeprowadzonych w ramach seminariów naukowych. Faza podsumowania wyników prac tego etapu projektu objęła ocenę zaproszonych prelegentów (ekspertów) oraz treści wystąpień przez uczestników (zob. rozdział 2.3.1), analizę statystyczną odpowiedzi udzielonych podczas badania kwestionariuszowego (zob. rozdział 2.3.2) oraz analizę wyników wypracowanych z grupą fokusową złożoną z uczestników seminariów (zob. rozdział 2.3.3).

2.3.1. Ocena prelegentów, treści wystąpień oraz aspektów organizacyjnych seminariów

W rozdziale uwzględniono ocenę zakresu merytorycznego seminariów oraz ich aspektów organizacyjnych. Zaprezentowane statystyki ocen prelegentów i seminariów zostały sporządzone na podstawie anonimowych kwestionariuszy ankietowych wypełnionych przez uczestników. W celu kompleksowej oceny warsztatów pod względem merytorycznym i organizacyjnym wyodrębniono kryteria przedstawione odpowiednio w dwóch poniższych 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	Efektywność w rozwiązywaniu problemów i wyjaśnianiu wątpliwości
Kryterium nr 5	Poprawa stanu wiedzy z danego zakresu

Tabela 3. Kryteria oceny części organizacyjnej seminariów

Kryterium nr 1	Standard obsługi warsztatów
Kryterium nr 2	Stan sali wykładowej oraz 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. Wyniki podsumowano w diagramach satysfakcji uczestników[11] przedstawionych poniżej (zob. rysunek 2–rysunek 9).

[11] Diagramy satysfakcji uczestników opracowano na podstawie ocen wystawionych w ankiecie ewaluacyjnej. Oceny dla każdego sektora i aspektu (organizacyjnego lub merytorycznego) seminarium zsumowano według zadanej skali, tj. każdej ocenie (w skali od 1 do 5) została przyporządkowana liczba ocen wystawionych. Dla większej przejrzystości przeskalowano liczbę wystąpień ocen do skali 10-stopniowej. Udział zadowolonych uczestników obliczono na podstawie procentowego udziału następujących ocen w całkowitej liczbie wystawionych ocen: dobry (3), bardzo dobry (4) i znacznie powyżej oczekiwań (5).

Sektor finansowy

Rysunek 2. Ocena aspektów merytorycznych seminarium dla sektora finansowego

Źródło: opracowanie własne

Uczestnicy seminarium poświęconego sektorowi finansowemu szczególnie wysoko ocenili wystąpienie prof. Stuarta Madnicka dotyczące funkcjonowania społeczności hackerskiej jako organizacji o rozproszonej infrastrukturze, a także zagrożeń i potencjalnych korzyści związanych z tym zjawiskiem.

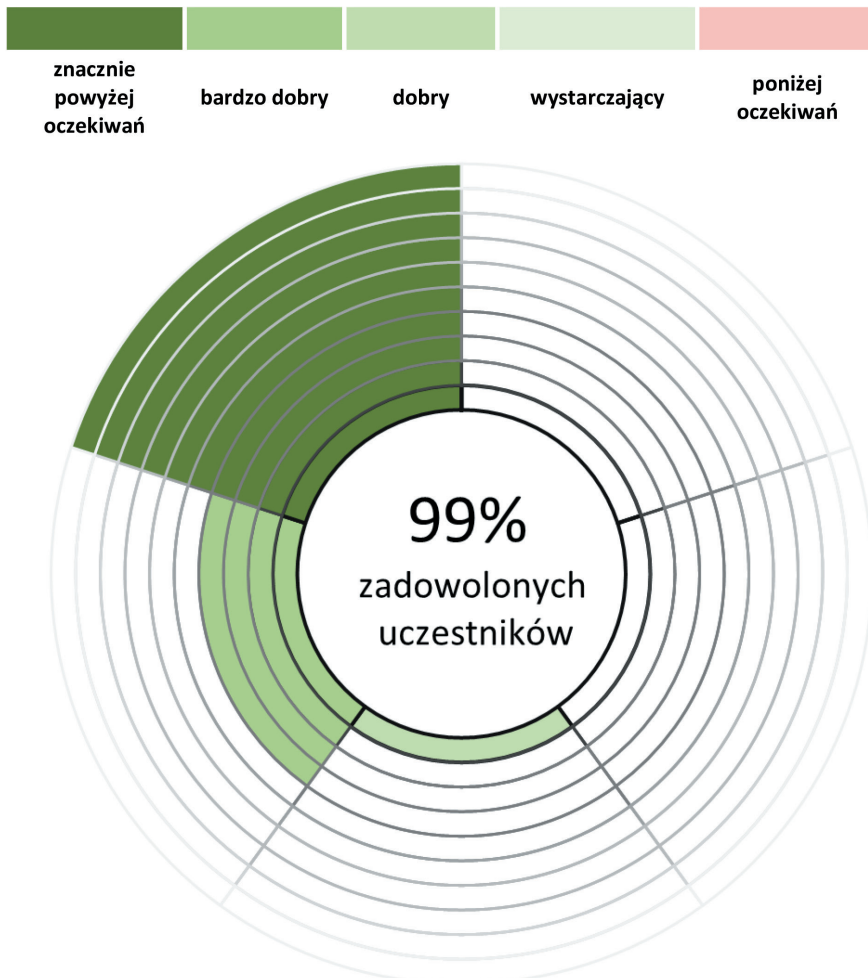
Rysunek 3. Ocena aspektów organizacyjnych seminarium dla sektora finansowego

Źródło: opracowanie własne

Uczestnicy wysoko ocenili również aspekty organizacyjne seminarium, w tym sprawnie poprowadzone zajęcia i wydajne wykorzystanie czasu.

Sektor ubezpieczeniowy

Rysunek 4. Ocena aspektów merytorycznych seminarium dla sektora ubezpieczeniowego

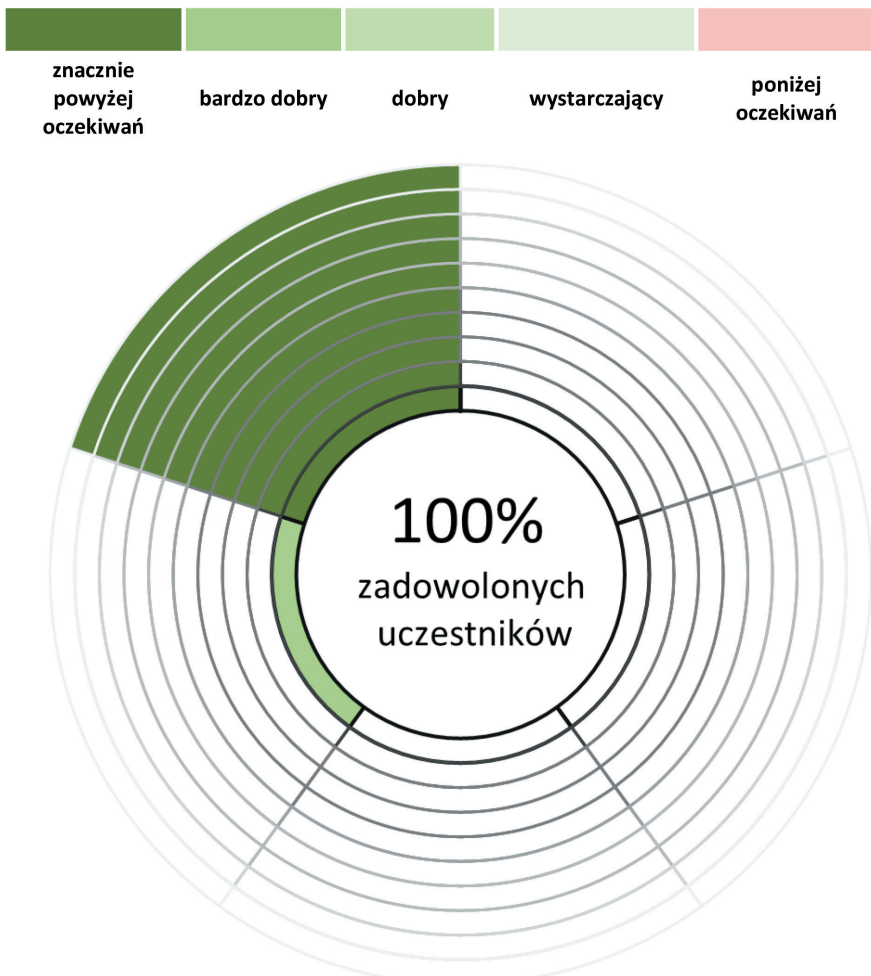


Źródło: opracowanie własne

Tu również najwyżej ocenionym prelegentem był Stuart Madnick. Przedstawiciele sektora ubezpieczeniowego zwrócili szczególną uwagę na problematykę konfliktu powstającego przy zapewnianiu wyższego poziomu

bezpieczeństwa kosztem braku poufności danych wrażliwych oraz wynikających z niego potencjalnych reperkusji.

Rysunek 5. Ocena aspektów organizacyjnych seminarium dla sektora ubezpieczeniowego

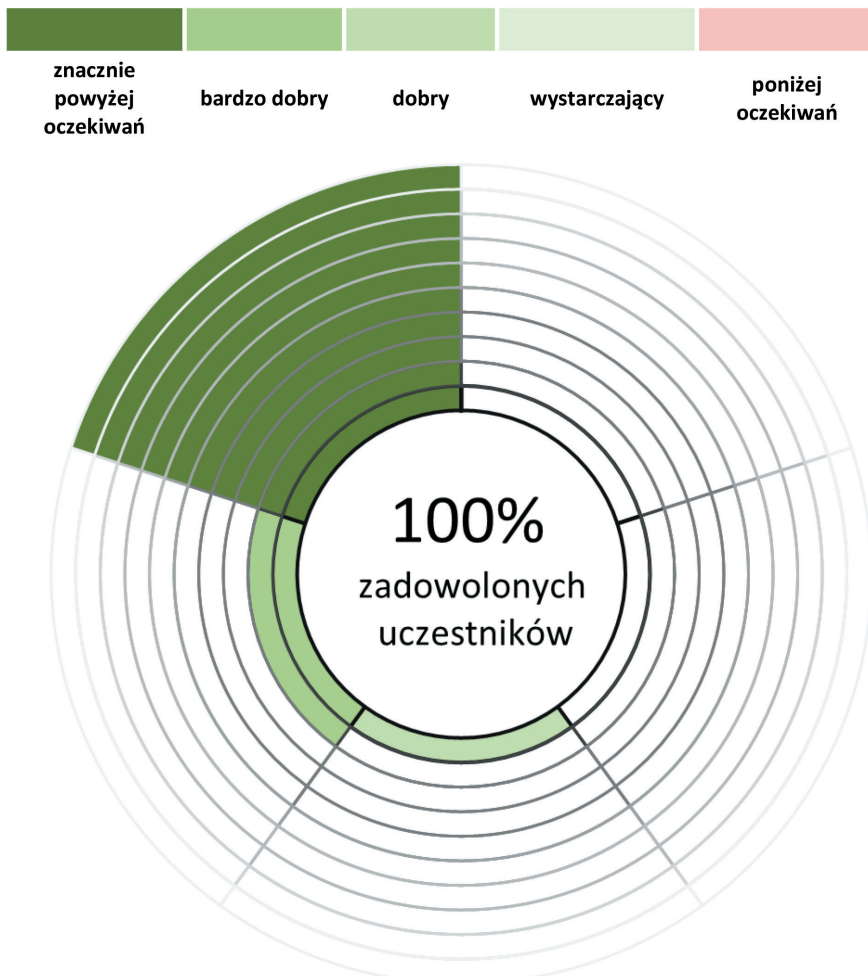


Źródło: opracowanie własne

Wysoko ocenione zostało również wystąpienie Adriana Done'a dotyczące zwiększania efektywności działalności operacyjnej poprzez zastosowanie odpowiedniego modelu zarządzania operacyjnego.

Sektor energetyczny

Rysunek 6. Ocena aspektów merytorycznych seminarium dla sektora energetycznego

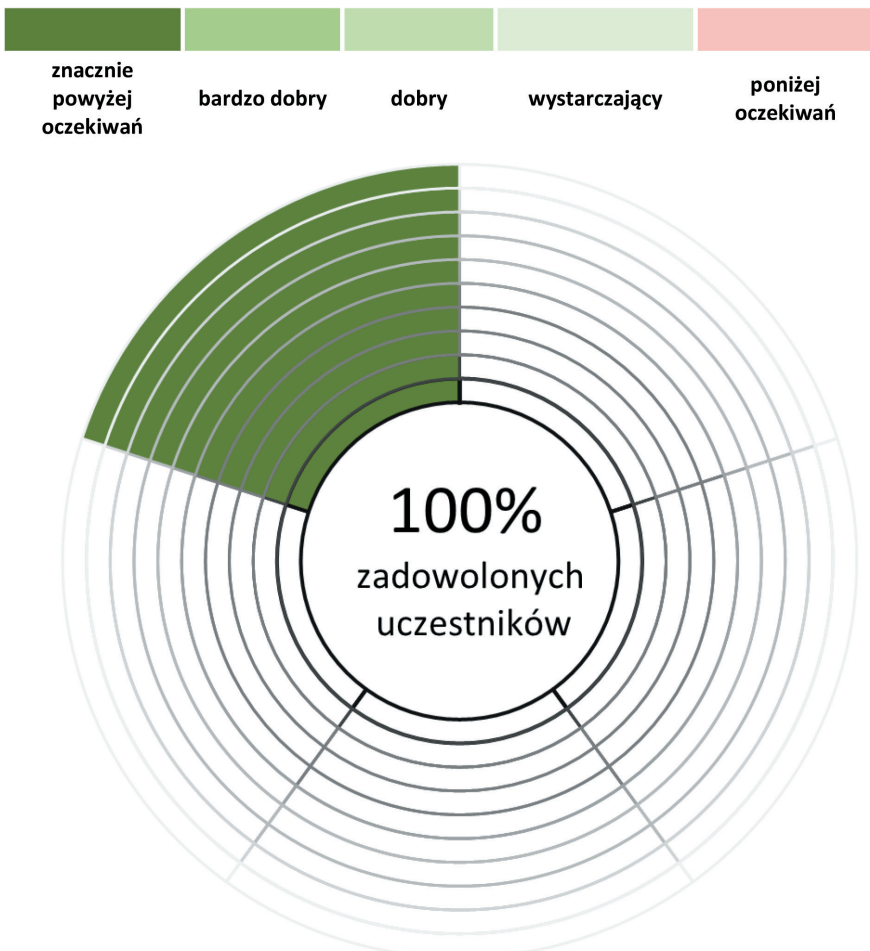


Źródło: opracowanie własne

Największym zainteresowaniem uczestników sektora energetycznego cieszyła się prelekcja Adriana Done'a dotycząca zastosowania metodyki zarządzania operacyjnego w kontekście przeciwdziałania przestępczości i wytwarzania odporności łańcucha wartości organizacji na szkodliwe działania zewnętrzne. Wysokie oceny otrzymał również dr Marcin Mrowiec, który przedstawił

problematykę przyczyn zjawisk przestępczych z punktu widzenia ekonomisty, uwzględniającą zarówno lokalną, jak i globalną sytuację makroekonomiczną, z którą muszą mierzyć się polskie organizacje.

Rysunek 7. Ocena aspektów organizacyjnych seminarium dla sektora energetycznego



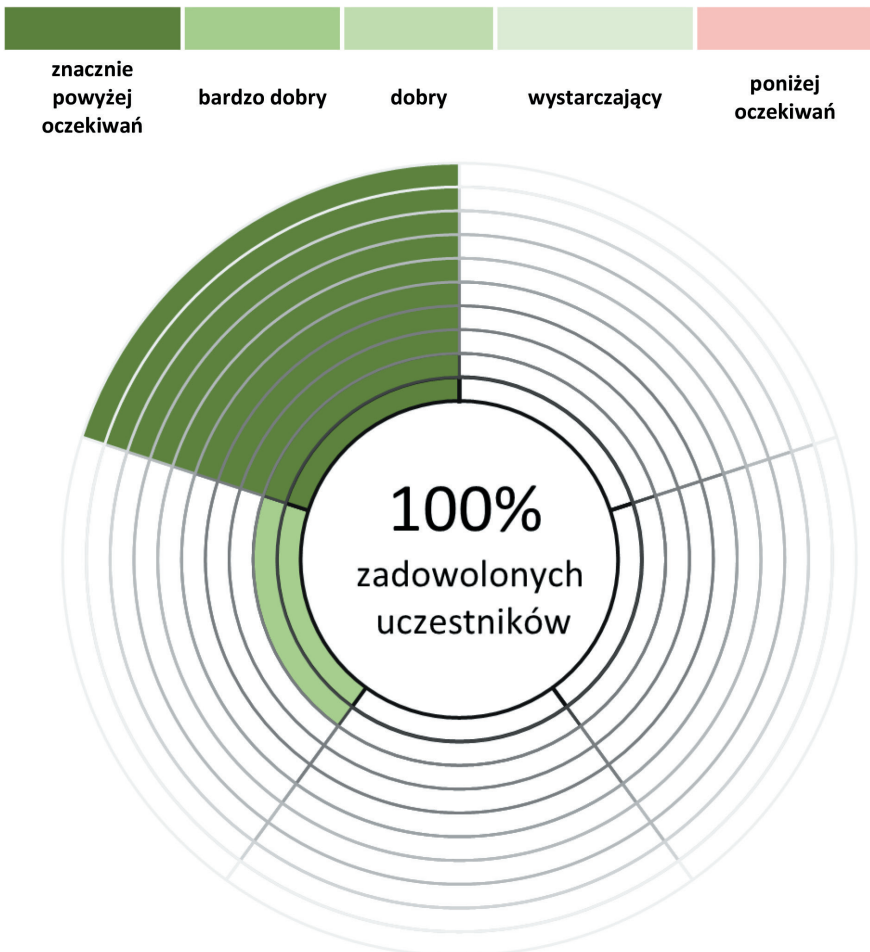
Źródło: opracowanie własne

Rysunek 8. Ocena aspektów merytorycznych seminarium poświęconego zarządzaniu ludźmi w organizacjach

Źródło: opracowanie własne

Najwyższe oceny ponownie otrzymał Adrian Done. Przedstawił problematykę zabezpieczania działalności operacyjnej w zarządzaniu ludźmi w organizacjach. Wysokie noty otrzymała również prelekcja Stuarta Madnicka dotycząca innowacyjnych rozwiązań z zakresu przeciwdziałania cyberprzestępczości w organizacjach na całym świecie.

Rysunek 9. Ocena aspektów organizacyjnych seminarium poświęconego zarządzaniu ludźmi w organizacjach



Źródło: opracowanie własne

Zarówno aspekty merytoryczne, jak i organizacyjne zostały bardzo wysoko ocenione przez uczestników. W szczególności uczestnicy części projektu dla obszaru zarządzania ludźmi w organizacjach podkreślali, że stworzone warunki sprzyjały zarówno rozwojowi personalnemu, jak i naukowemu.

2.3.2. Analiza statystyczna w obszarze metod zapobiegania przestępczości

Prace badawcze przeprowadzone w ramach niniejszej części projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" zostały wzbogacone o analizę statystyczną odpowiedzi udzielonych w badaniu ankietowym (zob. załącznik B – Kwestionariusz ankietowy). Celem analizy było zbadanie korelacji pomiędzy poszczególnymi odpowiedziami oraz wpływu profilu uczestnika na udzielone odpowiedzi, tak aby możliwe było wyłonienie czynników determinujących m.in. poziom wiedzy na temat metod zapobiegania przestępczości oraz ich skuteczności.

Pierwsza część analizy objęła wpływ parametrów personalnych uczestników, tj. doświadczenia zawodowego, wielkości oraz typu reprezentowanej instytucji, a także reprezentowanego sektora, na udzielane odpowiedzi. Głównym założeniem niniejszego modelu jest liniowy wpływ rozważanych parametrów na udzielone odpowiedzi. W celu estymacji istotności parametrów wykorzystana została metoda najmniejszych kwadratów oraz test parametryczny t-Studenta, wraz z założeniem błędu istotności I rodzaju na poziomie α=5% i hipotezą zerową stanowiącą o braku istotnego wpływu na zmienną zależną, tj. udzielone odpowiedzi.

Największy wpływ na opinie uczestników dotyczące możliwości zastosowania w Polsce metod zwalczania przestępczości stosowanych za granicą miała wielkość reprezentowanej organizacji. Nieco mniejsze znaczenie miało tu doświadczenie zawodowe (zob. tabela 4). W przypadku pozostałych parametrów brak jest podstaw do odrzucenia hipotezy zerowej. Jednakże na podstawie powyższych danych można wnioskować, że czynnikiem determinującym postrzeganie przydatności metod zwalczania przestępczości stosowanych za granicą jest staż pracy oraz wielkość organizacji reprezentowanej przez uczestnika.

Tabela 4. Istotność parametrów dla pytania nr 1 (liczba obserwacji n = 41)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,582135	0,179926	3,235	0,0026
Typ organizacji	0,226363	0,335313	0,6751	0,5038
Wielkość organizacji	0,685431	0,169198	4,051	0,0003
Reprezentowany sektor	0,274293	0,157509	1,741	0,0899
Współczynnik korelacji R^2	0,965354			

Podobną korelację istotności można zaobserwować dla pytania dotyczącego przydatności zarządzania operacyjnego w zwalczaniu przestępczości (zob. tabela 5). Warto jednak zauważyć spadek wartości współczynników dla wszystkich rozważanych parametrów. Można zatem przyjąć, że parametrem o pomijalnym wpływie na udzielone odpowiedzi jest typ reprezentowanej organizacji.

Tabela 5. Istotność parametrów dla pytania nr 2 (n =41)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,506778	0,191249	2,650	0,0118
Typ organizacji	0,125157	0,356414	0,3512	0,7275
Wielkość organizacji	0,596934	0,179845	3,319	0,0020
Reprezentowany sektor	0,254223	0,167421	1,518	0,1374
Współczynnik korelacji R^2	0,947867			

Tabela 6. Istotność parametrów dla pytania nr 3 (n = 41)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,555023	0,206445	2,688	0,0107
Typ organizacji	0,345964	0,384734	0,8992	0,3743
Wielkość organizacji	0,461827	0,194135	2,379	0,0226
Reprezentowany sektor	0,136140	0,180723	0,7533	0,4560
Współczynnik korelacji R^2	0,931078			

Również w przypadku pytania nr 3 (zob. załącznik B – Kwestionariusz ankietowy) można jednoznacznie stwierdzić istotność wielkości organizacji i doświadczenia zawodowego jako parametrów wpływających na udzielone odpowiedzi. Szczególne znaczenie dla rozważanego zjawiska ma staż pracy uczestnika (zob. tabela 6). Warto zauważyć, że opinia na temat redukcji kosztów uzyskanej dzięki wprowadzeniu zarządzania operacyjnego w najmniejszym stopniu zależy od reprezentowanego sektora, co może świadczyć o uniwersalności proponowanego rozwiązania.

Największą istotność w kształtowaniu odpowiedzi na pytanie dotyczące potencjalnej efektywności zaprezentowanej metodyki w kontekście zapobiegania przestępczości po raz kolejny należy przypisać wielkości organizacji oraz

doświadczeniu zawodowemu uczestników. Ponadto hipoteza zerowa również została odrzucona w przypadku reprezentowanego sektora (zob. tabela 7).

Tabela 7. Istotność parametrów dla pytania nr 4 (n = 41)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,473554	0,165480	2,862	0,0069
Typ organizacji	0,219041	0,308391	0,7103	0,4820
Wielkość organizacji	0,550992	0,155613	3,541	0,0011
Reprezentowany sektor	0,257640	0,144862	1,779	0,0835
Współczynnik korelacji R^2	0,959192			

Odpowiedzi na pytanie dotyczące znaczenia przejrzystości w zarządzeniu operacyjnym były silnie uzależnione od typu organizacji reprezentowanej przez uczestników oraz ich doświadczenia zawodowego. Uzyskane dane nie dały podstawy do odrzucenia hipotezy zerowej dla pozostałych parametrów. Jednakże z uwagi na małą wartość współczynnika dla reprezentowanego sektora można wnioskować, że ww. parametr posiada pomijalny wpływ na udzielone odpowiedzi (zob. tabela 8).

Tabela 8. Istotność parametrów dla pytania nr 5 (n = 41)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,707970	0,177410	3,991	0,0003
Typ organizacji	0,779019	0,330624	2,356	0,0239
Wielkość organizacji	0,239033	0,166832	1,433	0,1603
Reprezentowany sektor	0,0318337	0,155306	0,2050	0,8387
Współczynnik korelacji R^2	0,951888			

W przypadku opinii na temat potrzeby podejmowania prac nad systemem bezpieczeństwa cybernetycznego w Polsce największą istotnością charakteryzowały się doświadczenie zawodowe i wielkość organizacji (zob. tabela 9). Przeprowadzona analiza parametryczna jest podstawą dla wniosków dotyczących ogólnego wpływu parametrów na udzielone odpowiedzi.

Zaobserwowane dane pozwalają na wyłonienie doświadczenia zawodowego jako parametru o największej istotności w rozważanym modelu.

Tabela 9. Istotność parametrów dla pytania nr 6 (n = 41)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,702222	0,190507	3,686	0,0007
Typ organizacji	0,359959	0,353904	1,017	0,3155
Wielkość organizacji	0,499921	0,179460	2,786	0,0083
Reprezentowany sektor	0,261891	0,167063	1,568	0,1253
Współczynnik korelacji R^2	0,960957			

W dalszej części analizy skupiono się na zbadaniu korelacji pomiędzy odpowiedziami udzielonymi na poszczególne pytania. W tym celu przeprowadzono nieparametryczny test rho-Spearmana dla wybranych pytań (zob. tabela 10). Test ten został wybrany ze względu na wiarygodność pomiaru siły współzależności pomiędzy zmiennymi oraz adekwatność w przypadku braku występowania rozkładu normalnego wśród udzielonych odpowiedzi. Następnie, w celu weryfikacji hipotez o braku korelacji, zastosowano odpowiedni test z założonym poziomem istotności α=5%.

Tabela 10. Wyniki analizy korelacyjnej pomiędzy udzielonymi odpowiedziami dla wybranych pytań

	nr 1	**nr 2**	**nr 3**	**nr 4**	**nr 5**	**nr 6**	**nr 7**
nr 1		0,3373	0,5021	0,0382	0,2995	0,5507	0,5692
nr 2	0,3373		**0,0000**	**0,0000**	**0,0457**	**0,0428**	
nr 3	0,5021	**0,0000**		**0,0000**	**0,0003**	0,9384	0,5597
nr 4	0,0382	**0,0000**	**0,0000**		**0,0008**	0,4011	0,1514
nr 5	0,2995	**0,0457**	**0,0003**	**0,0008**		0,3700	0,3759
nr 6	0,5507	**0,0428**	0,9384	0,4011	0,3700		**0,0398**
nr 7	0,5692	0,2685	0,5597	0,1514	0,3759	**0,0398**	

Dla każdej z par pytań przeprowadzono test korelacji o hipotezie zerowej odpowiadającej brakowi korelacji pomiędzy udzielonymi odpowiedziami. Zgodnie z założonym poziomem istotności, typowym dla badań statystycznych,

można stwierdzić że korelacja z pewnością zachodzi dla wartości $p < 0,05$ (wyniki, dla których odrzucono hipotezę zerową, zostały pogrubione (zob. tabela 10 i załącznik B – Kwestionariusz ankietowy).

2.3.3. Analiza wyników uzyskanych z udziałem grupy fokusowej w kontekście metod zapobiegania przestępczości

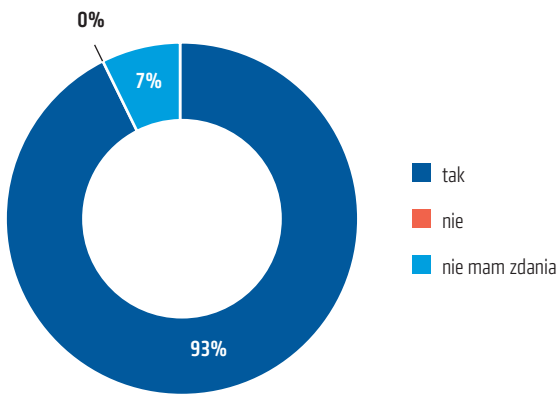
W ramach tego etapu projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" przeprowadzono analizę wyników wypracowanych z grupą fokusową złożoną z uczestników seminariów. Jej celem było jakościowe badanie opinii uczestników w obszarze metod zapobiegania przestępczości w Polsce i na świecie.

Grupa reprezentatywna poddana badaniu składała się z uczestników seminariów, przedstawicieli wyższej kadry kierowniczej spółek prywatnych, państwowych oraz agencji rządowych. Przeprowadzono szereg moderowanych wywiadów w zespołach o różnej liczebności (dyskusje plenarne oraz grupowe) oraz badanie kwestionariuszowe dotyczące opinii uczestników na temat metod przeciwdziałania przestępczości stosowanych obecnie w Polsce i na świecie. Przeprowadzone wywiady tematyczne, moderowane przez wybitnych ekspertów zaproszonych do projektu, miały na celu rekonstrukcję sposobu postrzegania skuteczności obecnie stosowanych metod zapobiegania przestępczości oraz reakcji na metody opierające się na innowacjach technologicznych i organizacyjnych. Badanie ankietowe przeprowadzone po zakończeniu seminariów miało na celu ilościowy pomiar w odniesieniu do rozważanych zjawisk, co pozwoliło zweryfikować opinie dotyczące zaproponowanych innowacyjnych rozwiązań z zakresu zapobiegania przestępczości i prawdopodobieństwa ich wdrożenia w Polsce.

Początkowy etap wywiadu koncentrował się na weryfikacji opinii na temat użyteczności zagranicznych metod zapobiegania przestępczości w Polsce. Podczas dyskusji grupowych i plenarnych skupiono się na metodach bazujących na innowacyjnych rozwiązaniach technologicznych, włączając w to rozwiązania oparte na sztucznej inteligencji, uczeniu maszynowym oraz organizacyjne. Obejmowały one m.in. rozwiązania polegające na wdrożeniu zarządzania operacyjnego w obszarze przeciwdziałania przestępczości.

Głównym elementem dyskusji była możliwość wdrożenia rozwiązań stosowanych za granicą w kontekście uwarunkowań panujących w polskich przedsiębiorstwach. Aż 93 proc. uczestników stwierdziło, że wykorzystanie ww. metod jest możliwe, pomimo występujących różnic kulturowo-społecznych (zob. rysunek 10). W wyniku dyskusji uczestnicy, wspólnie z zaproszonymi ekspertami, zauważyli że zaproponowane rozwiązania wykorzystują bardziej ogólne mechanizmy detekcji działalności przestępczej, które nie są charakterystyczne dla danego regionu, bądź grupy społecznej, co stanowi o ich skalowalności i adaptowalności. Ponad połowa uczestników uznała, że rozważane rozwiązania nie mogą zostać zaimplementowane w Polsce w prosty sposób i wymagają wdrożenia z uwzględnieniem uwarunkowań i specyfiki przestępstw o charakterze lokalnym.

Rysunek 10. Rozkład odpowiedzi uczestników na pytanie „Czy sposoby przeciwdziałania przestępczości stosowane za granicą mogą być Pani/Pana zdaniem wykorzystane w Polsce?"

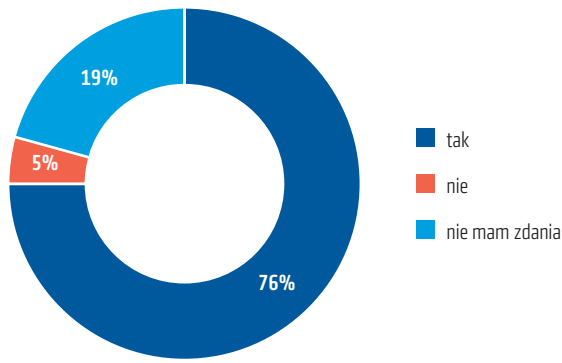


Źródło: opracowanie własne

Następnie dyskusja skupiła się na innowacyjnym zastosowaniu zarządzania operacyjnego w procesach, jako metodzie przeciwdziałania przestępczości. Pierwszy etap stanowiła bardziej ogólna debata na temat skłonności do wdrażania elementów zarządzania operacyjnego w organizacjach macierzystych uczestników seminariów. Jej celem było wstępne zweryfikowanie poziomu adekwatności zaprezentowanej metody w kontekście działalności instytucji reprezentowanych przez uczestników. Aż 76% z nich wyraziło chęć

zastosowania zarządzania operacyjnego w procesach wykorzystywanych w reprezentowanych przez nich organizacjach (zob. rysunek 11), zaś ponad połowa (58 proc.) stwierdziła, że pozwoliłoby to zredukować koszty.

Rysunek 11. Rozkład odpowiedzi uczestników na pytanie „Czy uważa Pan/Pani, że zaprezentowana metodyka zarządzania operacjami mogłaby zostać wdrożona w organizacji, którą Pan/Pani reprezentuje?"



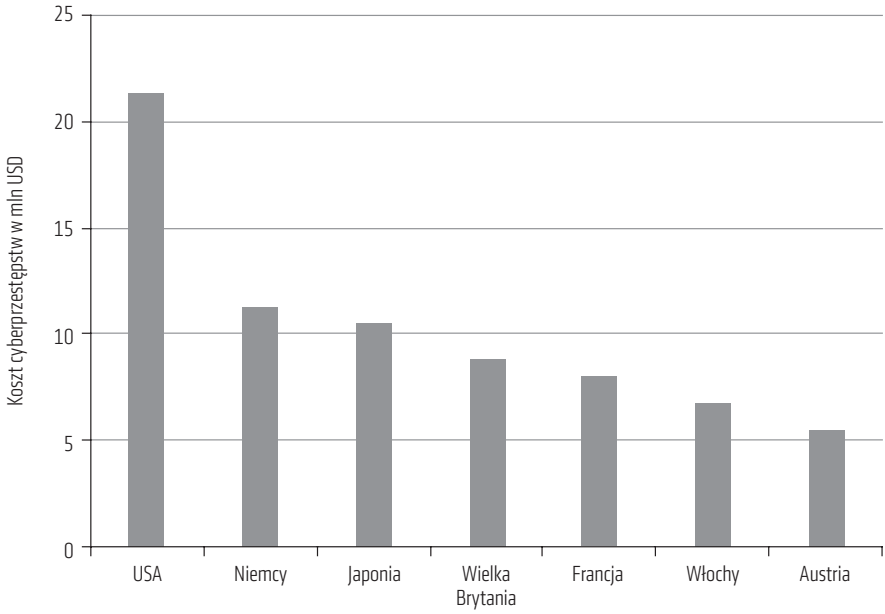
Źródło: opracowanie własne

Kolejnym zagadnieniem poruszonym podczas dyskusji był wpływ działalności przestępczej na koszty ponoszone przez organizacje na całym świecie. Zgodnie z analizą ekspertów Accenture w roku 2017[12] koszt samych cyberataków wyniósł 11,7 mld USD, co oznacza wzrost na poziomie 62 proc. w skali pięciu lat[13]. W poszczególnych krajach poddanych badaniu największy koszt cyberprzestępstw przypada na Stany Zjednoczone i wynosi ponad 21 mln USD (zob. rysunek 12). Choć Polska nie była uwzględniona w przytoczonej analizie, uczestnicy seminariów potwierdzili, że cyberataki w Polsce, pomimo mniejszej skali, mają trend wzrostowy w kontekście ilościowym oraz kosztowym.

[12] Badanie przeprowadzone przez Accenture dotyczyło kosztów cyberprzestępstw w siedmiu krajach dla 254 różnych organizacji.

[13] *Cost of Cyber Crime Study Insights on The Security Investments That Make a Difference*, Ponemon Institute LLC, Accenture 2017, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Rysunek 12. Koszt cyberprzestępczości (w mln USD) dla poszczególnych krajów

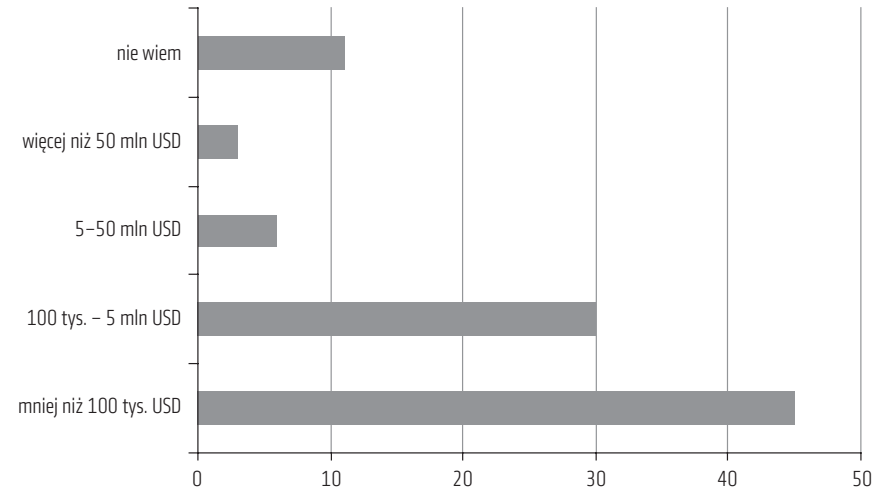


Źródło: opracowanie własne na podstawie danych Accenture[14]

Pomimo wzrostowych tendencji w obszarze cyberprzestępczości zdania uczestników dotyczące konieczności podejmowania prac w zakresie bezpieczeństwa cybernetycznego w Polsce były podzielone (zob. rysunek 14).

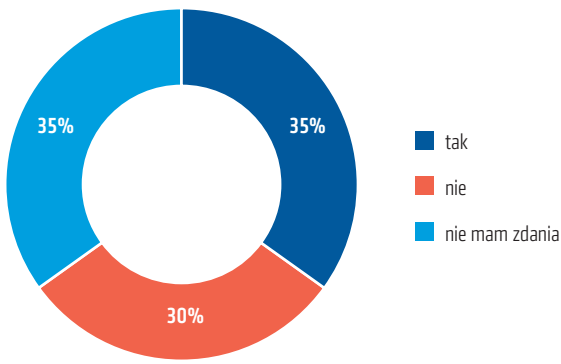
[14] *Cost of Cyber Crime Study Insights on The Security Investments That Make a Difference*…, op. cit.

Rysunek 13. Udział procentowy strat poniesionych przez przedsiębiorstwa na całym świecie przez oszustwa finansowe w latach 2015–2017



Źródło: opracowanie własne na podstawie danych PwC[15]

Rysunek 14. Rozkład odpowiedzi na pytanie „Czy widzi Pan/Pani potrzebę podejmowania prac nad systemem bezpieczeństwa cybernetycznego w Polsce?"



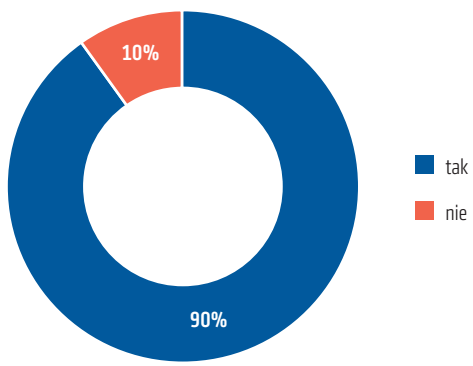
Źródło: opracowanie własne

Uczestnicy podkreślali również, że cyberprzestępstwa stanowią jedynie część kosztów ponoszonych z tytułu wszystkich działań przestępczych. Powyższe stwierdzenie jest zgodne z wynikami badań przeprowadzonych przez

[15] D. Lavion, *Pulling Fraud out of the Shadows*, PwC 2018, Global Economic Crime and Fraud Survey 2018.

PwC. Z raportu dotyczącego przestępstw gospodarczych[16] wynika, że niemal co drugie przedsiębiorstwo padło ofiarą oszustwa finansowego w ciągu ostatnich 24 miesięcy[17]. Uczestnicy zwrócili uwagę, że podobną tendencję można zaobserwować w polskiej gospodarce, co potwierdzają dane MSWiA[18] (wskazują, że w 2017 roku w Polsce doszło do ponad 180 tys. przestępstw o charakterze gospodarczym). Członkowie zaproszonej grupy reprezentatywnej stwierdzili, że tego typu przestępstwa często wynikają z nieprawidłowości w obszarze działalności operacyjnej. Większość uczestników zgodziła się, że wdrożenie metodyki zarządzania zaprezentowanej podczas seminariów może przełożyć się na zwiększenie efektywności wykrywania czynów przestępczych i ich zapobiegania (zob. rysunek 15).

Rysunek 15. Rozkład odpowiedzi na pytanie „Czy wdrożenie zaprezentowanej metodyki mogłoby przyczynić się do uzyskania większej efektywności w wykrywaniu i zapobieganiu przestępczości?"



Źródło: opracowanie własne

W trakcie dyskusji uczestnicy podkreślali też znaczenie przejrzystości w zarządzaniu operacjami w kontekście przeciwdziałania działalności przestępczej. Aż 90% ankietowanych stwierdziło, że większa przejrzystość

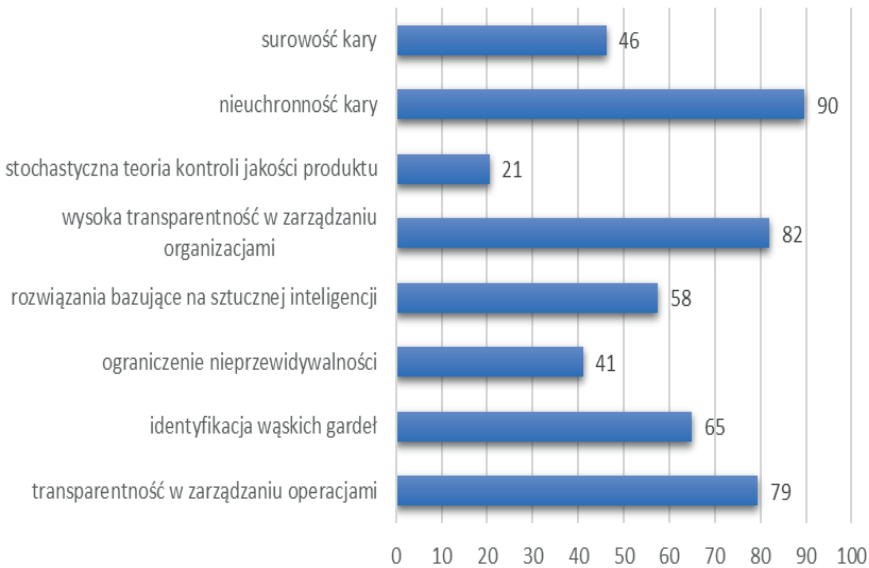
[16] Ibid.

[17] Badanie przeprowadzone pośród 7228 respondentów pochodzących z przedsiębiorstw rozlokowanych na całym świecie.

[18] *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

pozwoliłaby na zwiększenie efektywności w przeciwdziałaniu nieprawidłowościom i przestępstwom. Dalsza dyskusja poświęcona najskuteczniejszym metodom przeciwdziałania przestępczości posłużyła zidentyfikowaniu poziomu świadomości uczestników w rozważanym obszarze. Objęła m.in. kwestie związane z zarządzaniem operacyjnym, w tym ograniczenie nieprzewidywalności czy identyfikację kluczowych elementów działalności operacyjnej, tzw. wąskich gardeł. Uczestnicy w szczególności wskazywali na transparentność, zarówno w działalności operacyjnej, jak i zarządzaniu organizacją, która istotnie wpływa na ograniczanie możliwości powstania nieprawidłowości lub pojawienia się działań przestępczych. Dyskusja dotyczyła również aspektów regulacyjno-prawnych oraz związanych z nimi uwarunkowań społeczno-kulturowych. Uczestnicy wyróżnili przede wszystkim nieuchronność i surowość sankcji jako elementy skutecznego systemu przeciwdziałania przestępstwom, który powinien funkcjonować zarówno jako obowiązujące regulacje prawne, jak i na poziomie wewnętrznym organizacji w postaci ściśle przestrzeganego kodeksu postępowania. Kolejnym zagadnieniem poruszanym w dyskusji było zastosowanie rozwiązań bazujących na sztucznej inteligencji na potrzeby przeciwdziałania przestępczości. Ponad połowa uczestników była przekonana o ich wysokiej skuteczności, jednakże opinie były wprost proporcjonalnie zależne (według statystycznego modelu liniowego – zob. rozdział 2.3.2) od wielkości reprezentowanej organizacji. Zgodnie z przeprowadzoną dyskusją powyższa zależność jest wynikową nie tylko zróżnicowanych potrzeb instytucji różnej wielkości, ale stosunkowo wysokich kosztów wdrożenia i dedykowanej implementacji narzędzi bazujących na sztucznej inteligencji. Opinie uczestników dotyczące najskuteczniejszych metod przeciwdziałania przestępczości w Polsce zostały przedstawione na poniższym wykresie (zob. rysunek 16).

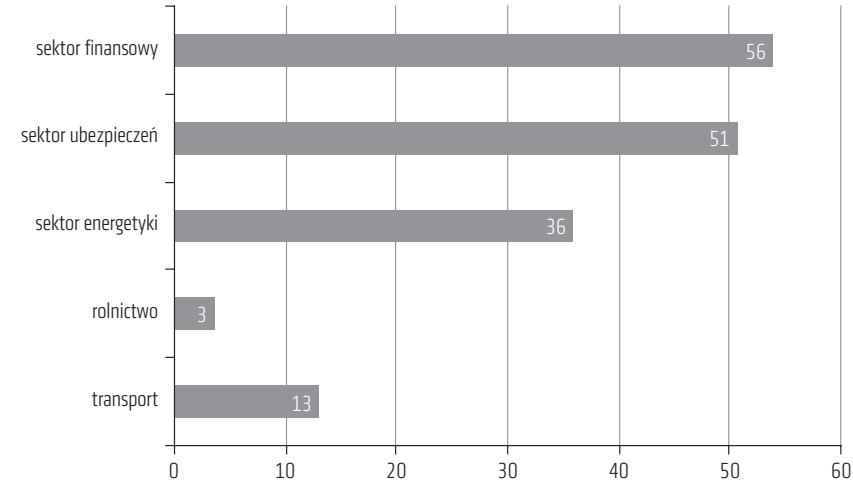
Rysunek 16. Udział procentowy opinii uczestników w zakresie najskuteczniejszych metod zapobiegania przestępczości



Źródło: opracowanie własne

Aby zbadać, które sektory, zdaniem uczestników, stosują najskuteczniejszą metodykę zapobiegania przestępczości, przeprowadzono stosowne badanie ankietowe (zob. pytanie nr 8, załącznik B – Kwestionariusz ankietowy) oraz dyskusję. Uznano, że sektor finansowy podejmuje najskuteczniejsze działania nakierowane na przeciwdziałanie przestępczości. Pełne zestawienie zostało przedstawione na poniższym wykresie (zob. rysunek 17).

Rysunek 17. Rozkład opinii uczestników w zakresie sektorów o najskuteczniejszej metodyce przeciwdziałania przestępczości



Źródło: opracowanie własne

3. Wnioski oraz zalecenia w zakresie wybranych metod zapobiegania przestępczości

Zgodnie z jedną z głównych tez postawionych podczas dyskusji seminaryjnych zagrożenie organizacji przez działalność o charakterze przestępczym wynika nie tylko z jej zdolności do odparcia ataku, ale również z umiejętności napastnika. W niniejszym rozdziale zawarto wnioski i rekomendacje uczestników dotyczące sylwetki przestępcy. Jest to zgodne z zaprezentowaną metodyką zarządzania operacyjnego jako elementu zabezpieczającego działalność operacyjną organizacji. Treści zawarte w niniejszym rozdziale są wynikiem dyskusji przeprowadzonych podczas seminariów oraz wiedzy eksperckiej, którą dzielili się zarówno zaproszeni prelegenci, jak i uczestnicy. Dzięki temu możliwe było kompleksowe ujęcie rozważanych zagadnień wraz z odniesieniem do sytuacji polskiej gospodarki i do uwarunkowań panujących na świecie.

3.1. Identyfikacja profilu przestępcy

Behawioryzm kryminalny (profilowanie kryminalne) jest narzędziem powszechnie wykorzystywanym przez kryminologów i śledczych na całym świecie[19]. Połączenie elementów psychologii stosowanej, nauk behawioralnych oraz kryminalistyki pozwala zidentyfikować podmioty odpowiedzialne za dane przestępstwo lub zbrodnię. Za jednego z pionierów metodyki profilowania kryminalnego uważany jest Cesare Lombroso, którego książka

[19] D.E.V. Malocco, *Criminal Profiling: A Basic Introduction*, 2014.

Criminal Man[20], wydana po raz pierwszy w 1876 roku, jest uznawana za kamień węgielny współczesnej kryminologii[21]. Wyniki badań przeprowadzonych przez Lombrosa na 383 więźniach dotyczyły m.in. wyodrębnienia czynników antropometrycznych decydujących o podwyższonych skłonnościach jednostki do popełnienia przestępstwa. Zgodnie z jego teorią osoba o zwiększonych skłonnościach do popełnienia przestępstwa, tzw. „urodzony przestępca" (ang. *born criminal*), posiada co najmniej pięć z osiemnastu zidentyfikowanych cech fizjonomicznych, w tym m.in. odstające bądź nadzwyczajnie małe uszy, nadmiernie długie ręce lub asymetryczną twarz. Powyższa charakterystyka stanowiła jedną z przełomowych prac w zakresie kryminalistyki i jedno z pierwszych opracowań dotyczących profilu kryminalistycznego, jako wyniku procesu pozwalającego na identyfikację cech osobowych, tendencji behawioralnych, charakterystyki geograficznej i demograficznej, a także cech fizycznych osoby na podstawie popełnionego przez nią przestępstwa[22].

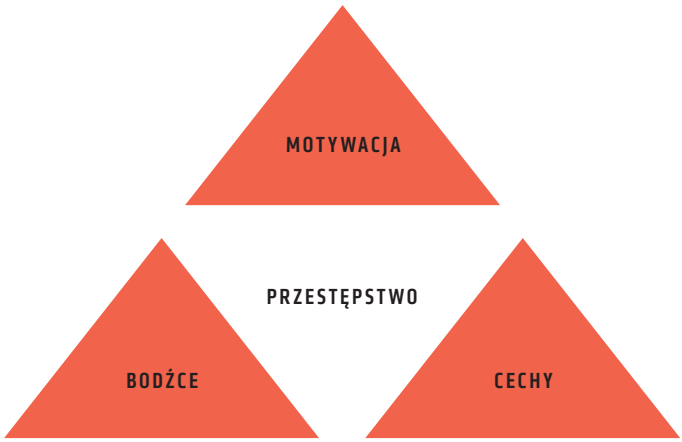
Wśród rozważanego zestawu cech oraz uwarunkowań charakterystycznych dla każdego przestępstwa można wyróżnić trzy główne kategorie opisujące osobę popełniającą przestępstwo, którym można przyporządkować powyższe parametry, tj. motywację, cechy osobowe i bodźce (zob. rysunek 18).

[20] C. Lombroso, M. Gibson, N.H. Rafter, *Criminal Man*, Duke University Press, Durham, NC, 2006.

[21] B.E. Turvey, *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, wyd. 4, Academic Press, Amsterdam Burlington, MA, 2012

[22] R.N. Kocsis, *Criminal Profiling: Principles and Practice*, Humana Press, Totowa, NJ, 2006.

Rysunek 18. Schemat czynników sprzyjających popełnieniu przestępstwa



Źródło: opracowanie własne

Jednym z zagadnień poruszonych w ramach tego etapu seminariów naukowych było wykorzystanie elementów techniki profilowania kryminalnego w kontekście przeciwdziałania przyczynom przestępczości. Główną tezą postawioną przez uczestników była możliwość wykorzystania profilów statystycznych osób popełniających dane przestępstwo dla potrzeb predykcji działań o charakterze przestępczym i wczesnej identyfikacji potencjalnych zagrożeń, co wpisuje się w metodykę zabezpieczania działań operacyjnych. Dyskusja koncentrowała się przede wszystkim na profilach powiązanych z dwoma rodzajami przestępstw, na które, według opinii uczestników, polska gospodarka jest najbardziej narażona, tj. oszustw oraz cyberataków. W ramach seminariów poddano analizie wykorzystanie techniki behawioryzmu kryminalnego jako metody zapobiegania przyczynom przestępczości, ze szczególnym uwzględnieniem profilu cyberprzestępcy oraz oszusta. Zgodnie z wytycznymi sformułowanymi przez uczestników przeprowadzona analiza stanowi pierwszy etap przygotowań do stworzenia predykcyjnego oprogramowania służącego identyfikacji działań o charakterze przestępczym, bazującego na mechanizmach nauczania maszynowego. Stworzenie takiego oprogramowania stanowi jedną z rekomendacji sformułowanych w następstwie seminariów.

3.1.1. Profil oszusta

Zdaniem zaproszonych ekspertów oszustwa stanowią jeden z największych problemów funkcjonowania organizacji na całym świecie. Potwierdzają to badania i analizy[23, 24]. Choć nakłady na ograniczanie i wykrywanie oszustw rosną, nie przekładają się wcale na ich spadek: w ostatnich latach tego typu przestępstwa utrzymały się na niezmiennym poziomie. Uczestnicy seminariów wskazywali, że zjawisko to może być spowodowane tzw. paradoksem kontrolnym[25], tj. znacznym wzrostem liczby wykrywanych oszustw wynikającym z wprowadzenia dodatkowych zabiegów i środków ochronnych. Ponadto zagrożenie oszustwami pozostaje wysokie niemal bez względu na sektor, czy wielkość organizacji, pomimo iż większe organizacje stykają się z proporcjonalnie wyższą liczbą oszustw. W wyniku dyskusji zaproponowano wykorzystanie technik behawioryzmu kryminalnego w działaniach zapobiegawczych. W tym celu, w oparciu o opinie uczestników oraz zaproszonych ekspertów, a także analizy przeprowadzone przez uznane instytucje na całym świecie, stworzono profil oszusta oraz jego proces ewolucji w czasie. Jest to punkt wyjścia dla dalszych badań zainicjowanych przez niniejszy projekt.

Nawiązując do klasyfikacji czynników sprzyjających przestępstwu (zob. rysunek 18), w przypadku oszustwa można wyróżnić trzy czynniki skłaniające do jego popełnienia, tj.:

- okazja do popełnienia oszustwa, np. brak transparentności w kulturze organizacji,
- motywacja do oszustwa, np. zła sytuacja materialna oszusta,
- możliwość racjonalizacji swojego postępowania, np. chęć poprawy wyników finansowych organizacji poprzez ukrycie straty lub kosztów.

Pierwszym etapem identyfikacji czynników sprzyjających popełnieniu przestępstwa było wyróżnienie motywacji oraz racjonalizacji, która im

---

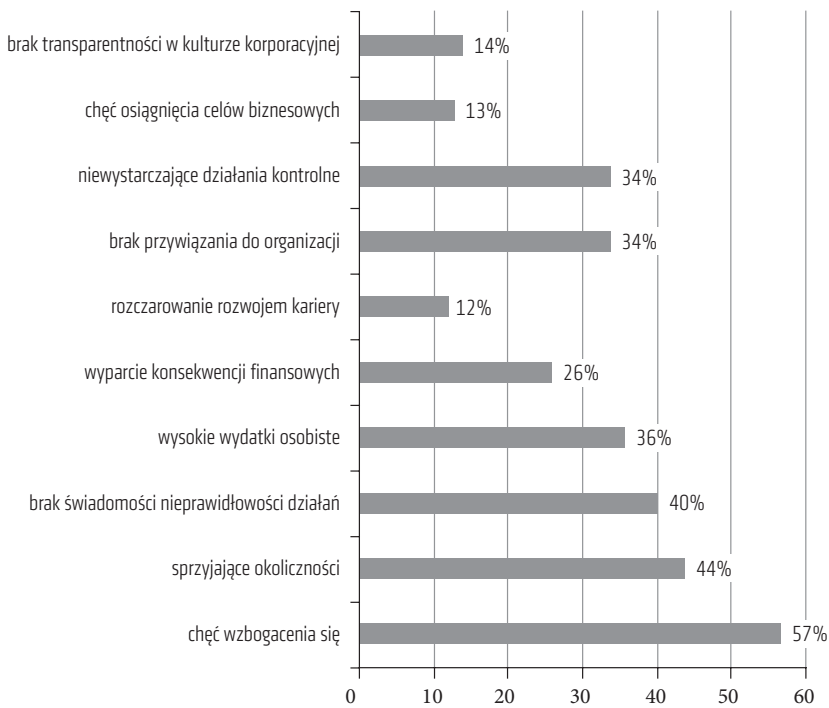
[23] C. Nestler i in., *Economic Crime: People, Culture and Controls. The 4th Biennial Global Economic Crime Survey*, Martin Luther University, Investigations and Forensic Services, PwC 2007, https://www.pwc.com/gx/en/economic-crime-survey/pdf/gecs_engineering_and_construction_supplement.pdf

[24] *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*, Association of Certified Fraud Examiners, Austin, Texas, USA, 2018.

[25] E. Hacker, A. Nilsson, *Fraud, Corruption and the Paradox of Control*, w: The Southern Business & Economic Journal, 2008, t. 31, nr 3/4, s. 49–71.

towarzyszy. Według światowych badań[26, 27] głównymi motywami popełniania oszustwa jest chęć wzbogacenia się (chciwość), sprzyjające okoliczności oraz brak świadomości nieprawidłowości działań. Najczęstszą racjonalizacją wykorzystywaną przez oszustów jest chęć osiągnięcia zakładanych celów biznesowych przez reprezentowaną organizację. Zestawienie dotyczące udziału poszczególnych czynników skłaniających do oszustwa przedstawia poniższy rysunek (zob. rysunek 19).

Rysunek 19. Udział procentowy motywów i okoliczności sprzyjających popełnianiu oszustwa



Źródło: opracowanie własne na podstawie danych PwC[28]

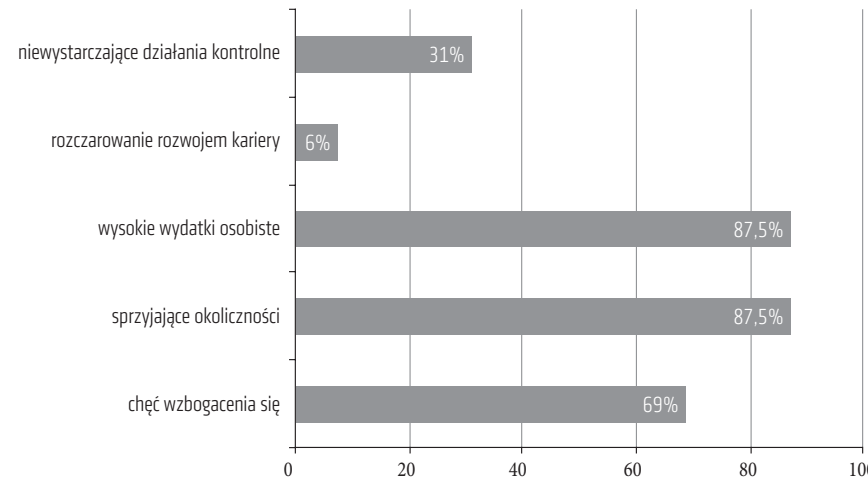
[26] P. Marais i in., *Global Profiles of the Fraudster: Technology Enables and Weak Controls Fuel the Fraud*, KPMG International, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-thefraudster.pdf (dostęp: 05.2016).

[27] C. Nestler i in., *Economic Crime: People…*, op. cit.

[28] Ibid.

Podobne badania przeprowadzone w Polsce[29] wykazały, że najpowszechniejszymi czynnikami na tym rynku są sprzyjające okoliczności (87,5%) oraz wysokie koszty życia (87,5%). Uczestnicy seminariów podkreślali również, że motywacją do popełnienia oszustwa w ich organizacjach były przede wszystkim kwestie finansowe (chęć wzbogacenia się), co również znajduje odzwierciedlenie w badaniu przeprowadzonym przez KPMG[30]. Pełne zestawienie udziału poszczególnych czynników przedstawiono poniżej (zob. rysunek 20).

Rysunek 20. Udział procentowy motywów i okoliczności sprzyjających popełnianiu oszustwa w Polsce



Źródło: opracowanie własne na podstawie danych KPMG[31]

Dalsza dyskusja poświęcona została analizie profilu oszusta pod kątem cech demograficznych, tj. płci, wykształcenia, wieku, stażu pracy oraz rodzaju pełnionej funkcji i ich wpływu na popełniane przestępstwa. W tym celu uczestnicy seminariów zalecili analizę dostępnych danych w zakresie popełnianych oszustw na przestrzeni lat, co pozwoli na zidentyfikowanie tendencji w ramach rozważanego zjawiska.

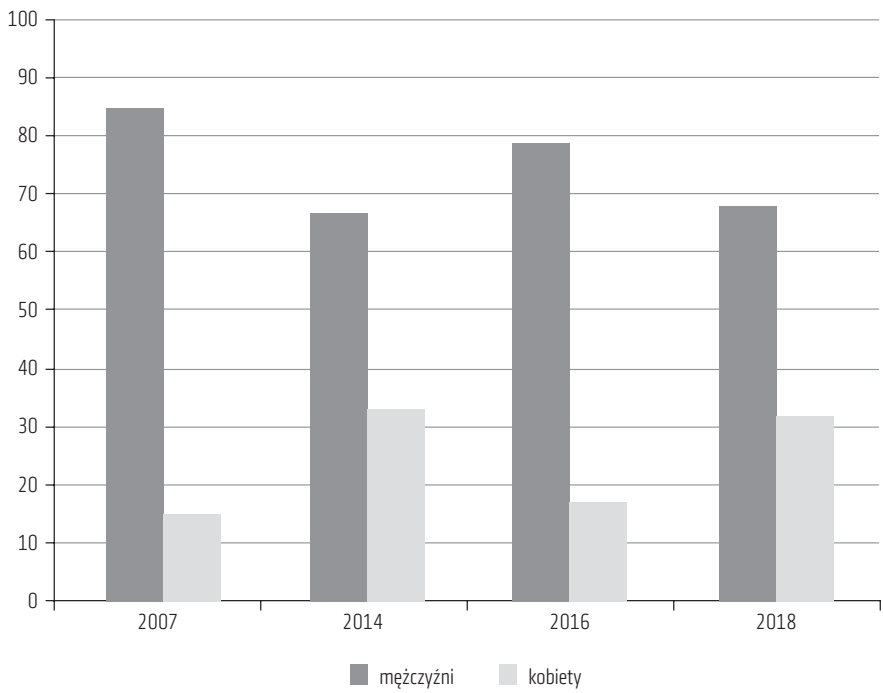
[29] A. Gawrońska-Malec i in., *Profil korporacyjnego oszusta Edycja 2016*, KPMG w Polsce 2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/pl-Raport-KPMG-Profil-korporacyjnego-oszusta.pdf

[30] Ibid.

[31] Ibid.

Pierwszy etap analizy dotyczył weryfikacji płci oszusta, jako potencjalnego czynnika ostrzegawczego. Aby zbadać utrzymujący się trend, zestawiono dane obrazujące udział osób obu płci w oszustwach w latach 2007–2018 (zob. rysunek 21). Ze zgromadzonych danych wynika, że dużo większy udział w oszustwach na całym świecie mają mężczyźni. Jest to zgodne z opinią uczestników seminariów, którzy od wielu lat obserwują podobną tendencję w Polsce. Powyższą tezę potwierdzają niezależne badania przeprowadzone przez KPMG, według których aż 87,5% oszustw w 2016 roku popełnili mężczyźni[32].

Rysunek 21. Udział osób obydwu płci w oszustwach na świecie dla lat 2007, 2014, 2016 i 2018



Źródło: opracowanie własne na podstawie danych PwC[33], ACFE[34], [35] oraz KPMG[36]

[32] Ibid.

[33] C. Nestler i in., *Economic Crime: People*…, op. cit.

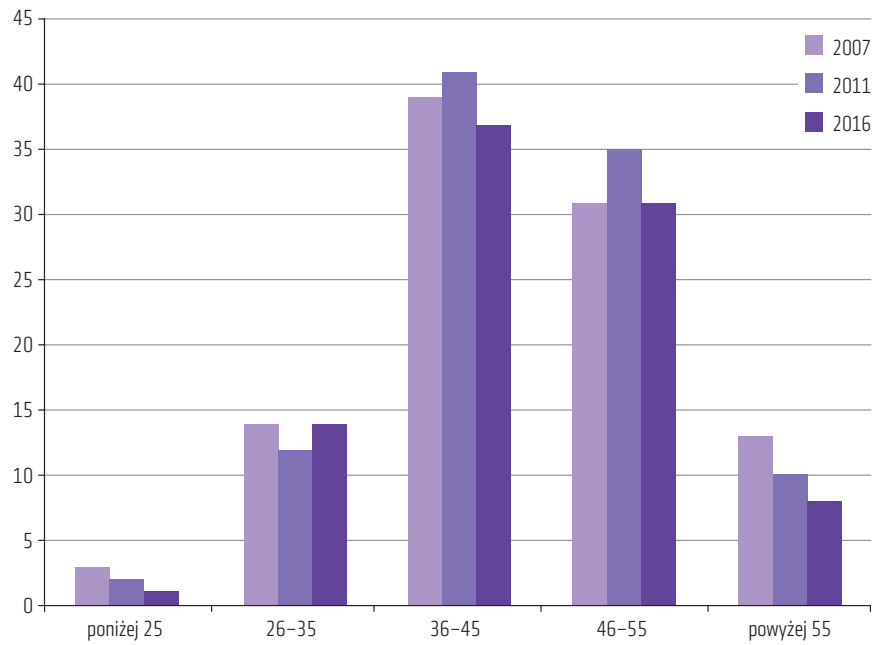
[34] *Report to the Nations: On Occupational Fraud and Abuse 2014*, Association of Certified Fraud Examiners, Austin, Texas, 2014, Global Fraud Study, https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

[35] *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*…, op. cit.

[36] P. Marais i in., *Global Profiles of the Fraudster…*, op. cit.

Kolejnym zagadnieniem poddanym analizie był związek pomiędzy wiekiem osoby a skłonnością do popełniania oszustwa. Na podstawie dostępnych danych można stwierdzić, że średnio niemal połowa oszustw jest popełniana przez osoby między 36. a 45. rokiem życia, zaś drugą grupę o podwyższonym ryzyku stanowią ludzie w wieku od 46 do 55 lat (zob. rysunek 22). Obserwując znaczny spadek w liczbie popełnianych oszustw poza dwoma rozważanymi grupami wiekowymi, można zauważyć, że jedynie co czwarte oszustwo nie jest popełniane przez osoby w wieku od 26 do 55 lat. Na podstawie wiedzy eksperckiej uczestników można również stwierdzić, że podobna tendencja obserwowana jest w Polsce gdzie według badań KPMG[37] 81 proc. oszustw zostało popełnionych z udziałem osób w wieku od 26 do 55 lat.

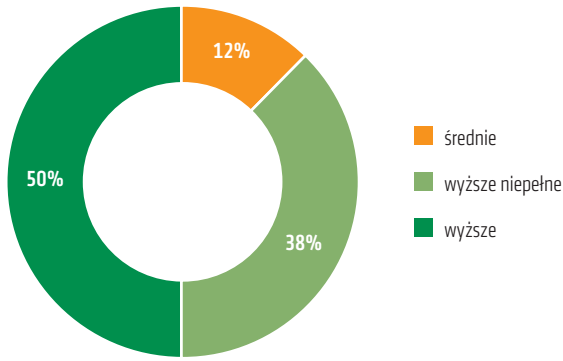
Rysunek 22. Udział w oszustwach osób z różnych przedziałów wiekowych dla lat 2007, 2011, 2016



Źródło: opracowanie własne na podstawie danych KPMG[38] i ACFE[39]

[37] A. Gawrońska-Malec i in., *Profil korporacyjnego oszusta Edycja 2016*…, op. cit.
[38] P. Marais i in., *Global Profiles of the Fraudster*…, op. cit..
[39] *Report to the Nations: On Occupational Fraud and Abuse 2014*…, op. cit.

Rysunek 23. Podział osób popełniających oszustwa z uwzględnieniem poziomu wykształcenia



Źródło: opracowanie własne na podstawie danych PwC[40]

Kolejnym zagadnieniem poruszonym w ramach dyskusji seminaryjnej była zależność pomiędzy poziomem wykształcenia a skłonnością do popełnienia oszustwa. Zgodnie z wiedzą ekspercką uczestników, większość oszustw korporacyjnych w Polsce jest popełniana przez osoby z wyższym wykształceniem, bądź wyższym niepełnym. Podobną tendencję można dostrzec w badaniu przeprowadzonym przez PwC, które wykazało że aż połowa tego typu przestępstw jest popełniana przez osoby, które ukończyły studia wyższe. Jednak w przypadku innych oszustw, włączając w to m.in. wyłudzenia oraz oszustwa ubezpieczeniowe, zależność ta nie jest tak jednoznaczna.

Zgodnie z wiedzą ekspercką uczestników niektóre dane sugerują, że większą skłonność do popełniania przestępstw przejawiają osoby z niższym wykształceniem tj. podstawowym lub średnim. Wobec braku dostatecznych danych należy uznać poziom wykształcenia jako zmienną obarczoną dużą niepewnością przy tworzeniu profilu oszusta. Aby zwiększyć wiarygodność rozważanej zmiennej, uczestnicy seminariów zalecili dalsze badania związane z wpływem poziomu wykształcenia oraz innych cech demograficznych na skłonność do popełniania oszustw oraz ich skalę.

Dalsza część analizy skupiła się na czynnikach związanych z funkcjonowaniem jednostki w organizacji. Wzięto pod uwagę staż pracy, dział zatrudnienia oraz piastowane stanowisko.

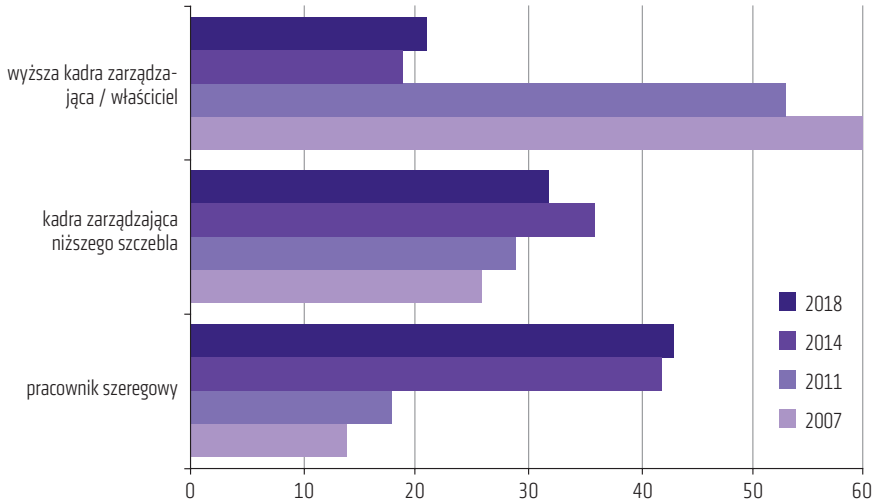
[40] C. Nestler i in., *Economic Crime: People…*, op. cit.

Pierwszym parametrem poddanym analizie było piastowane stanowisko. Można zaobserwować, że w ostatnich latach udział pracowników szeregowych w oszustwach gwałtownie wzrósł, zaś zmalał udział przedstawicieli wyższej kadry zarządzającej (zob. rysunek 24). Uczestnicy seminariów potwierdzili, że w ostatnich latach podobny trend utrzymuje się w Polsce, tj. obserwuje się większy udział oszustw popełnianych przez pracowników szeregowych niż pracowników pełniących inne funkcje, jednakże w mniejszej skali. Zaproszeni eksperci podkreślali również, że w zależności od pełnionego stanowiska, oszustwa często przybierają różną skalę, tj. oszustwa przedstawicieli wyższej kadry zarządzającej dotyczą znacznie większych kwot niż w przypadku pracowników szeregowych, co łatwo można powiązać z zakresem kompetencji osoby popełniającej oszustwo. Powyższą tezę potwierdza również analiza przeprowadzona przez ACFE, gdzie wykazano, że średnie straty wynikające z oszustwa mogą wahać się w granicach od 75 tys. do 500 tys. USD w zależności od roli pełnionej przez osobę popełniającą przestępstwo[41].

Kolejnym z rozważonych czynników ryzyka był dział zatrudnienia oszusta. Jak wykazały dostępne dane oraz wiedza ekspercka uczestników, departamentem gdzie popełnia się najwięcej oszustw i gdzie poziom popełnianych oszustw jest najbardziej stabilny, jest dział operacyjny (zob. rysunek 25). W związku z powyższym uczestnicy podkreślali również znaczenie wprowadzenia do organizacji skutecznej metodyki zarządzania operacyjnego pozwalającej na ograniczenie tego problemu. W przypadku innych działów widoczny jest spadek udziału popełnianych oszustw na rzecz innych obszarów działalności organizacji.

[41] *Report to the Nations: On Occupational Fraud and Abuse 2014…*, op. cit.

Rysunek 24. Rodzaj funkcji pełnionej przez osoby popełniające wykryte oszustwo z podziałem na lata



Źródło: opracowanie własne na podstawie danych KPMG[42] i ACFE[43, 44]

Ostatnią z cech poddanych analizie w kontekście czynników zwiększających ryzyko popełnienia oszustwa jest staż pracownika w danej organizacji. Przeanalizowano dostępne dane[45, 46] dotyczące udziału pracowników o różnym stażu w oszustwach w latach 2007, 2011 i 2014 (zob. rysunek 26). Na ich podstawie zaobserwować można tendencję spadkową wśród osób pracujących powyżej trzech lat w danej organizacji. Szczególną uwagę uczestników zwrócił również wysoki i stabilny, w rozważanym okresie, udział osób o stażu pracy z przedziału od sześciu do 10 lat, co może sugerować obszar o podwyższonym ryzyku. Biorąc pod uwagę powyższe obserwacje, uczestnicy zalecili dalsze badania w zakresie tworzenia sieci powiązań formalnych i nieformalnych w organizacjach dla potrzeb identyfikacji potencjalnych zagrożeń.

---

42 P.D. Oswalt i in., *Who is the Typical Fraudster? KPMG Analysis of Global Patterns of Fraud*, KPMG, USA 2011, https://www.ub.unibas.ch/digi/a125/sachdok/2011/BAU_1_5663361.pdf

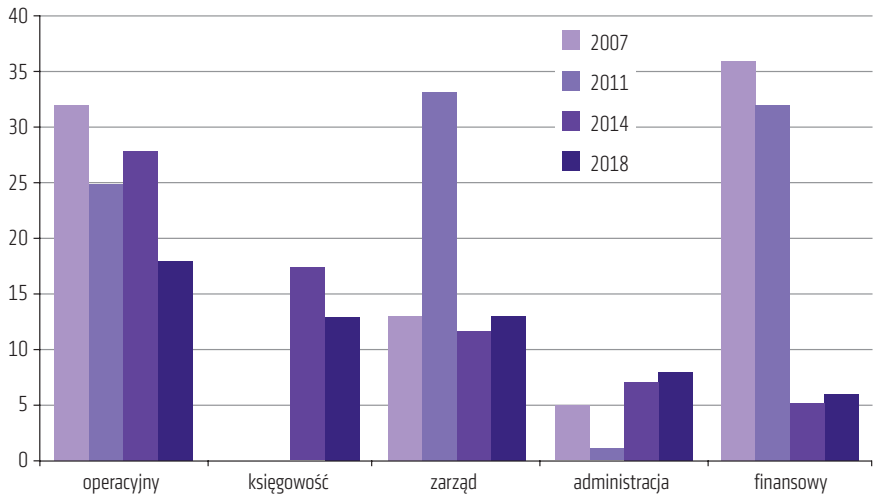
43 *Report to the Nations: On Occupational Fraud and Abuse 2014…*, op. cit.

44 *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse…*, op. cit.

45 P.D. Oswalt i in., *Who is the Typical Fraudster? KPMG Analysis…*, op.cit.

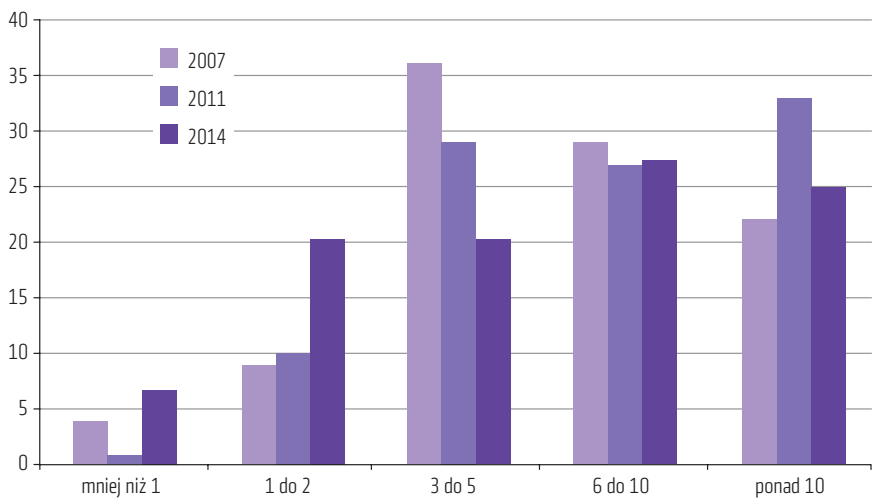
46 *Report to the Nations: On Occupational Fraud and Abuse 2014…*, op. cit.

Rysunek 25. Udział pracowników poszczególnych działów organizacji w oszustwach z podziałem na lata



Źródło: opracowanie własne na podstawie danych PwC[47], KPMG[48] i ACFE[49]

Rysunek 26. Udział w oszustwach pracowników o różnym stażu pracy



Źródło: opracowanie własne na podstawie danych KPMG i ACFE

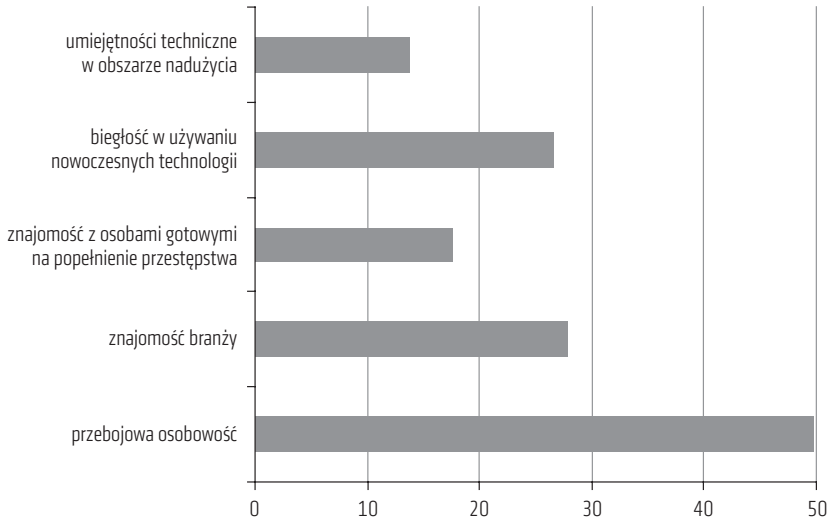
[47] C. Nestler i in., *Economic Crime: People…*, op. cit.
[48] P. Marais i in., *Global Profiles of the Fraudster…*, op. cit.
[49] *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse…*, op. cit.

Dalsza dyskusja seminaryjna dotyczyła weryfikacji oraz identyfikacji umiejętności charakterystycznych dla sprawców oszustw w organizacjach w Polsce i na świecie. Według opinii uczestników oszuści w Polsce charakteryzują się przede wszystkim dużą znajomością branży oraz mechanizmów funkcjonowania organizacji. Powyższą tezę potwierdza badanie przeprowadzone przez KPMG[50], zgodnie z którym aż 87,5 proc. analizowanych oszustw w Polsce w roku 2016 zostało popełnionych przez osoby o dużej znajomości branży, w której działała organizacja. Dodatkowo, w ramach ww. analizy, wyróżniono inne cechy wspólne charakteryzujące sprawców oszustw poddanych badaniu, w tym:

- znajomość branży (87,5 proc.),
- pewność siebie i asertywność (68,8 proc.),
- wysokie umiejętności w zakresie wykorzystywania nowoczesnych technologii (12,5 proc.),
- powiązania formalne bądź nieformalne z osobami gotowymi na popełnienie przestępstwa (37,6 proc.),
- wysoki poziom wiedzy technicznej w obszarze, w którym wystąpiło oszustwo (6,3 proc.).

[50] A. Gawrońska-Malec i in., *Profil korporacyjnego oszusta, Edycja 2016*…, op. cit.

Rysunek 27. Udział oszustów wykazujących poszczególne umiejętności w przestępstwach popełnionych w roku 2016



Źródło: opracowanie własne na podstawie danych KPGM[51]

Analogiczna analiza dotycząca najczęściej występujących umiejętności wśród sprawców oszustw została przeprowadzona dla danych dotyczących tego typu przestępstw popełnionych w 81 krajach na całym świecie (zob. rysunek 27). Niemal połowę oszustw w 2016 roku (49,5 proc.) popełniły osoby dobrze znające branżę. Podobny trend obserwowany jest w Polsce, co potwierdzają zarówno dane, jak i opinia zaproszonych ekspertów.

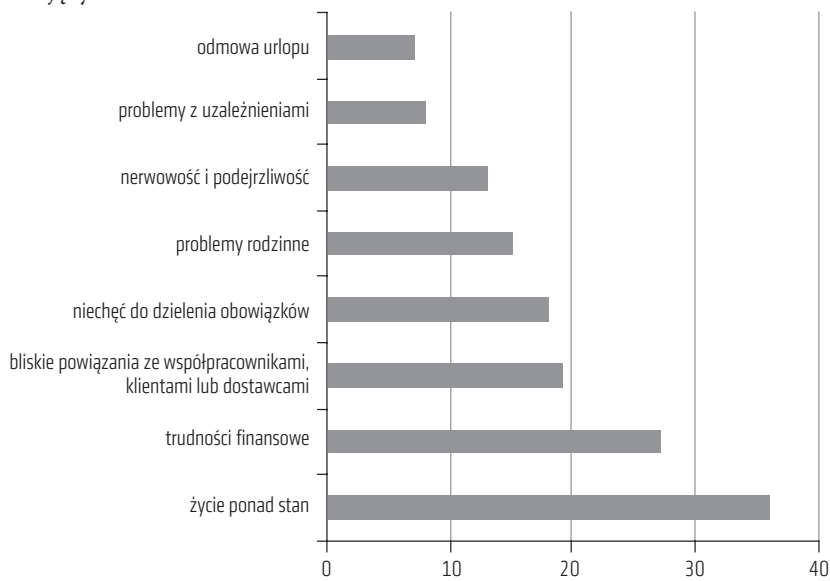
Ostatnim elementem przeprowadzonej analizy była identyfikacja charakterystycznych postaw oraz zachowań mogących sugerować zwiększoną skłonność do popełnienia oszustwa. Uczestnicy seminariów, bazując na swoim doświadczeniu, rozpoznali trzy symptomy, które mogą decydować o większym prawdopodobieństwie popełnienia nadużycia, tj.:

- trudna sytuacja finansowa,
- chęć pracy poza regularnym przedziałem funkcjonowania całej organizacji,
- nadzwyczaj bliskie relacje z klientem lub dostawcą.

[51] P. Marais i in., Global Profiles of the Fraudster…, op. cit.

Uczestnicy zasugerowali również, że warto pogłębić dyskusję nad rozważanym zagadnieniem poprzez analizę badań dotyczących najczęściej obserwowanych zachowań wśród oszustów na całym świecie.

Rysunek 28. Najczęściej obserwowane zachowania i postawy wśród osób popełniających oszustwa



Źródło: opracowanie własne na podstawie danych ACFE[52]

Według badań przeprowadzonych przez ACFE szczególną uwagę należy zwrócić na pracowników żyjących ponad stan. Średnio co trzecie z analizowanych oszustw zostało popełnione przez osoby przejawiające tego typu zachowania. Pełne zestawienie najczęściej obserwowanych zachowań zostało zilustrowane powyżej (zob. rysunek 28).

Celem analizy była identyfikacja cech najczęściej spotykanych pośród osób popełniających szeroko rozumiane oszustwa i nadużycia. Zgodnie z zaleceniami uczestników seminariów powyższe wnioski mają stanowić punkt wyjścia dla dalszych prac dedykowanych zastosowaniu statystycznego

[52] *Report to the Nations: On Occupational Fraud and Abuse 2012*, Association of Certified Fraud Examiners, Austin, Texas, 2012, Global Fraud Study, https://www.acfe.com/uploaded-files/acfe_website/content/rttn/2012-report-to-nations.pdf

profilu oszusta w zautomatyzowanej detekcji osób obarczonych wysokimi skłonnościami do nadużyć dla potrzeb zapobiegania oszustwom i nadużyciom w Polsce.

3.1.2. Profil cyberprzestępcy

W wyniku dyskusji przeprowadzonej podczas seminariów uczestnicy oraz zaproszeni specjaliści zgodzili się, że szeroko rozumiane cyberprzestępstwa stanowią obecnie jedno z największych zagrożeń dla funkcjonowania globalnej gospodarki. Potwierdzają to liczne analizy przeprowadzone przez uznane instytucje na całym świecie[53, 54, 55]. Na ich podstawie można zaobserwować wzrost liczby niemal wszystkich typów cyberataków. Warto też podkreślić, że zdaniem ekspertów wzrost ten jest zbyt znaczący oraz powszechny, aby można było go tłumaczyć zwiększaniem nakładów na wykrywanie ataków (paradoks kontrolny). Jednym z wniosków sformułowanych przez uczestników było wykorzystanie profilowania kryminalnego na rzecz stworzenia sylwetki cyberprzestępcy. Taki profil ma być podstawą dla dalszych badań w zakresie oprogramowania pozwalającego na zautomatyzowaną estymację czynników ryzyka oraz detekcję potencjalnych aktów cyberprzestępców. Koncepcja oraz wnioski jakościowe zostały sformułowane w wyniku dyskusji przeprowadzonych podczas seminariów, zaś dane liczbowe pochodzą z prac badawczych SRI International oraz innych dostępnych analiz.

Pierwszym elementem niniejszej analizy jest klasyfikacja cech demograficznych, które sprzyjają popełnieniu cyberprzestępstwa przez jednostkę, tj. takich, które występują u większości cyberprzestępców. Zgodnie z danymi SRI International typowy cyberprzestępca ma od 31 do 40 lat

---

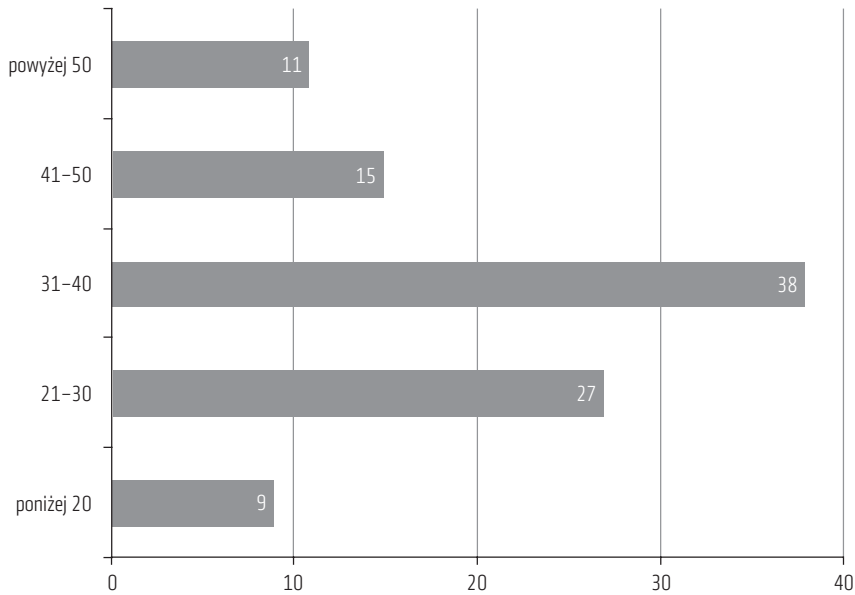
[53] G. Cleary i in., *Internet Security Threat Report*, Symantec, http://images.mktgassets.symantec.com/ Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_ (dostęp: 03.2018).

[54] *Facing Forward: Cyber Security in 2019 and Beyond*, FireEye 2018, SECURITY PREDICTIONS 2019, https://content.fireeye.com/predictions/rpt-security-predictions-2019

[55] *Small and Mighty. How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats*, CISCO, CISCO Cybersecurity Special Report, San Jose, https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf (dostęp: 07.2018).

(zob. rysunek 29), najczęściej (w 76 proc. przypadków) jest to mężczyzna, często białoskóry (70 proc.), zaś połączenie wszystkich powyższych cech, tj. białoskóry mężczyzna w wieku od 31 do 40 lat, występuje w 31 proc. przypadków cyberataków poddanych analizie. Warto zauważyć, że, jak podkreślają zaproszeni eksperci, podobieństwo do stereotypowego obrazu subkultury hackerskiej jest jedynie pozorne.

Rysunek 29. Typowy wiek cyberprzestępcy



Źródło: opracowanie własne na podstawie danych SRI International

Początkowo cyberprzestępstwa były problemem regionalnym, charakterystycznym dla społeczeństwa zachodniego. Obecnie przestępstwa te popełniane są na całym świecie. Kolejnym przekłamaniem występującym w typowym obrazie cyberprzestępcy jest postrzeganie go, jako stroniącego od ludzi, często borykającego się z problemami w komunikacji interpersonalnej. Zgodnie z opinią prof. Stuarta Madnicka obecnie za większość cyberataków odpowiadają nie pojedyncze osoby, a dobrze zorganizowane grupy przestępcze, których głównym motywem działania są korzyści finansowe. Potwierdzają to dane SRI International, wskazujące że połowa grup cyberprzestępczych składa się z co najmniej sześciu członków, zaś co czwarta z nich

jest aktywna od mniej niż pół roku. Powyższe zjawisko jest bezpośrednio związane z upowszechnieniem narzędzi niezbędnych do przeprowadzenia cyberataków. Zgodnie z opinią Stuarta Madnicka potwierdzoną przez niezależne badania[56], współczesne grupy cyberprzestępcze to sprawnie działające organizacje, posiadające szeroki wachlarz usług, narzędzi oraz produktów pozwalających na samodzielne przeprowadzenie ataku bez konieczności posiadania wiedzy specjalistycznej. Uczestnicy zwrócili uwagę, że wyłonienie się organizacji pośród grup cyberprzestępczych może pozwolić na stworzenie mechanizmu identyfikacji ich członków poprzez analizę powiązań formalnych i nieformalnych pomiędzy osobami o zwiększonych czynnikach ryzyka, tj. posiadającymi cechy cyberprzestępcy/oszusta. W związku z powyższym uczestnicy zalecili powołanie grupy badawczej dedykowanej stworzeniu mechanizmu identyfikacji powiązań formalnych i nieformalnych na potrzeby wykrywania działalności przestępczej. Jeff Klaben z SRI International podkreślił również, że identyfikacja powiązań może mieć szczególne znaczenie w obliczu wzrastającej liczby cyberataków wewnętrznych, tj. podejmowanych przez pracowników instytucji, które, z jednej strony, są rezultatem powszechnej dostępności narzędzi umożliwiających nadużycia, a z drugiej wiążą się z koniecznością istnienia informatora wewnętrznego, niezbędnego do przeprowadzenia bardziej wyrafinowanego cyberataku.

Podczas dyskusji podsumowującej uczestnicy zauważyli, że sylwetki współczesnych oszustów i cyberprzestępców mają wiele cech wspólnych. Wynika to z coraz powszechniejszej dostępności narzędzi pozwalających na stosunkowo proste przeprowadzenie cyberataku. Ponadto uczestnicy seminariów wskazali na konieczność przeprowadzenia badań w zakresie mechanizmów identyfikacji powiązań formalnych i nieformalnych w organizacjach w kontekście przeciwdziałania zarówno przestępczości konwencjonalnej, jak i szeroko rozumianym cyberatakom. Takie mechanizmy mogłyby stać się szczególnie przydatnym narzędziem w procesie rekrutacji i ewaluacji pracowników.

[56] D. Manky, *Cybercrime as a Service: A Very Modern Business*, Computer Fraud & Security, 2013, t. 2013, nr 6, s. 9–13.

3.2. Elementy strategii cyberbezpieczeństwa organizacji

Przetwarzanie informacji w organizacjach oraz komunikacja między podmiotami życia społecznego i gospodarczego zostały zdominowane przez narzędzia informatyczne połączone za pośrednictwem sieci Internet. Z tego względu szczególnym przedmiotem uwagi i jednym z dominujących komponentów całościowej metodologii zapewnienia bezpieczeństwa organizacji powinno być jej bezpieczeństwo cybernetyczne.

Bezpieczeństwo cybernetyczne rozumiane jest jako proces zapewnienia bezpieczeństwa danych w drodze zapobiegania, wykrywania oraz, jeśli okaże się to konieczne, reagowania na atak[57]. Strategie organizacji dotyczące bezpieczeństwa cybernetycznego są *de facto* kosztowymi modelami zarządzania ryzykiem cybernetycznym opartymi na przyczynowo-skutkowej analizie działań, które zostały podjęte na rzecz zapewnienia bezpieczeństwa, oraz tych, których zaniechano ze względu na wysokie koszty, dopuszczając możliwość wystąpienia pewnych rodzajów ataków. Strategie te nie są zestawem działań, które gwarantują organizacji pełne bezwarunkowe zabezpieczenie przed każdym możliwym rodzajem ataku. Taka interpretacja znajduje potwierdzenie chociażby na gruncie normy PN-ISO/IEC 15408-1:2002, powszechnie znanej pod nazwą *Common Criteria*, będącej zestawem procedur służących definiowaniu zagrożeń oraz odpowiadających im zabezpieczeń systemów teleinformatycznych[58]. To podejście do roli strategii bezpieczeństwa ujawniło się także podczas kryzysu wywołanego szeregiem ataków w maju 2017 roku, gdzie wykorzystano oprogramowanie typu *ransomware,* znane jako *WannaCry*. Zgodnie z informacjami dostarczonymi przez prof. Madnicka większość organizacji zdecydowałaby się na zapłatę „okupu" w zamian za odblokowanie komputerów, a nie na inwestycję w zapobieżenie skutkom ataku. Główną motywacją dla podjęcia takiej decyzji byłyby względy finansowe, bo koszt wdrożenia odpowiednich rozwiązań byłby wielokrotnie wyższy od średniej

[57] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, National Institute of Standards and Technology, Gaithersburg, MD, http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf (dostęp: 02.2014).

[58] *PN-ISO/IEC 15408-1: 2002: Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny.*

wysokości okupów żądanych przez napastników (według danych przytoczonych przez prof. Madnicka w 2017 roku średni koszt dla organizacji związany z atakiem tego rodzaju wyniósł 133 tys. USD).

Płynie stąd wniosek, że budowanie strategii bezpieczeństwa należy poprzedzić świadomym wyborem zagrożeń, na które strategia ta będzie odpowiadać. Można tego dokonać jedynie w drodze identyfikacji bieżących wektorów ataku, w oparciu o pełne zrozumienie środowiska technologicznego, w którym funkcjonuje organizacja oraz świadomość aktualnych i przyszłych zagrożeń.

3.2.1. Cyberprzestępczość jako usługa

Proceder ten, którego angielski źródłosłów, *Cybercrime-as-a-Service,* nawiązuje do terminu *Everything-as-a-Service*[59] zapożyczonego z terminologii stosowanej do określenia szeregu nowoczesnych technologii informatycznych[60], polega na odpłatnym oferowaniu ataków cybernetycznych za pośrednictwem sieci Dark Web. Uczestnicy seminariów uznali, że istota tego zjawiska wynika z faktu, że wiedza z zakresu bezpieczeństwa cybernetycznego nie jest wymogiem koniecznym do przeprowadzenia ataku.

[59] G. Collins i in., *Everything-as-a-service: Modernizing the Core Through a Services Lens, w: Tech Trends 2017: The Kinetic Enterprise*, Deloitte University Press, s. 78–91, https://www2.deloitte.com/insights/us/en/focus/tech-trends/2017/everything-as-a-service.html

[60] D. Barker, *An Unofficial Guide to Whatever-as-a-Service – Gadgetopia*, https://gadgetopia.com/post/9981 (dostęp: 26.01.2019).

W poniższej tabeli znajduje się zestawienie typów usług, które zostały uznane za szczególnie istotne przez uczestników seminarium.

Nazwa usługi	Rozwinięcie nazwy usługi	Wyjaśnienie
VDass	Vulnerability Discovery as a Service	Usługa polegająca na identyfikacji luk w zabezpieczeniach infrastruktury cyfrowej klienta oraz estymacji stopnia narażenia na atak przez strony trzecie. Usługa, świadczona również przez firmy z branży IT, obejmuje pełny audyt zabezpieczeń organizacji oraz stworzenie odpowiednich rekomendacji zaradczych[61].
EaaS	Exploit as a Service	Jedna z usług oferująca częściowy bądź całkowity dostęp do systemu wskazanej ofiary poprzez wykorzystanie luk w jej systemie teleinformatycznym. Często stosowana jako pierwsza faza ataku ransomware[62].
DaaS	Deception as a Service	Usługę można rozumieć jako wariant podejścia ***Security through obscurity***. Pozwala zwiększyć poziom bezpieczeństwa poprzez wykorzystanie tzw. technik podstępu, które mają zmylić atakującego w oparciu o fałszywe dane bądź zasoby. Przykładami implementacji rozważanej usługi może być np. stworzenie wirtualnej sieci zasobów na potrzeby ochrony prawdziwych danych[63]. Jest to usługa skierowana do innych cyberprzestępców pozwalająca na ukrycie ich prawdziwej tożsamości.
PaaS	Payload as a Service	Usługa zapewnia modyfikację plików stanowiących przedmiot komunikacji między aktorami atakowanego systemu pod kątem umieszczenia w nich szkodliwego kodu. Zwykle taki atak ma na celu usunięcie danych bądź uzyskanie dostępu do systemu. Najczęściej atak przeprowadza się w ramach łańcucha wartości (atakującym bądź zleceniodawca jest podmiot posiadający wiedzę o strukturze systemu teleinformatycznego ofiary)[64].
BNaaS	Botnet as a Service	Jest to metoda przeprowadzenia innego typu ataku za pośrednictwem zdalnie kontrolowanej sieci komputerów, tzw. sieci botnet, na wybrany przez klienta zasób bądź element infrastruktury teleinformatycznej. Najczęściej atak ten przybiera formę ataku DDoS[65].

Uczestnicy seminariów zgodnie stwierdzili, że współczesna społeczność cyberprzestępców w warstwie operacyjnej przypomina sprawnie działającą organizację, co może stanowić istotny czynnik zagrażający wszystkim sektorom gospodarki. Podczas dyskusji uznano, że powszechność usług przytoczonych powyżej może zostać wykorzystana na rzecz zwiększenia poziomu

[61] *RiskSense Vulnerability Discovery*, RiskSense 2018.

[62] *Exploits as a Service*, Trend Micro 2016, Cybercrime-as-a-Service Series, https://documents.trendmicro.com/assets/guides/executive-brief-exploits-as-a-service.pdf

[63] D. Fraunholz, D. Reti, H.D. Schotten, *Deception as a Service: A Reverse Web Proxy Framework*, Intelligent Networks Research Group, German Research Center for Artificial Intelligence 2017, https://www.researchgate.net/profile/Daniel_Fraunholz/publication/324569615_Deception_as_a_Service_A_Reverse_Web_Proxy_Framework/links/5bfbe460458515b41d0f5995/Deception-as-a-Service-A-Reverse-Web-Proxy-Framework.pdf?origin=publication_detail

[64] *What Does Payload Mean?*, https://www.techopedia.com/definition/5381/payload

[65] R. Jovel, E. Ananin, *DDoS-for-Hire Service Powered by Bushido Botnet*, Fortinet, https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered-by-bushido-botnet-.html (dostęp: 26.10.2018).

bezpieczeństwa. W szczególności ww. usługi można zastosować bezpośrednio (jako środki ochrony, np. technikę *Deception-as-a-Service*) lub w celu wykrycia luk bezpieczeństwa (np. poprzez przeprowadzenie kontrolowanych testów podatności infrastruktury organizacji na cyberataki danego typu). Kolejny wniosek sformułowany przez uczestników seminarium dla obszaru zarządzania ludźmi w organizacjach dotyczył wykorzystania opisanych wyżej usług jako zestawu metod pozwalających lepiej zrozumieć sposób działania grup cyberprzestępczych, co może przyczynić się do opracowania skuteczniejszych rozwiązań na rzecz przeciwdziałania cyberatakom.

3.2.2. Metody typu *Bug Bounty* odnajdywania luk w systemach bezpieczeństwa organizacji z perspektywy decydentów

Celem metody typu *Bug Bounty* jest wykrywanie luk bezpieczeństwa systemów informatycznych organizacji przy aktywnym zaangażowaniu społeczności *ethical hackers*. Polega ona na tworzeniu publicznie dostępnych programów motywacyjnych (ang. *incentive programs*), które są zachętą dla tzw. *security researchers* (nazywanych również łowcami nagród, ang. *bounty hunters*) do odnajdywania luk zabezpieczeń systemów informatycznych danej organizacji. Raporty dotyczące tych luk są składane do działu organizacji odpowiedzialnego za bezpieczeństwo teleinformatyczne. Na podstawie dostarczonych informacji organizacja weryfikuje podatność swoich systemów na wyszczególnione w raporcie ataki, klasyfikuje zagrożenia według przyjętej skali oraz dokonuje stosownych poprawek w systemie bezpieczeństwa. Researcher otrzymuje wynagrodzenie w zależności od kategorii istotności wykrytych zagrożeń, zgodnie z regulaminem programu. Poniżej zaprezentowano zestawienie średnich nagród ze względu na poziom doświadczenia organizacji w przeprowadzaniu programów *Bug Bounty* oraz istotność wykrytego zagrożenia (zob. tabela 11).

Aktualną wyczerpującą listę tego typu programów opublikowanych przez organizacje z całego świata można znaleźć na stronie firmy HackerOne, Inc., zrzeszającej międzynarodową społeczność researcherów[66].

[66] https://hackerone.com/bug-bounty-programs

Tabela 11. Zestawienie zaleceń dla wysokości nagród (w USD) w zależności od doświadczenia organizacji w prowadzeniu programów typu *Bug Bounty* oraz istotności zidentyfikowanej luki bezpieczeństwa

	Krytyczny poziom istotności	Wysoki poziom istotności	Średni poziom istotności	Niski poziom istotności
Poziom I	2 000	750	300	150
Poziom II	3 000	1 000	500	250
Poziom III	5 000	2 000	750	250–500
Poziom IV	7 500	3 000	1 000	250–750
Poziom V	10 000	5 000	2 500	250–1000

Źródło: opracowanie własne na podstawie https://www.hackerone.com/resources/bug-bounty-basics (dostęp: 27.01.2019)

Jako argument w dyskusji o zasadności oraz efektywności kosztowej przeprowadzania programów typu *Bug Bounty*, prof. Madnick przytoczył przykład programu „Hack the Pentagon" utworzonego w 2017 roku przez Departament Obrony Stanów Zjednoczonych (U.S. Department of Defense, DoD). W ramach tego programu grupa 1400 zakwalifikowanych researcherów zidentyfikowała 138 nagrodzonych zagrożeń. Pula nagród wyniosła 150 tys. USD. Podczas niezależnego trzyletniego programu identyfikacji zagrożeń realizowanego przez zewnętrznego audytora za kwotę 5 mln USD, zidentyfikowano jedynie 10 słabości systemu bezpieczeństwa. W listopadzie 2018 roku Departament Obrony uruchomił kolejną edycję programu „Hack the Pentagon"[67]. Uczestnicy uznali wysoką skuteczność tego typu metod i zgodzili się, że powinny zostać włączone do zestawu metod strategii bezpieczeństwa organizacji w Polsce.

W sektorze prywatnym programy typu *Bug Bounty* są powszechnie uznaną praktyką pozwalającą na wykrywanie luk zabezpieczeń[68]. Uczestnicy seminariów zgodzili się, że organizacja tego typu programów będzie sprzyjała budowaniu wizerunku organizacji jako podmiotu:

[67] *Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital*, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/ (dostęp: 27.01.2019).

[68] *Hacking the Pentagon*, https://www.usds.gov/report-to-congress/2017/fall/hack-the-pentagon/ (dostęp: 27.01.2019).

a. aktywnie zaangażowanego w proces budowania bezpieczeństwa organizacyjnego, bezpieczeństwa swoich partnerów oraz klientów,
b. społecznie odpowiedzialnego, doceniającego rolę współpracy ze społecznością researcherów na rzecz budowania bezpiecznej przestrzeni informacyjnej.

Według prof. Madnicka dedykowane platformy, takie jak HackerOne, w istotny sposób wspomagają organizacje w przeprowadzeniu programów *Bug Bounty* oferując kontrolowane, bezpieczne środowisko i zapraszając do partycypacji jedynie wyselekcjonowaną, zamkniętą grupę specjalistów (w tym kontekście, do określenia tej grupy używa się terminu *blue hats*).

Podziękowania

Ani podsumowane w niniejszym raporcie badania, ani sam projekt „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" nie osiągnęłyby zakładanych celów bez zaangażowania grona zaproszonych ekspertów, 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.

PROWADZONE PANELE	• An introduction to operations management (OM): Benihana case • Controlling processes: Kristen's Cookie case • Lecture & workshop: using OM to combat crime in finance • Lecture & workshop: using OM to combat crime in managing people
OBECNIE PEŁNIONE FUNKCJE	• Konsultant • Inwestor prywatny
NAJWAŻNIEJSZE PUBLIKACJE[69]	1. Done A., Voss C., Rytter N. G., *Best Practice Interventions: Short-term Impact and Long-term Outcomes, Journal of Operations Management*, t. 29, nr 5, s. 500–513, 07.2011. 2. Done A., *Global Trends*. London: Palgrave Macmillan UK, 2012. 3. Done A., *Supply-chain Evolution: Knowledge-based Perspectives*, IESE Business School, 2011. 4. Done A., *Supply Chain Knowledge Management: A Conceptual Framework, IESE Business School*, nr D/900, 2011. 5. Done A., *Developing Supply Chain Maturity, IESE Business School*, 2011.

[69] Pięć najczęściej cytowanych prac spośród dorobku naukowego. Selekcja odbyła się na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 24.10.2018).

Stuart Madnick, Ph.D.

PROWADZONE PANELE	• What every manager should know about cybersecurity: popular myths and misunderstandings exposed • Cybercrime ecosystem: the Dark Web and Cybercrime-as-a-service • Conflict between data privacy and security
OBECNIE PEŁNIONE FUNKCJE	• Dyrektor Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)3 przy MIT Sloan School of Management • Profesor technologii informacyjnej w MIT Sloan School of Management (John Norris Maguire Professor of Information Technologies) oraz MIT School of Engineering • Wicedyrektor programu Total Data Quality Management (TDQM) • Wicedyrektor programu Productivity From Information Technology (PROFIT)
NAJWAŻNIEJSZE PUBLIKACJE[70]	1. Abdel-Hamid T. K., Madnick S. E., *Lessons Learned from Modeling the Dynamics of Software Development, Commun. ACM*, 1989, t. 32, nr 12, s. 1426–1438. 2. Goh C. H., Bressan S., Madnick S., Siegel M., *Context Interchange: New Features and Formalisms for the Intelligent Integration of Information, ACM Trans. Inf. Syst.*, 1999, t. 17, nr 3, s. 270–293,. 3. Siegel M., Madnick S. E., *A Metadata Approach to Resolving Semantic Conflicts*, w: *Proceedings of the 17th International Conference on Very Large Data Bases*, San Francisco, CA, USA, 1991, s. 133–145. 4. Wang R. Y., Kon H. B., Madnick S. E., *Data Quality Requirements Analysis and Modeling*, w: *Proceedings of IEEE 9th International Conference on Data Engineering*, 1993, s. 670–677. 5. Wang J. R., Madnick S. E., *The Inter-database Instance Identification Problem in Integrating Autonomous Systems, w: Proceedings. Fifth International Conference on Data Engineering*, 1989, s. 46–55.

Dr Marcin Mrowiec

PROWADZONE PANELE	• Ludzie i kapitał. Perspektywy gospodarki Polski w kontekście wyzwań demograficznych • Czym jest pieniądz? Zarys historii systemów monetarnych w kontekście bieżących wyzwań i propozycji reform
OBECNIE PEŁNIONE FUNKCJE	• Główny Ekonomista Banku PKO SA
NAJWAŻNIEJSZE PUBLIKACJE[71]	1. Mrowiec M., *Austriacka szkoła ekonomii: jak może pomóc wyjaśnić stagnację gospodarki Japonii*, Wydawnictwo Naukowe PWN, Warszawa 2017. 2. Mrowiec M., *Ekonomia jako nauka o celowym działaniu. Paradygmat szkoły austriackiej oraz krytyka keynesizmu i monetaryzmu, Ekonomia – Uniwersytet Ekonomiczny we Wrocławiu*, nr 3 (24), s. 11–25, 2013. 3. Mrowiec M., *Koncepcja pieniądza i kredytu Ludwiga von Misesa – pieniądz fiducjarny jako forma interwencji w mechanizm wolnego rynku, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, 2013, t. 914, nr 14, s. 5–19.

[70] Pięć najczęściej cytowanych prac spośród dorobku naukowego. Selekcja odbyła się na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 24.10.2018).

[71] Ibid.

Jeff Klaben, Ph.D.

PROWADZONE PANELE	• Cybersecurity and technology risk management • Trustworthy technologies and innovation: the human factor • Trustworthy technologies and innovation in the insurance sector
OBECNIE PEŁNIONE FUNKCJE	• Chief Information Security Officer w SRI International
NAJWAŻNIEJSZE PUBLIKACJE[72]	McCarthy N. K., Klaben J., Todd M., *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Informaton at Risk*, McGraw-Hill, Nowy Jork 2012.
PATENTY	1. Porras P. A., Klaben J., Lincoln P. D., Fong M. W., Chapin N., *Impact Analyzer for a Computer Network*, US20160218933A1, 28.07.2016. 2. Porras P. A., Klaben J., Lincoln P. D., Chapin N., *Multimodal Help Agent for Network Administrator*, US20160219078A1, 28.07.2016. 3. Porras P. A., Klaben J., Lincoln P. D., Chapin N., *Natural Language Dialog-based Security Help Agent for Network Administrator*, US20160219048A1, 28.07.2016

[72] Pięć najczęściej cytowanych prac spośród dorobku naukowego. Selekcja odbyła się na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 24.10.2018).

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

Improving performance

1. Czy sposoby przeciwdziałania przestępczości stosowane za granicą mogą być Pani/Pana zdaniem wykorzystane w Polsce?	1	2	3	4	5
2. Czy uważa Pan/Pani, że zaprezentowana metodyka zarządzania operacjami mogłaby zostać wdrożona w organizacji, którą Pan/Pani reprezentuje?	1	2	3	4	5
3. Czy wykorzystanie wybranych rozwiązań dotyczących zarządzania operacjami pozwoliłoby na redukcję kosztów ponoszonych przez Pana/Pani organizację?	1	2	3	4	5

4. Czy wdrożenie zaprezentowanej metodyki mogłoby przyczynić się do uzyskania większej efektywności w wykrywaniu i zapobieganiu przestępczości?	1	2	3	4	5
5. Czy większa przejrzystość w zarządzaniu operacjami pozwoliłaby w Państwa firmie na skuteczniejsze przeciwdziałanie nieprawidłowościom i ewentualnym przestępstwom?	1	2	3	4	5
6. Czy widzi Pan/Pani potrzebę podejmowania prac nad systemem bezpieczeństwa cybernetycznego w Polsce?	1	2	3	4	5
7. Czy uważa Pan/Pani, że rozwiązania z zakresu bezpieczeństwa stosowane na świecie mogą być wykorzystane w prosty sposób w Polsce?	1	2	3	4	5
8. Najskuteczniejsze metody zwalczania przestępczości to:					
a) transparentność w zarządzaniu operacjami	1	2	3	4	5
b) identyfikacja wąskich gardeł	1	2	3	4	5
c) ograniczenie nieprzewidywalności	1	2	3	4	5
d) wykorzystywanie narzędzi bazujących na sztucznej inteligencji	1	2	3	4	5
e) wysoka transparentność w zarządzaniu organizacjami	1	2	3	4	5
f) stochastyczna teoria kontroli jakości produktu	1	2	3	4	5
g) nieuchronność kary	1	2	3	4	5
h) surowość kary	1	2	3	4	5
i) inne:	1	2	3	4	5
9. Sektory charakteryzujące się najskuteczniejszą metodyką zwalczania przestępczości w Polsce:					
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) rolnictwo	1	2	3	4	5
e) transport	1	2	3	4	5
f) inny:	1	2	3	4	5

Spis rysunków

Spis tabel

Bibliografia

Barker D., *An Unofficial Guide to Whatever-as-a-Service – Gadgetopia*, https://gadgetopia.com/post/9981 (dostęp: 26.01.2019).

Bohn R.E., *Kristen's Cookie*, Harvard Business School Case Collection, 1986, nr 686093-PDF-ENG.

Cleary G., Corpin M., Cox O., Hon L., Nahorney B., O'Brien D., O'Gorman B., i in., *Internet Security Threat Report*, Symantec, http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_ (dostęp 03.2018).

Collins G., Krumkachev P., Aspin G., Metzger M., Radeztsky S., Srinivasan S., *Everything-as-a-service: Modernizing the Core Through a Services Lens*, w: *Tech Trends 2017: The Kinetic Enterprise*, Deloitte University Press, s. 78–91, https://www2.deloitte.com/insights/us/en/focus/tech-trends/2017/everything-as-a-service.html

Demos T., *Banks Build Line of Defense for Doomsday Cyberattack*, *Wall Street Journal*, sekc. Markets, https://www.wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401 (dostęp: 3.12.2017).

Fraunholz D., Reti D., Schotten H.D., *Deception as a Service: A Reverse Web Proxy Framework*, Intelligent Networks Research Group, German Research Center for Artificial Intelligence 2017, https://www.researchgate.net/profile/Daniel_Fraunholz/publication/324569615_Deception_as_a_Service_A_Reverse_Web_Proxy_Framework/links/5bfbe460458515b41d0f5995/Deception-as-a-Service-A-Reverse-Web-Proxy-Framework.pdf?origin=publication_detail

Gawrońska-Malec A., Czyżewski Z., Helm J., Peer M., *Profil korporacyjnego oszusta Edycja 2016*, KPMG w Polsce 2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/pl-Raport-KPMG-Profil-korporacyjnego-oszusta.pdf

Hacker E., Nilsson A., *Fraud, Corruption and the Paradox of Control,* w: The Southern Business & Economic Journal, 2008, t. 31, nr 3/4, s. 49–71.

Hołyst B., *Kryminologia*, Wolters Kluwer, Warszawa 2016.

Jovel R., Ananin E., *DDoS-for-Hire Service Powered by Bushido Botnet*, Fortinet, https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered--by-bushido-botnet-.html (dostęp: 26.10.2018).

Kocsis R.N., *Criminal Profiling: Principles and Practice*, Humana Press, Totowa N.J 2006.

Lavion D., *Pulling Fraud out of the Shadows*, PwC 2018, Global Economic Crime and Fraud Survey 2018.

Lombroso C., Gibson M., Rafter N.H., *Criminal Man*, Duke University Press, Durham, NC, 2006.

Malocco D.E.V., *Criminal Profiling: A Basic Introduction*, 2014.

Manadhata P.K., *An Attack Surface Metric*, Carnegie Mellon University 2008, http://reports--archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf#page=45&zoom=100,0,382

Manky D., *Cybercrime as a Service: A Very Modern Business*, Computer Fraud & Security, 2013, t.2013, nr 6, s. 9–13.

Marais P., Girgenti R.H., DeRaad J., Jamieson G., Ostwalt P., Friedman D., Drolet S., i in.., *Global Profiles of the Fraudster: Technology Enables and Weak Controls Fuel the Fraud*, KPMG International, 05.2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf (dostęp 05.2016)

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, National Institute of Standards and Technology, Gaithersburg, MD, http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf (dostęp: 12.02.2014).

Nestler C., Skalak S., Wilkinson J., Parton T., Doker J., Stanley R., Madasi L., i in.., *Economic Crime: People, Culture and Controls. The 4th Biennial Global Economic Crime Survey*, Martin Luther University, PwC 2007, Investigations and Forensic Services, https://www.pwc.com/gx/en/economic-crime-survey/pdf/gecs_engineering_and_construction_supplement.pdf

Oswalt P.D., Powell R., Leishman M., Girgenti R.H., Colebourne I., Jamieson G., *Who is the Typical Fraudster? KPMG Analysis of Global Patterns of Fraud*, KPMG, USA 2011, https://www.ub.unibas.ch/digi/a125/sachdok/2011/BAU_1_5663361.pdf

Porter M.E., *Competitive Advantage: Creating and Sustaining Superior Performance*, Free Press, Riverside 2008.

Sasser W.E., *Benihana of Tokyo*, Harvard Business School Case Collection, 1972, nr 673–057.

Turvey B.E., *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, wyd. 4, Academic Press, Amsterdam Burlington, MA, 2012.

Report to the Nations: On Occupational Fraud and Abuse 2012, Association of Certified Fraud Examiners, Austin, Texas, 2012, Global Fraud Study, https://www.acfe.com/uploadedfiles/acfe_website/content/rttn/2012-report-to-nations.pdf

Report to the Nations: On Occupational Fraud and Abuse 2012, Association of CertifiedFraud Examiners, Austin, Texas, 2012, Global Fraud Study, https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

Report to the Nations: On Occupational Fraud and Abuse 2014, Association of Certified Fraud Examiners, Austin, Texas, 2014, Global Fraud Study, https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

Exploits as a Service, Trend Micro 2016, Cybercrime-as-a-Service Series, https://documents.trendmicro.com/assets/guides/executive-brief-exploits-as-a-service.pdf

Cost of Cyber Crime Study Insights on the Security Investments That Make a Difference, Ponemon Institute LLC, Accenture 2017, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, Austin, Texas, USA, 2018.

Facing Forward: Cyber Security in 2019 and Beyond, FireEye 2018, Security Predictions 2019, https://content.fireeye.com/predictions/rpt-security-predictions-2019

RiskSense Vulnerability Discovery, RiskSense 2018.

Small and Mighty. How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats, CISCO, San Jose, USA, 07.2018, CISCO Cybersecurity Special Report, https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

PN-ISO/IEC 15408-1:2002: Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny.

What Does Payload Mean?, https://www.techopedia.com/definition/5381/payload

Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/ (dostęp: 27.01.2019).

Hacking the Pentagon, https://www.usds.gov/report-to-congress/2017/fall/hack-the-pentagon/ (dostęp: 27.01.2019).

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
Łukasz WOJCIESZAK, Politechnika Świętokrzyska
Jolanta STANIENDA, Uniwersytet Ekonomiczny w Krakowie
Marek BIELECKI, Akademia Sztuki Wojennej

ROZDZIAŁ I

Improving Performance. Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w kontekście metodyki

BARTŁOMIEJ ORĘZIAK[1], MARCIN WIELEC[2]

1. Improving Performance: Wprowadzenie

Moduł Improving Performance został skoncentrowany na rozwiązaniach zidentyfikowanych problemów w module Assessing Foundations w świetle wybranych sektorów polskiej gospodarki. Zatem prowadząc dalsze prace naukowe związane z realizacją międzynarodowego projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości"[3], stwierdzono zasadność pogłębienia problematyki rynku finansowego, energetycznego, ubezpieczeniowego oraz zarządzania ludźmi w organizacji. Celem było wypracowanie analizy na specyficznej płaszczyźnie Improving Performance. Projektowanym efektem było zaprezentowanie ogólnego przeglądu wybranego obszaru z punktu widzenia metod zapobiegania przestępczości (komparatystryczne ujęcie polskich problemów) na tle starannie

[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/

wyselekcjonowanych zagadnień pomocniczych. Całościowo oraz finalnie prowadzone badania w zamiarze badaczy miały zakończyć się dokonaniem podejścia analitycznego dotyczącego rynku finansowego, ubezpieczeniowego, energetycznego oraz zarządzania ludźmi w organizacji w świetle technologii utrudniających dokonywanie przestępstw w tych wymiarach nie tylko w sferze Improving Performance[4], ale także w świetle modułów Assessing Foundations[5], Transforming People and Organizations[6] oraz Heading Into the Future[7]. Zgodnie z powyższym, zajęto się wskazanymi zagadnieniami oraz oceną poziomu zaawansowania i zakresu wykorzystania technologii zapobiegających dokonywanie przestępstw. Dodatkowo uzyskano oraz zaktualizowano wiedzę na temat zagranicznych rozwiązań i zagrożeń dla fundamentalnych zasad polskiego porządku prawnego. Ogół dokonywanych analiz uwzględniał fakt, że badanie przyczyn powstawania sytuacji, w których dochodzi do przestępstw w obszarze rynku finansowego, ubezpieczeniowego, energetycznego oraz zarządzania ludźmi w organizacji, zostało zakwalifikowane jako główny segment badawczy oraz analityczny cel Projektu[8].

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

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

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

[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.), *Rynek 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. Improving Performance: Przedmiot prac

Moduł Improving Performance został poświęcony problematyce zarządzania operacjami, gdzie zakres tematyczny obejmował ten proces w poszczególnych obszarach badawczych, kreatywność i innowacyjność w zarządzaniu, nowe technologie integrujące informacje w tym procesie oraz rozwiązania problemów przestępczości w przedstawionych działach. Relewantne dla przedmiotu prowadzonych badań okazały się zagadnienia dotyczące zarządzania cyberbezpieczeństwem oraz wykorzystywaniem najnowszych technologii w przeciwdziałaniu przestępczości. Analizy typu Improving Performance polegały w szczególności na skoncentrowaniu się w stronę konkretnych obszarów polskiej gospodarki. Umożliwiło to przedstawienie założenia związanego z pracami nad najnowszymi rozwiązaniami prawnymi, gospodarczymi, technologicznymi oraz organizacyjnymi z zakresu przeciwdziałania przestępczości. Dodatkowo – pomimo tożsamości analizowanych zagadnień – inne było w stosunku do nich podejście analityczne skoncentrowane na problematyce sektorowej.

Na rynku finansowym w wymiarze Improving Performance podczas całych prac badawczych pochylono się nad zagadnieniem metod zapobiegania przyczynom przestępczości zarówno w kontekście rozwiązań organizacyjnych ułatwiających zachowanie kontroli instytucji finansowej nad operacjami realizowanymi przez jej pracowników, procesu podejmowania decyzji, zarządzania operacjami w instytucjach finansowych, 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 powyżej segmentów badawczych umożliwiło dokonanie analizy typu Improving Performance.

Na rynku energetycznym w wymiarze Improving Performance podczas całych prac badawczych pochylono się nad zagadnieniem metod zapobiegania przyczynom przestępczości zarówno w kontekście procesu podejmowania decyzji, zarządzania ryzykiem, operacjami na rynku energetycznym, przestępstw popełnianych na rynku energetycznym, zorganizowanej

przestępczości na rynku energetycznym oraz wykorzystania nowoczesnych technologii w energetyce, jak i form dokonywania przestępstw w tym obszarze oraz metod zapobiegania im. Odpowiednie sprofilowanie wskazanych powyżej segmentów badawczych umożliwiło dokonanie analizy typu Improving Performance.

Na rynku ubezpieczeniowym w wymiarze Improving Performance podczas całych prac badawczych pochylono się nad zagadnieniem metod zapobiegania przyczynom przestępczości zarówno w kontekście procesu podejmowania decyzji w zakładzie ubezpieczeń, zarządzania ryzykiem, operacjami na rynku ubezpieczeniowym oraz 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 powyżej segmentów badawczych umożliwiło dokonanie analizy typu Improving Performance.

W zarządzaniu ludźmi w organizacji w wymiarze Improving Performance podczas całych prac badawczych pochylono się nad zagadnieniem metod zapobiegania przyczynom przestępczości zarówno w kontekście 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. Odpowiednie sprofilowanie wskazanych powyżej segmentów badawczych umożliwiło dokonanie analizy typu Improving Performance.

W związku z powyższym, niestandardowe ujęcie problematyki przeciwdziałania przestępczości pozwoliło na fundamentalną analizę przedstawionych segmentów badawczych oraz aktualnie stanowi podstawy do dalszych prac i ukazuje konieczność podjęcia współpracy, w tym współpracy międzynarodowej.

3. Improving Performance: Metodologia

Właściwie dobrana i wrażliwa na przedmiot analizy metodologia stanowi fundament odpowiednio przygotowanych oraz nakierunkowanych na kryteria ewaluacyjne[9] badań naukowych. W module Improving Performance wykorzystano pełne instrumentarium, jakie daje klasyczna dla nauk prawnych metoda dogmatyczno-formalna (egzegeza treści aktu prawnego oraz hermeneutyka językowa). Dodatkowo została wykorzystana metoda prawnoporównawcza, gdzie posłużono się w jej ramach metodą komparatystyki prawniczej Kötza i Zweigerta. Zawiera ona w sobie pięć faz, które powinny stanowić określony porządek chronologiczny działania. Zgodnie z powyższym, następują po sobie: 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 wykorzystanego katalogu metod i technik badawczych należą także metody i techniki: heurystyczne (odroczone wartościowanie, transpozycja, sugerowanie oraz metody złożone), funkcjonalne (hermeneutyka swobodna),

[9] Np. oryginalność, racjonalnośći praktyczność teorii, perspektywa, kompleksowość orazkompatybilność badań, prawdopodobieństwo iperspektywa zastosowania, korzyści ekonomiczne orazspołeczne, promowanie efektów, przejrzystość i przystępność.

[10] Zob. ogólnie: R. Tokarczyk, *Komparatystyka prawnicza*, Oficyna a Wolters Kluwer business, Warszawa 2008.

analizy i krytyki piśmiennictwa, analizy i konstrukcji logicznej, badania dokumentów, monograficzne oraz obserwacyjne. Badacze dokonujący analiz wzięli pod uwagę również mate-językowo określony 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, strategii oraz dokumentów operacyjnych; liczba opracowanych rozwiązań; liczba pilotaży (wdrożeń) wypracowanych rozwiązań).

4. Improving Performance: Potencjalni beneficjenci prac projektowych

Z uwagi na fakt, że moduł Improving Performance stanowił jedną z czterech zasadniczych części prac projektowych (inne: Assessing Foundations, Transforming People and Organizations oraz Heading Into the Future), konieczne okazało się określenie właściwej grupy potencjalnych beneficjentów. Stanowiło to także organizacyjną podstawę przepływu informacji w ramach Projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości". Powyższe jest niezbędne w celu dystrybucji jasnych, praktycznych oraz użytecznych rekomendacji, wytycznych oraz wymiernych rezultatów. Prowadzone prace związane z ustaleniem i zapobieganiem przyczynom przestępczości nakierunkowano, co już podkreślano, na cztery podstawowe obszary polskiej gospodarki: finanse, ubezpieczenia, energetyka oraz zarządzanie ludźmi w organizacji. Każdy z wymienionych obszarów posiada swoją specyficzną listę potencjalnych beneficjentów, niezależnie od prowadzonego modułu, oraz wspólną listę podmiotów naukowych mogących być zainteresowanymi wynikami prowadzonych analiz, także abstrahującą od podziału modułowego. Oznacza to, że lista potencjalnych beneficjentów modułów Assessing Foundations, Improving Performance, Transforming People and Organizations oraz Heading Into the Future jest identyczna.

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. Improving Performance: Ochrona praw człowieka jako istotny element prac projektowych

Niezależnie od dokonywanych podziałów systematyzujących prace projektowe (np. Improving Performance) oraz nakierunkowanych na gradację realizowanych zadań kwestią niezwykle istotną jest wskazanie na fundamentalne prawa i wolności człowieka, które zyskują miano przewodnika po prowadzonych pracach badawczych. Sygnalizowana zależność była także brana pod uwagę w ramach przedmiotowych prac projektowych. Podczas każdych badań naukowych mających na celu wypracowanie wymiernych rezultatów oraz rekomendacji, które mają znaleźć uznanie wśród zarówno teoretyków, jak i praktyków, konieczne jest uwzględnianie określonej matrycy prawno-człowieczej. Uwaga ta ma szczególne znaczenie, jeżeli wyniki prowadzonych prac analitycznych mogą znaleźć odzwierciedlenie normatywne bądź mogą być implementowane w instytucjach oraz firmach zarządzających zasobami ludzkimi, co rodzi swoiste pole potencjalnego zagrożenia. Autorsko wyselekcjonowany katalog praw człowieka jest jedynie matrycą limitującą oraz profilującą rozwiązania projektowe. Z uwagi na przypisywanie przedmiotowej problematyce statusu wiodącego prawa i wolności wskazywano zbiorczo w kontekście wszystkich czterech modułów analitycznych. Zatem zapobieganie przyczynom przestępczości, w tym metody jej zwalczania, w finansach, energetyce, ubezpieczeniach oraz zarządzaniu ludźmi w organizacji wypada konfrontować z zakresem i wykładnią regulacji z zakresu konstytucyjnej ochrony praw i wolności (Konstytucja Rzeczypospolitej Polskiej[11]) oraz europejskiej ochrony praw człowieka (1. Unia Europejska – Karta praw podsta-

[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. z 1997 r. Nr 78 poz. 483; 2001 Nr 28 poz. 319; 2006 Nr 200 poz. 1471; 2009 Nr 114 poz. 946).*

wowych 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".

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

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

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

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. Improving Performance: Uzasadnienie prowadzenia prac badawczych

Powodów uzasadniających prowadzenia prac badawczych związanych z analizą korelacji prawa, gospodarki i technologii na rzecz zapobiegania przyczynom przestępczości na rynku finansowym, energetycznym, ubezpieczeniowym oraz zarządzania ludźmi w organizacji w kontekście Improving Performance jest wiele. Racjonalne jest przedstawienie tych najważniejszych, bazując na podziale sektorowym.

Uzasadnieniem podejmowania prac badawczych na rynku finansowym w świetle Improving Performance jest określenie metod zapobiegania przestępczości, biorąc pod uwagę np. kwestię przeciwdziałania aktualnym nadużyciom, które podlegają nieustannej transformacji. Banki i fundusze inwestycyjne oraz inni aktorzy rynku finansowego to struktury, które powinny dostosowywać się do zmieniającej się rzeczywistości, co oznacza, że istotnym zadaniem jest wprowadzanie technologii informatycznej jako narzędzia zapobiegającemu przestępczości.

Uzasadnieniem podejmowania prac badawczych na rynku energetycznym w świetle Improving Performance jest określenie metod zapobiegania przestępczości, biorąc pod uwagę np. straty dla zakładów energetycznych, które są powodowane m.in. kradzieżą energii elektrycznej oraz składników infrastruktury energetycznej. Przedmiotowe przestępstwa powodują również wiele newralgicznych płaszczyzn zagrożeń zarówno dla osób, jak i instytucji. Ten sektor polskiej gospodarki narażony jest również na działalność zorganizowanych grup przestępczych czy pranie pieniędzy.

Uzasadnieniem podejmowania prac badawczych na rynku ubezpieczeniowym w świetle Improving Performance jest określenie metod zapobiegania przestępczości, biorąc pod uwagę np. fakt, że ten typ przestępczości od kilku lat budzi w kraju coraz większy niepokój, stanowiąc przedmiot zainteresowania zarówno podmiotów objętych ubezpieczeniami, jak i organów ścigania czy też szeroko pojętego rynku ubezpieczeniowego. Związane jest to także nie tylko z kosztami społecznymi, ale również ze stratami samych zakładów ubezpieczeń, akcjonariuszy oraz ubezpieczonych. Obowiązujące prawo powinno chronić sytuację finansową ubezpieczycieli, gdyż przestępstwa ich dotyczące mogą znacznie utrudnić prowadzenie działalności gospodarczej.

Uzasadnieniem podejmowania prac badawczych w zarządzaniu ludźmi w organizacji w świetle Improving Performance jest określenie metod zapobiegania przestępczości, biorąc pod uwagę np. fakt unikania przez przedsiębiorstwa wywiązywania się ze zobowiązań wobec pracowników, co stanowi jeden z głównych i wielce problematycznych wątków w ich dzisiejszym funkcjonowaniu. Chodzi nie tyle o brak wypłaty wynagrodzeń dla pracowników, ile o wymuszanie na nich pracy niezgodnej z regulacjami prawnymi oraz na zakłócaniu równowagi pomiędzy czasem przeznaczonym na pracę i na rodzinę.

Uzasadniona jest zatem naukowa analiza prawa, gospodarki i technologii w kontekście zapobiegania przyczynom przestępczości finansowej, energetycznej, ubezpieczeniowej oraz w zarządzaniu ludźmi w organizacji w świetle Improving Performance.

ROZDZIAŁ II

Zapobieganie oszustwom finansowym

ALINA KLONOWSKA[1], MAGDALENA MAŁECKA-ŁYSZCZEK[2],
MAŁGORZATA SNARSKA[3], JOANNA WYROBEK[4]

1. Teoretyczne podstawy zapobiegania przestępstwom finansowym

Istniejące modele motywacji do oszustw przedstawiają jednocześnie koncepcję im zapobiegania. Według teorii trójkąta oszustw konieczne jest usunięcie jednego z czynników: presji, racjonalizacji lub okazji. Oczywiście nie da się tych czynników wyeliminować całkowicie, ale już samo zmniejszenie ich skali może ograniczyć skalę oszustw.

---

[1] Doktor nauk ekonomicznych, zatrudniona na stanowisku adiunkta 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 e-mail: 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, zatrudniona na stanowisku adiunkta 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.

[4] Doktor habilitowany nauk ekonomicznych, zatrudniona na stanowisku profesora w Katedrze Finansów Przedsiębiorstw w Kolegium Ekonomii, Finansów i Prawa Uniwersytetu Ekonomicznego w Krakowie. Zainteresowania naukowe obejmują zarządzanie finansami przedsiębiorstw. Adres e-mail: wyrobekj@uek.krakow.pl

Zmniejszenie presji można uzyskać poprzez wychowanie nastawione mniej na dobra materialne, a więcej na bezpośrednie zaangażowanie rodziców w ten proces i wspólnie spędzany czas[5]. Rosnący dochód na mieszkańca i podnoszenie standardów życia również potencjalnie obniża presję na dorabianie się za każdą cenę[6], bo wyższy dochód zaspokaja więcej potrzeb człowieka. Człowiek żyjący w skrajnej biedzie może nie mieć nic do stracenia. Korzystna byłaby zmiana mentalności i podejścia do państwa, które obecnie jest zbliżone do mentalności południowej, na korzyść mentalności ludów północy – gdzie państwo jest traktowane jako godne zaufania i dobrowolnie wspierane[7]. Również poprawa wizerunku whistleblowerów może pomóc w częstszym zgłaszaniu przestępstw[8].

Kolejnym elementem redukcji presji wydaje się być przejrzystość przetargów publicznych i wszelkich działań urzędów publicznych, począwszy od rządu, na gminach skończywszy[9]. Innym pomocnym narzędziem wydaje się być stabilność polityczna, ekonomiczna i prawna. Nieustanne zmiany i reformy powiększają strach i niepewność, a to sprzyja powstawaniu nieprawidłowości[10].

Bardzo istotnym elementem redukcji presji jest przekonanie potencjalnych przestępców, że nie unikną kary. Brak karalności bowiem prowadzi do presji na pracowników i menedżerów, że co prawda dane postępowanie jest dalekie od etycznego, ale skoro nie ma za to kary, to mają robić to samo, aby podnieść zyski. Redukcja tego problemu to zarówno uproszczenie przepisów, jak i zatykanie luk w prawie.

Wydaje się również, że wpływ na poziom presji może mieć sztywność struktur społecznych i przekonanie społeczne o możliwości awansu społecznego dzięki ciężkiej i uczciwej pracy. Istnieje np. sporo opracowań pokazujących

---

[5] O. Górniok O., *Przestępczość gospodarcza i jej zwalczanie*, Wydawnictwo Naukowe PWN, Warszawa, 1994, s. 135.

[6] Ibid., s. 41.

[7] M. Pasternak-Malicka, *Mentalność i moralność podatkowa a reakcje gospodarstw domowych na obowiązek podatkowy*, „Modern Management Review", 2013, nr 18 (20), s. 87–98.

[8] W. Rogowski, *Whistleblowing czyli czego się nie robi dla pozyskania zaufania inwestorów*, „Przegląd Corporate Governance", 2007, nr 2 (10), s. 3.

[9] A. Kojder, *Korupcja i poczucie moralne Polaków*, w: *Kondycja moralna społeczeństwa polskiego*, red. J. Mariański, Wydawnictwo WAM, Kraków 2002, s. 233–252.

[10] O. Górniok, *Przestępczość gospodarcza…*, op. cit., s. 135.

wpływ powtarzania klasy na prawdopodobieństwo bycia skazanym. Zależność jest silna i statystycznie istotna[11].

Drugim elementem potencjalnego przerwania trójkąta oszustw jest **uniemożliwienie zracjonalizowania** przestępstwa. Im lepszy kręgosłup moralny rozwinąć w człowieku, im trudniej mu nałożyć błoto psychologiczne, tym trudniej siebie oszukiwać, że zły czyn służył większemu dobru.

Lekarstwem na racjonalizację może być konfrontacja ludzi z faktami. Przekonanie o niezwykle zawyżonych daninach publicznych w Polsce można korygować przedstawieniem rzeczywistych danych. Niestety, ludzie często cechują się konserwatyzmem w wyznawanych poglądach i być może dlatego część krajów stosuje propagandę – bo zwykłe, rzetelne fakty mogą nie być wystarczające, aby ktoś zmienił zdanie. Również obniżenie tolerancji na oszustwa i przestępstwa jest bardzo ważnym czynnikiem zapobiegawczym. Zagrożenie odrzuceniem społecznym lub przez rodzinę także jest takim czynnikiem[12]. Niestety, przynajmniej w przypadku niektórych rodzajów przestępstw finansowych tolerancja Polaków zamiast maleć, rośnie[13].

Trzecim elementem zapobiegania przestępczości jest likwidacja **okazji** ku nim. Oczywiste jest, że przede wszystkim warunkiem braku okazji jest skuteczny nadzór i sprawne systemy kontroli, których nie można wyłączyć ani obejść (nawet osoby posiadające do nich dostęp). To oznacza m.in. także jasne wyznaczenie kompetencji każdego systemu i każdej instytucji oraz przepływ informacji pomiędzy nimi, a także odpowiednie uprawnienia decyzyjne i operacyjne. Eksperci uważają, że służby te w Polsce nie są najlepiej zorganizowane, są niedoinwestowane[14], niedostatecznie wyposażone w środki prawne, materialne oraz kadrowe[15]. W Polsce instytucje zajmujące się przestępczością finansową to m.in.: Generalny Inspektor Informacji Finansowej

---

[11] O. Eren, B. Depew, S. Barnes, *Test-based promotion policies, dropping out, and juvenile crime*, „Journal of Public Economics", 2017, nr 153, s. 9–31.

[12] J. Solska, *Polacy coraz bardziej tolerancyjni wobec finansowych przekrętów*, „Polityka", 22.08.2019, https://www.polityka.pl/tygodnikpolityka/rynek/1716548,1,polacy-coraz-bardziej-tolerancyjni-wobec-finansowych-przekretow.read (dostęp: 1.09.2019).

[13] Ibid.

[14] J. Trubarska, *System antyterrorystyczny w Polsce – wybrane zagadnienia*, „Zeszyty Naukowe AON", 2016, nr 4 (105), s. 153–166.

[15] A. Kubiczek, *Przestępczość gospodarcza – czy można ją ograniczyć?*, „Nierówności społeczne a wzrost gospodarczy", 2015, nr 2 (42), s. 276.

wspomagany przez Departament Informacji Finansowej Ministerstwa Finansów (który wykonuje zadania Polskiej Jednostki Analityki Finansowej), NBP, Agencja Bezpieczeństwa Wewnętrznego, CBA, Policja (w tym cyberpolicja), KNF, GPW, ZBP (Związek Banków Polskich)[16], KIBR, Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa, prezesi sądów apelacyjnych (w odniesieniu do notariuszy), naczelnicy urzędów celno-skarbowych, wojewodowie lub starostowie (wobec stowarzyszeń), pomiędzy którymi są rozłożone różne kompetencje[17]. Oprócz instytucji państwowych aktywną walkę z przestępczością prowadzą banki, które (na mocy ustawy z 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu oraz prawie bankowym) muszą zapobiegać przestępstwom finansowym. Warto wspomnieć, że w ramach struktur policyjnych działa jednostka ARO (Asset Recovery Office), czyli biuro do spraw odzyskiwania mienia (dopiero przypadek ukradzionego mienia ma charakter prewencyjny). W przypadku zwalczania terroryzmu (i finansowania terroryzmu) odpowiedzialny jest GIIF, Służba Celna, Straż Graniczna, Policja i ABW[18].

Z uwagi na częsty międzynarodowy charakter oszustw i prania brudnych pieniędzy zapobieganie im opiera się zwykle na współpracy licznych służb i banków z wielu krajów, aby wyśledzić sprawców, narzędzia oraz pieniądze, które ukradli. Wiele państw koordynuje także swoje ustawodawstwo i systemy nadzoru, aby jednolicie reagować i zapobiegać przestępczości finansowej. Przekazują sobie dobre i złe doświadczenia, aby szybciej wypracowywać skuteczne rozwiązania. Współpraca między służbami i instytucjami jest niezmiernie ważna, podobnie jak przekazywanie danych i odpowiednich

[16] Związek Banków Polskich FinECERT.pl – wspiera Członków oraz podmioty współpracujące w zakresie wykrywania, analizowania podatności, zagrożeń i incydentów oraz koordynując i zarządzając incydentami o skutkach oddziaływania: sektorowych, międzysektorowych i międzynarodowych.

[17] Zwalczaniem przestępczości finansowej w skali światowej zajmują się m.in. Interpol, FATF (ang. *Financial Action Task Force* – inicjatywa grupy G7), Komitet Bazylejski (ang. BCBS – Basel Committee on Banking Supervision), Grupa Wolfsburg (stowarzyszenie 13 banków), Międzynarodowy Fundusz Walutowy, Światowe Forum Ekonomiczne, Instytut Finansów Międzynarodowych, Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy, Biuro Narodów Zjednoczonych ds. narkotyków i przestępczości (ang. UNODC), CARIN (ang. Camden Assets Recovery Interagency Network,) w Unii Europejskiej Europol, OLAF.

[18] J. Trubalska, *System antyterrorystyczny w Polsce…*, op. cit.

środków i narzędzi oraz jasnych i skutecznych strategii oraz wyszukiwanie ukradzionych aktywów.

Polska aktywnie także walczy z korupcją, m.in. wdrażając konwencję OECD (z 1997 roku o zwalczaniu przekupstwa zagranicznych funkcjonariuszy publicznych w międzynarodowych transakcjach handlowych), własne programy zwalczania korupcji, realizuje także programy Międzynarodowego Funduszu Walutowego oraz Banku Światowego, w ramach których są realizowane cztery cele[19]: zapobieganie korupcji i oszustwom w projektach finansowanych przez te instytucje, pomaganie w redukowaniu korupcji, tworzenie strategii wsparcia dla krajów z wyraźnym nakierowaniem na zwalczanie korupcji oraz wspomaganie międzynarodowych programów do walki z korupcją. Programy walki z korupcją[20] przewidują tworzenie w organizacjach kultury nieakceptującej łapówkarstwa , uświadamianie społeczeństwu jego szkodliwości, aby była potępiana społecznie, tworzenie przekonania, że korupcja zostanie wykryta i ukarana, kontrola nowych programów publicznych i działań, czy są zabezpieczone przed działaniami korupcyjnymi, testowanie, czy programy publiczne przechodzą pozytywnie przez kontrolę antykorupcyjną, wzmacnianie kontroli antykorupcyjnej.

Innym elementem kontroli są biegli rewidenci i obowiązkowy audyt sprawozdań finansowych wszystkich dużych podmiotów gospodarczych i finansowych. Co prawda, audyt sprawozdań finansowych to nie to samo co audyt śledczy, jednak rewidenci mają obowiązek zgłaszania wykrytych nieprawidłowości. Z kolei nad solidnością audytu sprawozdań finansowych (zewnętrzni biegli rewidenci są częściowo zależni od władz spółki, bo to one dokonują wyboru która firma wykona audyt co rodzi konflikt interesów) czuwa rada nadzorcza, a nad solidnością rady nadzorczej czuwają akcjonariusze (szczególnie ci aktywni, dynamicznie nadzorujący działania spółki).

Kolejnym ogniwem redukowania okazji do popełniania przestępstw finansowych są odpowiednie procedury wewnętrzne zapobiegające oszustwom. Jakkolwiek część z systemów jest nieskuteczna i zrobiona na pokaz, to jednak coraz częściej można zaobserwować systemy skuteczne i zapobiegające

[19] G. Ksenia, *Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective?*, „Journal of Financial Crime", 2008, nr 15 (2), s. 223–233.

[20] P. Gottschalk, *Policing financial crime*, Brown Walker Press, Floryda 2009, s. 115.

przynajmniej części z przestępstw. Badania wskazują, że z uwagi na zaufanie, jakim się cieszą sprawcy przestępstw finansowych, zwalczanie takich oszustw to przede wszystkim zmiana środowiska, w którym dochodzi do przestępstw, a nie samych przestępców[21]. Próbą regulacji nadzoru korporacyjnego jest ustawa Sarbanesa-Oxleya z 2002 r. w Stanach Zjednoczonych, a w Polsce dobre praktyki ładu korporacyjnego, które przygotował Komitet Dobrych Praktyk Forum Corporate Governance i które zostały przyjęte przez GPW w 2002 r.[22] Praktyki te nie są jedynie stosowane w spółkach notowanych na GPW – stanowią bardzo istotne źródło informacji dla wszystkich większych przedsiębiorstw w Polsce.

Istotnym narzędziem w walce z przestępczością finansową jest rosnący trend świadomego, etycznego inwestowania, w ramach którego akcjonariusze nadzorują działania spółek pod kątem etyki działań, nadzoru właścicielskiego, a także zrównoważonego rozwoju i reagują na złamanie ich zaufania[23]. Bardzo skuteczne są działania aktywnych udziałowców i klientów, jeżeli w reakcji na oszustwo czy nieprawidłowości wycofują oni swoje inwestycje lub zmieniają dostawcę (klienci).

Nie można także nie wspomnieć o informowaniu społeczeństwa o nowych i istniejących zagrożeniach oszustwami finansowymi, co można uzyskać poprzez dostęp do osób fizycznych przez internet, telewizję, radio i prasę. Zwykle w każdym kraju istnieje instytucja, której zadaniem jest nie tylko zwalczanie przestępczości finansowej (często jest to podzielone na jej różne rodzaje), ale także za uczenie się o nowych formach tych przestępstw. Dużą pomocą jest Interpol. W Polsce publiczne informacje o przestępstwach i zagrożeniach można znaleźć m.in. na stronach KNF, NBP, ZBP.

Ważną rolę w zapobieganiu przestępstwom finansowym odgrywają także władze ustawodawcze, zapobieganie bowiem przestępstwom finansowym wymaga wdrażania nowych regulacji w ślad za nowymi technikami oszustw,

---

[21] Ibid., s. 111.

[22] K. Winiarska (red.), *Zakres zastosowań audytu wewnętrznego*, w: *Audyt wewnętrzny. Teoria i zastosowanie*, Difin, Warszawa 2017, s. 137–159.

[23] I.I. Hansen, *Corporate financial crime: social diagnosis and treatment*, „Journal of Financial Crime", 2009, nr 16, s. 28–40.

aby były one uregulowane i prosto było sprawców ukarać[24]. Jednym z bardzo istotnych aktów prawnych związanych z walką z przestępczością finansową jest RODO, czyli ogólne rozporządzenie o ochronie danych osobowych.

Innym narzędziem uskuteczniania walki z przestępstwami finansowymi jest nadzór organizacji prawniczych nad etycznością prawników. Niekiedy prawnicy i notariusze pomagają przestępcom w popełnianiu oszustw przez tworzenie strategii ukrywania ukradzionych pieniędzy[25].

Wiele krajów realizuje także programy przewidywania przyszłych przestępstw i aktywnego im zapobiegania poprzez wdrażanie nowych przepisów oraz narzędzi nadzoru i kontroli. Jeżeli przewiduje się granualizację przestępstw, które będą dotykały ogromną liczby ludzi, ale wielkość szkody będzie znikoma, to tworzone są narzędzia pozwalające wykrywać takie oszustwa. Jeżeli oczywiste jest, że liczba logowań do banków z telefonów komórkowych będzie lawinowo rosła (i że systemy bankowe nie są przygotowane na taką liczbę logowań), to wdrażane są przepisy i procedury mające zapobiec możliwym konsekwencjom tego zagrożenia (m.in. zatrudnianie żywych osób do nadzoru). Planowanie pozwala nie tylko przygotować rozwiązania, ale także zaplanować współpracę instytucji i służb ze sobą, gdy dojdzie do danego rodzaju przestępstwa. Na poziomie organizacji tworzone są nowe sposoby ustalania odpowiedzialności i nadzoru pracowników właśnie pod kątem nowych przestępstw.

2. Postulaty dotyczące poprawy systemu prawnego w zakresie przepisów dotyczących przestępczości finansowej

Przestępstwa na rynkach finansowych przynależą do szerokiej puli przestępstw gospodarczych, których specyfiką jest to, iż – w odróżnieniu od typowej przestępczości przeciwko mieniu – w większości przypadków stanowią

[24] P. Hardouin, *Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing*, „Journal of Financial Crime", 2009, nr 16 (3), s. 199–209.

[25] H. Nelen, F. Lankhorst, *Facilitating organized crime: the role of lawyers and notaries*, w: D. Siegel, H. Nelen (eds), *Organized crime: Culture, Markets and Policies*, Springer, New York 2008, s. 127–142.

kategorię, której rejestrowane w regularnych statystykach zależy w znacznie większym stopniu od aktywności wykrywczej organów kontrolnych oraz organów ścigania. Postępowania są zazwyczaj wszczynane nie na podstawie doniesień osób poszkodowanych, lecz w oparciu o informacje własne organów państwowych pozyskane w wyniku realizowanych przez nie działań, a zarejestrowane w statystykach przypadki stanowią tylko pewien wycinek szerszej puli zjawisk. Pełne rozmiary tejże przestępczości (przy uwzględnieniu ciemnej liczby, tj. skali przestępstw pozostających poza wiedzą właściwych organów ścigania), nie są znane i mogą podlegać wyłącznie szacowaniu. Dodatkowo brak jest spójnych statystyk wszystkich służb, organów i instytucji, które pozwalają na przekrojowe określenie skali zjawiska tejże przestępczości[26].

Pierwsza część niniejszego opracowania odnosząca się do wskazania właściwych/możliwych rodzajów przestępstw na rynkach finansowych i sankcji, jakie są związane z ich popełnieniem, zobrazowała, z jak szerokim zakresem przedmiotowym mamy do czynienia w obranym obszarze tematycznym. Dlatego uwagi czynione w ramach niniejszego punktu będą miały charakter przykładowy, dotykający wybranych aspektów możliwych do wyeksponowania w obliczu istniejących tutaj *wicked problems*.

Pierwsza z poruszanych kwestii, na jakie należy zwrócić uwagę, to **niejasność przepisów**, która przekłada się na niejednoznaczne oceny co do możliwości kwalifikacji określonych czynów jako przestępstw na rynku finansowym. Przykładowo: klauzula normatywna „bez zezwolenia", użyta w typizacji przestępstwa z art. 171 ust. 1 u.p.b. nie jest do końca adekwatna treściowo. Zezwolenie kojarzone z indywidualnym aktem administracyjnym (decyzją administracyjną) jest wprawdzie najczęstszym sposobem dopuszczenia do wykonywania reglamentowanej przez państwo działalności bankowej, ale nie jedynym w świetle obowiązujących przepisów. W szczególnych przypadkach uchylenie reglamentacji w tej sferze działalności gospodarczej następuje na mocy rozporządzenia Rady Ministrów (banki państwowe – art. 14 ust. 1 u.p.b.) czy umowy agencyjnej zawartej między bankiem a przedsiębiorcą , o której bank jedynie zawiadamia KNF (art. 6a ust. 1 pkt 1 i ust. 2 u.p.b.).

[26] Załącznik do uchwały nr 181 Rady Ministrów z dnia 6 października 2015 r. w sprawie „Programu przeciwdziałania i zwalczania przestępczości gospodarczej na lata 2015–2020" (M.P. 2015 poz. 1069), s. 8.

Zasadne wydaje się zatem, aby w drodze kolejnej nowelizacji zmienić brzmienie klauzuli „bez zezwolenia" i zastąpić ją szerszym sformułowaniem, którego zakres obejmie różne źródła uprawniające do prowadzenia działalności bankowej, np.: „Kto bez wymaganego zezwolenia lub upoważnienia zawartego w odrębnych przepisach albo nie będąc do tego uprawnionym w inny sposób określony w ustawie (…)" albo syntetycznie „Kto nie będąc do tego uprawnionym (…)"[27]. Jak podkreśla się w literaturze przedmiotu, prawo karne może być efektywne tylko wówczas, gdy hipoteza normy sankcjonującej jest sformułowana w taki sposób, aby organy stosujące prawo mogły ją egzekwować, gdyż niewykonalność sankcji stwarza poczucie bezradności i prowadzi do obniżenia prestiżu prawa karnego. W związku z tym w doktrynie prawniczej wysuwany jest postulat, aby **nie tworzyć nieefektywnych przepisów zawierających opisy czynów, których nie sposób udowodnić**. Dzieje się tak choćby w przypadku **manipulacji transakcyjnych, które od zachowań legalnych (np. spekulacji giełdowej) można odróżnić tylko na podstawie przeżyć psychicznych i negatywnych intencji ich sprawcy**, czyli po wnikliwym zbadaniu strony podmiotowej przestępstwa. Wina rozumiana jest jako określony psychicznie stosunek sprawcy do popełnionego czynu i wyraża psychiczne zaangażowanie sprawcy w dokonywany czyn. Przestępstwem nie jest zaś czyn, który odpowiada pewnemu opisowi danego przepisu prawa, ale popełniony został w sposób niezawiniony (brakuje winy). Manipulacji instrumentami finansowymi można jednakże dokonać jedynie w sposób umyślny. W rezultacie art. 39 ust. 2 pkt 1 i 2 u.o.i.f. nie nadaje się do penalizacji ze względu m.in. na: nieprecyzyjność czynności sprawczej i nieprzewidywalność określających ją przepisów (niefakultatywne odesłania do uchwały KNF, wydanie której Komisja uznaje za zbędne), wykorzystywanie w rekonstrukcji znamion czynności sprawczej kontratypów o charakterze domniemania bezprawności – na sprawcę przerzucany jest ciężar dowodu, co jest w sprzeczności z zasadą domniemania niewinności[28].

---

[27] Tak: P. Bachmat, *Prokuratorska praktyka ścigania przestępstw z art. 171 ust. 1 i 3 prawa bankowego. Przypadki umorzeń oraz odmów wszczęcia postępowania*, „Prawo w Działaniu", 2014, nr 18, s. 178–179.

[28] C. B. Martysz, 2.1. *Ochrona karnoprawna*, w: *Manipulacje instrumentami finansowymi i insider trading*, LEX, 15.08.2019, https://sip.lex.pl/#/monograph/369369510/283885 (dostęp: 29.08.2019).

Ponadto w obszarze przestępstw na rynkach finansowych widoczne jest **rozproszenie przepisów i duża ich kazuistyka**[29]. Praktycznych trudności przysparza również konieczność łączenia regulacji z obszaru prawa cywilnego, administracyjnego i nieodzownego w przypadku przestępstw – prawa karnego. W rezultacie konieczne jest wzmacnianie spójności systemowej zewnętrznej i wewnętrznej. Nie jest to kwestia jedynie dywagacji natury teoretycznej, ale dążenie do **zwiększenia spójności rozsianych po ustawach szczegółowych przestępstw** ma swój istotny wymiar praktyczny. Przykładowo w art. 178 u.o.i.f. (przestępstwo nieuprawnionego obrotu instrumentami finansowymi) ustawodawca nie przewidział tzw. klauzuli odpowiedzialności zastępczej. Oznacza to, że w konkretnej sprawie zachodzi trudny w praktyce wymóg dokładnego rekonstruowania i wykazania, że dana osoba fizyczna swoim zachowaniem realizowanym w zorganizowanej wieloosobowej strukturze wypełniła znamiona sprawstwa pojedynczego albo innej formy zjawiskowej popełnienia przestępstwa (sięgając do art. 18 k.k.). A przecież w przeciwnym przypadku osoba taka nie może odpowiadać karnie. Tym samym w praktyce pominięcie przez ustawodawcę klauzuli odpowiedzialności zastępczej może prowadzić do istotnej dysfunkcjonalności analizowanego przepisu[30].

Dodatkowa trudność może wynikać i z tego, iż rodzimy ustawodawca zdecydował się na zastosowanie tzw. techniki kryminalizacji blankietowej – tzn. dla odczytania pełnej zawartości normatywnej przepisów karnych należy ustalić odpowiednie pozakarne przepisy odniesienia (czyli stanowiące treść wypełniającą blankiet)[31]. Z uwagi na dokonujące się nowelizacje tych przepisów i konieczność zdekodowania sieci regulacji pozakarnych nie zawsze jest to zadaniem łatwym.

Kolejną płaszczyznę analizy rodzi problematyka pozyskiwania stosownych dowodów w przypadku omawianego typu przestępstw. Tak naprawdę w przypadku z każdego ze wskazanych w pierwszej części niniejszego opracowania rodzajów przestępstw, siłą rzeczy spotykamy się z **trudnościami dowodowymi** i dlatego silny nacisk należy położyć na **szkolenie służb i pozyskiwanie**

[29] Por. P. Ochman, *Karnoprawna ochrona rynku kapitałowego*, Londyn 2014, s. 32.

[30] R. Zawłocki, Art. 178, w: *Komentarz do ustawy o obrocie instrumentami finansowymi*, w: *Prawo rynku kapitałowego. Komentarz*, LEX, 19.08.2019, https://sip.lex.pl/#/commentary/587675945/473385 (dostęp: 28.08.2019).

[31] P. Ochman, *Karnoprawna ochrona…*, op. cit., s. 331.

fachowców dysponujących należytą wiedzą pozwalająca na prawidłowe ustalanie stanu faktycznego i wychwytywanie dysfunkcji i mechanizmów przestępczych. Dlatego tak jak zróżnicowane i rozproszone po licznych ustawach są przestępstwa przeciwko rynkowi finansowemu (gdyż jak zostało wskazane, odnoszą się do rozmaitych aspektów związanych z jakże szerokim pojęciem rynku finansowego), tak liczne są możliwe przestępstwa w tym obszarze i tym samym wiele jest metod przestępczego działania, a ponadto stale one ewoluują. Chcąc zobrazować niniejsze kwestie, można sięgnąć np. do art. 229 k.k[32], którego § 1 odnosi się m.in. do podejmowania czynności mogących udaremnić lub znacznie utrudnić czynności dowodowe. Jak słusznie zauważa się w literaturze przedmiotu, prowadzone w tych sprawach wysiłki dowodowe nie są łatwe z powodu niemożności pełnego wyliczenia wszystkich sposobów przestępczego postępowania. Należy dowieść uniemożliwianie lub znaczne utrudnienie w uzyskaniu wymienionych w art. 229 § 1 i 2 k.k. efektów (umowy kompensacyjne, transfer *pricing*, wycena przedmiotów majątkowych poniżej ich wartości lub w nadmiernej wysokości). Natomiast świadczenie innych usług bankowych z § 2 to zamiar trwałego podejmowania zachowań polegających na zatajaniu pochodzenia lub zabezpieczenia transferowanych środków przed zajęciem[33]. Wysiłki gromadzenia dowodów tego przestępstwa napotykają na przeszkody, chociażby z tego względu, że w momencie

[32] Art. 299 § 1 k.k.: „Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8". Jak i § 2: „Karze określonej w § 1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w § 1, lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem".

[33] Z. Kukuła, 11.5. *Pranie brudnych pieniędzy (k.k.)*, w: *Poszukiwanie dowodów przestępstw gospodarczych* Wydawnictwo Prawnicze LexisNexis, 15.08.2019, https://sip.lex.pl/#/monograph/369306195/238753 (dostęp: 26.08.2019).

dokonania blokady ze strony GIIF dla organizatorów procederu jest oczywiste, że został on wykryty, a to uruchamia wysiłki zmierzające do zacierania śladów przestępczej działalności (głównie w dokumentach finansowo-księgowych), co powoduje często utratę kluczowych dowodów. Postępowanie dowodowe w początkowej fazie koncentruje się wokół osób wynajętych do tego celu przez grupy przestępcze, skupiając na nich (a nie rzeczywistych sprawcach) zainteresowania organów ścigania i właściwych służb. Od strony prawnodowodowej podstawowe źródło stanowi rejestr transakcji prowadzonych przez GIIF. Wykorzystaniu podlegają tutaj dokumenty otrzymywane z banków wraz ze stanem obrotów na rachunku oraz danymi na temat ich posiadaczy. Dlatego celowe wydaje się zwrócenie do organów podatkowych i wywiadu skarbowego, skorzystanie z wiedzy biegłych z zakresu księgowości i finansów. W wielu tego rodzaju sprawach należy sięgać po przedsięwzięcia operacyjno-rozpoznawcze, łącznie z uruchomieniem takich form jak utrwalanie dźwięku i obrazu[34]. Natomiast innego rodzaju trudności dowodowe będzie rodziło chociażby udowodnienie popełnienia przestępstwa z art. 171 ust.1 u.p.b., gdzie istotne będzie udowodnienie (i to jest w praktyce najtrudniejsze), że celem gromadzenia środków pieniężnych było obciążenie ich ryzykiem[35]. Jeszcze inne trudności dowodowe rodzi środowisko bankowości elektronicznej, w którym coraz częściej dochodzi do popełnienia przestępstwa. W tym obszarze ślady w tradycyjnym znaczeniu występują w ograniczonym zakresie, natomiast podstawową rolę odgrywają ślady w elektronicznym zapisie. Jak wskazuje się w literaturze przedmiotu, dowodem elektronicznym jest informacja przechowywana lub przesyłana w postaci elektronicznej o znaczeniu dowodowym, a więc informacja np. zapisana na nośniku elektronicznym (dysku twardym komputera, w pamięci telefonu), dokument komputerowy (teksty tworzone w Wordzie, zdjęcia), dane cyfrowe (tzw. logi komputerowe), np. ukazujące historię logowania z danego IP (*Intentet Protocol*) komputera na dany serwer. Dowody elektroniczne mają zatem swoje cechy specyficzne, które w porównaniu z tradycyjnymi dowodami stanowią istotne *novum* wymagające uwzględnienia ich odrębności w procesie dowodzenia.

[34] Z. Kukuła, 11.5. *Pranie brudnych pieniędzy…*, op.cit.

[35] A. Kawulski, Art. 171, w: *Prawo bankowe. Komentarz*, Wydawnictwo Prawnicze LexisNexis, 19.08.2019, https://sip.lex.pl/#/commentary/587390265/187705 (dostęp: 26.08.2019).

Sprawca popełniający przestępstwo za pomocą internetu nie pozostawia tradycyjnych śladów identyfikujących (np. pismo ręczne, ślady biologiczne, daktyloskopijne), co powoduje, że indywidualizm sprawcy zaciera się. Specyficzne cechy dowodów elektronicznych determinują sposób prowadzenia procesu dowodowego. W pierwszej kolejności istotne jest zapewnienie udziału w czynnościach związanych z poszukiwaniem, zabezpieczaniem i utrwalaniem dowodów elektronicznych ekspertów, którzy posiadają specjalistyczną wiedzę w tym zakresie. Stosowne działania powinny być podjęte bez zbędnej zwłoki z uwagi na fakt, że dowody elektroniczne w każdej chwili mogą zostać usunięte z komputera. Niezwykle istotną kwestią jest zabezpieczanie, utrwalanie i przechowywanie dowodów elektronicznych. Co przekłada się na możliwość późniejszego ich wykorzystania na etapie czynności dowodowych w postępowaniu sądowym jako pełnowartościowych dowodów przestępstwa nadających się do przypisania na ich podstawie winy sprawcy bez obawy, że drugiej stronie postępowania uda się skutecznie podważyć ich wiarygodność. Dopuszczone przez sąd jako materiał dowodowy będą mogły być jedynie te dane, które zostały przygotowane w sposób zapewniający ich integralność i niepodważalną autentyczność, umożliwiając ich wykorzystanie w toku postępowania przed sądem jako pełnowartościowe dowody, których prawdziwość trudno jest zakwestionować[36].

Jednocześnie należy mieć na uwadze, że w praktyce organów ścigania i wymiaru sprawiedliwości to właśnie dowody elektroniczne będą odgrywały coraz istotniejszą rolę ze względu na postępujący rozwój nowych technik i tym samym rosnącą liczbę przestępstw pozostawiających ślady elektroniczne. Zdając sobie sprawę, że skuteczna walka z cyberprzestępczością wymaga zwiększonej, szybkiej i dobrze funkcjonującej współpracy międzynarodowej w sprawach karnych, Polska ratyfikowała Konwencję Rady Europy o cyberprzestępczości[37]. Oczywiście należy zauważy, iż na bieżąco podejmowane są stosowne działania, które mają usprawnić postępowania dowodowe w analizowanym obszarze. W tym kontekście należy przywołać chociażby 236a k.p.k.

---

[36] Szerzej: M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, KNF, Warszawa 2014, s. 42–48.

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

odnoszący się do odpowiedniego stosowania przepisów dotyczących zatrzymania rzeczy oraz przesłuchania do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną[38].

Z nowszych aktywności należy wskazać , że 14 sierpnia 2019 r. Prezydent RP Andrzej Duda podpisał przygotowaną przez Ministerstwo Sprawiedliwości ustawę reformująca k.p.k., która rezygnuje z niepotrzebnych przesłuchań, słusznie zauważając, iż poważnym obciążeniem dla policji i prokuratury w dochodzeniach i śledztwach jest nierzadko konieczność przesłuchiwana wszystkich pokrzywdzonych w sprawach dotyczących setek, a nawet tysięcy osób. Jeśli spojrzy się na sprawy oszustw internetowych czy też piramid finansowych[39] – kolejny pokrzywdzony zazwyczaj nie wprowadza do postępowania żadnych nowych faktów, a jedynie powiela już ustalone treści. Tym samym w założeniu nowelizacji **rezygnacja z obowiązku przesłuchiwania wszystkich pokrzywdzonych powinna przełożyć się na jakże potrzebne usprawnienie i przyspieszenie postępowań przygotowawczych, a także zapobiegnie zbędnemu przesłuchiwaniu pokrzywdzonych**.

Widoczne jest również zaostrzanie kar. Spoglądając chociażby na finansowanie przestępstw o charakterze terrorystycznym (art. 165a k.k.), proponuje się zaostrzenie odpowiedzialności karnej z 12 lat pozbawienia wolności na 15 lat (VIII.3451, Projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw). Jednocześnie pamiętać cały czas należy, że regulacje w obszarze przestępczości na rynkach finansowych muszą być kreowane mając na uwadze zarówno **odstraszający charakter kary, ale i zachowanie wymogu jej proporcjonalności**[40].

---

[38] Szerzej: A.Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo", 2003, nr 10, s. 16–25.

[39] Szerzej: M. Pachucki, *Piramidy i inne oszustwa na rynku finansowym*, KNF, Warszawa 2016, s. 7–17.

[40] Zob. np.: Zmiana ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz niektórych innych ustaw – projekt z dnia 6 sierpnia 2019 r., VIII, 3755.

3. Opis zasad budowy systemów stosowanych do wykrywania przestępstw finansowych

Zapobieganie przestępstwom finansowym wymaga od instytucji finansowych budowy systemów nadzoru i kontroli dostępu do danych, a także transakcji dokonywanych przez klientów oraz pracowników. Poniżej zostały omówione podstawowe zasady budowy takich systemów.

Jednym z narzędzi walki z przestępczością finansową jest zabezpieczenie cyberbezpieczeństwa. Organizacje muszą chronić swoje cyberbezpieczeństwo[41], a to poprzez określanie najbardziej zagrożonych obszarów i priorytetów oraz szacowanie, jakiego poziomu bezpieczeństwa potrzebują. Typowe systemy ochrony danych i systemów obejmują następujące narzędzia[42]:

- kontrolę dostępu do danych opartą na autoryzacji i autentykacji,
- korporacyjne firewalle, zarówno sprzętowe, jak i softwareowe,
- systemy wykrywania wtargnięć do systemu,
- oprogramowanie antywirusowe, antyphishingowe,
- szyfrowanie danych,
- certyfikaty elektroniczne dla plików,
- audyty systemu i jego bezpieczeństwa.

W praktyce pojęcie „systemu" rozumie się bardzo szeroko i często włącza się do niego pracowników, którzy są testowani pod kątem ostrożności przy otwieraniu załączników z e-maili, które np. nie są napisane poprawną polszczyzną albo zawierają błędy ortograficzne lub w wyraźny sposób są podróbką oryginalnej korespondencji. Pracownikom celowo podsyła się fałszywe e-maile, aby wyrobić w nich ostrożność. Podobnie zresztą część instytucji testuje uczciwość pracowników za pomocą podstawionych klientów.

W zakresie prania brudnych pieniędzy banki i instytucje nadzoru poszukują i identyfikują następujące działania[43]:

---

[41] M.P. Gallaher, A.N. Link, B.R. Rowe, *Cyber Security: Economic. Strategies and Public Policy Alternatives*, Cheltenham, Northampton 2008.

[42] K. Laudon, *Management information systems: managing the digital firm*, Prentice Hall, New York 2010.

[43] J. Leeuw, *Monitoring & Surveillance, About financial crime, prevention of market abuse and detecting suspicious trading behavior*, Entrima, dokument elektroniczny, 2019 oraz K.M. Kingsly, *Financial Crime Investigation*, Christian Faith Publishing Inc., New York, s. 170

1. Używanie sfałszowanych dokumentów.
2. Rachunek jest wyłącznie używany na depozyty gotówkowe.
3. Klient posługuje się fałszywymi danymi albo danymi trudnymi do sprawdzenia, odmawia udzielania dodatkowych informacji.
4. Rachunek otworzono dla kilku współposiadaczy, ale nie są powiązani rodzinnie ani biznesowo.
5. Rachunek otwarto dla firmy krajowej, ale obraca się na nim walutami obcymi niepowiązanymi z prowadzoną działalnością.
6. Rachunek służy stopniowemu przenoszeniu aktywów z jednej firmy do drugiej.
7. Czasami na potrzeby prania brudnych pieniędzy (i tylko w tym celu) tworzone są całe przedsiębiorstwa lub grupy przedsiębiorstw, których jedynym celem jest otwarcie (bardzo aktywnego) rachunku bankowego.
8. Brak uzasadnienia ekonomicznego dla realizowanych transakcji.
9. Kwoty transakcji są znacznie wyższe niż dochody klienta lub ich charakter jest zupełnie odmienny od charakteru działalności klienta.
10. Klient sam sobie udziela pożyczki.
11. Tworzenie złudzenia wzrostu wartości danego instrumentu finansowego.
12. Udawanie, że klient wygrał na loterii albo w kasynie.
13. Skomplikowana struktura właścicielska mająca na celu ukrycie, kto jest prawdziwym właścicielem przedsiębiorstwa.
14. Fałszywe przychody i zyski, których jednostka nigdy nie zrealizowała.
15. Wydawanie pieniędzy na luksusowe dobra lub na inne bardzo wysokie inwestycje.
16. Działalność typowa dla prania brudnych pieniędzy: bary, restauracje, kluby nocne, maszyny wendingowe, działalność hurtowa, handel nieruchomościami, bankomaty, gotówkę do banku wpłacają losowe osoby (kurierzy).

W zakresie depozytów systemy w instytucjach finansowych powinny być w stanie identyfikować następujące zachowania[44]:

1. Na rachunek są wpłacane lub wypłacane duże kwoty pieniężne.

---

oraz *The Specialist Property Law Regulator, Anti-money laundering red flags*, https://www.clc-uk.org/wp-content/uploads/2018/07/180710-AML-red-flags.pdf (dostęp: 11.09.2019).

[44] J. Leeuw, *Monitoring & Surveillance…*, op. cit.; K.M. Kingsly *Financial Crime Investigation…*, op. cit., s. 180.

2. Gotówka jest wpłacana w różnych oddziałach tego samego banku.
3. Używanie wpłatomatów dla depozytów.
4. Przedstawianie not bankierskich o podejrzanym wyglądzie.
5. Klient nagle podpisuje ogromny kontrakt, gdy zazwyczaj podpisywał małe kontrakty.
6. Używanie do zakupów czeków od osób trzecich.
7. Zakupy przekraczające przynajmniej pozornie możliwości finansowe właściciela rachunku.

W zakresie operacji gotówkowych systemy powinny posiadać zdolność wykrywania następujących działań[45]:

1. Wymiana małych nominałów na duże nominały.
2. Dzielenie transakcji na części, których wartość jest poniżej wartości, przy której występuje konieczność identyfikacji stron transakcji.
3. Rozliczanie transakcji bez użycia rachunku bankowego.

W zakresie transferów międzynarodowych[46] systemy powinny wyszukiwać transakcje i sytuacje obejmujące:

1. Nacisk klienta na szybkość transakcji bez zwracania uwagi na koszty.
2. Zniknięcie klienta po tym, jak bank zażądał dokumentacji lub dokumentacja jest niekompletna.
3. Transakcje są powiązane z rajami podatkowymi albo krajami o zagrożeniu terroryzmem.

W zakresie finansowania terroryzmu banki i organizacje poszukują następujących działań[47]:

1. Brak widocznych działań w celu zebrania środków deponowanych na rachunku bankowym, które jednak na niego trafiają (a klient jest bezrobotny albo ma bardzo niskie dochody).

---

[45] J. Leeuw, *Monitoring & Surveillance*…, op. cit.; K.M. Kingsly, *Financial Crime Investigation*…, op. cit., s. 190.

[46] J. Leeuw, *Monitoring & Surveillance*…, op. cit.; B. Peterson, *Red Flags and Black Markets: Trends in Financial Crime and the Global Banking Response*, „Journal of Strategic Security", 2013, 6 (5), nr 3, s. 298–308.

[47] J. Leeuw, *Monitoring & Surveillance*…, op. cit.; B. Peterson, *Red Flags and Black Markets*…, op. cit.; FATF Report, *Terrorist Financing Risk Assessment Guidance*, lipiec 2019, http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf (dostęp: 11.09.2019).

2. Brak ekonomicznego uzasadnienia transakcji albo adres klienta lub dane osobowe są nieprawdziwe, albo transakcje nie mają żadnego związku ze sposobem życia lub zarobkowania klienta (szczególnie korzystanie z sejfów).
3. Przelewy środków na rzecz organizacji charytatywnych znajdujących się w rajach podatkowych lub krajach, gdzie działają terroryści, szczególnie z wielu różnych rachunków bankowych.
4. Podejrzanie duża liczba transakcji w jednym oddziale banku lub przeciwnie – mała liczba transakcji, ale w wielu oddziałach tego samego banku.
5. Podejrzane i sprzeczne ze sobą adresy IP logowania do rachunku bankowego, wypłaty i wpłaty przez podejrzane osoby niedające się sprawdzić, kim są.
6. Opróżnianie rachunku za pomocą jednej wypłaty albo zmiany środków na rachunku sugerują sprzedaż całego majątku klienta banku (i ewentualnie zamianę na kryptowaluty), klient informuje bank o zamknięciu rachunku (albo klient spłaca nagle całe swoje zadłużenie albo zadłużenie innej firmy albo klienta).
7. Aktywność klienta online wskazuje na ekstremistyczne poglądy a wypłaty z konta sugerują podróże do krajów zagrożonych terroryzmem (i generalnie dużo wypłat z bankomatu poza granicami kraju, klient też dużo podróżuje),
8. Środki na koncie są wpłacane lub wypracowywane przez firmę, w której pracują osoby tego samego obcego obywatelstwa, szczególnie jeżeli są to kraje zagrożone lub wspierające terrorystów, osoby działające na rachunku mają ten sam adres lub telefon, a adres jest adresem firmy.
9. Wiele rachunków organizacji dobroczynnych i przedsiębiorstw przelewa pieniądze na zagraniczne rachunki kilku odbiorców.
10. Okresy braku transakcji, które mogą oznaczać okresy szkolenia lub walk terrorystycznych.

W zakresie walki z łapówkarstwem organizacje są zachęcane do tworzenia strategii i polityki antykorupcyjnej i każdy pracownik musi ją podpisać. Wiele uregulowanych lub zrzeszonych zawodów posiada swoje kody etyczne wymagające uczciwości oraz sądy wewnętrzne, jeżeli dojdzie do złamania tych zasad.

Jeżeli chodzi o oszustwa popełniane przez pracowników instytucji finansowych i przedsiębiorstw, system powinien identyfikować następujące aktywności[48]:

1. Osoby pracujące lub prywatnie współpracujące z inną firmą lub firmami (również z dostawcami lub podwykonawcami), nadmiernie z nimi powiązane.
2. Pracownicy chciwi na pieniądze, które są gotowi zarabiać za każdą cenę.
3. Pracownicy, którzy są nadmiernie powściągliwi w odniesieniu do wykonywanej pracy, nadmiernie zestresowani bez wyraźnej przyczyny.
4. Pracownicy reagujący agresywnie na próby kontroli ich pracy, próbują odwlec kontrolę, wypytują o jej zakres i cel albo o procedury i zasady, które nie mają związku z ich stanowiskiem.
5. Pracownicy udzielający różnych odpowiedzi na to samo pytanie zadane przez różne osoby.
6. Osoby o szerokim kręgu znajomych wśród osób w organizacji.
7. Pracownicy zajmujący kluczowe stanowiska posiadające bardzo dużą kontrolę, a także osoby, które przeszły przez wiele stanowisk w firmie, posiadają dużą wiedzę i doświadczenie pozwalające im dokonać oszustwa.
8. Pracownicy uzależnieni od zakupów, od silnych używek, usiłujący pożyczać pieniądze od innych, wielokrotnie pożyczający pieniądze, których często nie zwracają (z brakiem umiejętności kontrolowania własnych wydatków) i zwykle silnie zadłużeni, również osoby żyjące ponad stan.
9. Osoby pracujące do późnych godzin nocnych, kiedy nie ma już innych pracowników, co pozwala im na włamania do systemów firmy.
10. Pracownicy nadmiernie obciążeni pracą, które ze względu na stres mogą zmieniać swoje zachowanie, jak również odmawiający wykorzystania urlopu wypoczynkowego.
11. Pracownicy, którzy niedawno rozpoczęli pracę, a teraz z niej rezygnują, pracownik pracował sezonowo i teraz kończy kontrakt albo

[48] K.M. Kinsly, *Financial Crime Investigation…*, op. cit., s. 150 oraz B. Peterson, *Red Flags and Black Markets…*, op. cit., oraz DETECT Inc., *Red Flag Indicators of Fraud*, http://mcsip.org/wp-content/uploads/2016/11/MCSIP_Red_Flag_Indicators_of_Fraud.pdf (dostęp: 20.09.2019).

jest niezadowolony i sam już złożył rezygnację, pracownik zmieniał często miejsce pracy.

12. Skargi klientów na brakujące sprawozdania albo podejrzane transakcje, liczne reklamacje, skargi osób współpracujących z przedsiębiorstwem.
13. Rosnące bez powodu koszty, duża część płatności wykonywanych w gotówce, odnotowane nietypowe transakcje, brakuje dokumentów.
14. Słabe i niedopracowane procedury audytu wewnętrznego, brak skutecznej kontroli nad pracownikami, brak okresowej albo wyrywkowej kontroli uczciwości pracowników.

W zakresie przestępstw rynkowych systemy powinny być w stanie wykrywać następujące działania[49]:

1. W przypadku *insider tradingu* wystąpienie dużych transakcji przed ogłoszeniem ważnej informacji wpływające na cenę aktywów, a także transakcje, w efekcie których występują nagłe i gwałtowne zmiany cen akcji albo wolumenu zleceń, zanim pojawi się informacja o znacznym wpływie na cenę akcji.
2. W przypadku manipulacji rynkiem lista podejrzanych transakcji jest dłuższa i obejmuje:
   - transakcje wykonywane przez osoby mające znaczny wpływ na rynek, które oddziałują znacząco na cenę instrumentu finansowego;
   - duże transakcje stanowiące dużą część dziennego wolumenu, może to być seria transakcji jedna za drugą w określonym czasie danego dnia i której towarzyszyły albo zmiana ceny, albo zmienności, albo wolumenu;
   - transakcje bez ekonomicznego sensu, np. nie następuje przeniesienie własności albo wymiana jest na taki sam instrument finansowy albo bardzo podobny;
   - transakcje odwracające pozycję inwestora o dużej wartości, stanowiące dużą część dziennego wolumenu;
   - niezwykle rentowne transakcje, dużo powyżej średniej dla indeksów giełdowych;

[49] Zachowania te zostały opisane w zaleceniach ACER (ang. Agency for the Cooperation of Energy Regulators) jako wskazujące na zagrożenie insider tradingiem albo manipulowaniem rynku, https://acer.europa.eu/Official_documents/Other%20documents/4th%20Edition%20ACER%20Guidance%20REMIT%20-%204th%20Update.pdf (dostęp: 10.09.2019).

- transakcje wykonywane na sam koniec sesji albo w okresach, kiedy obliczane są indeksy giełdowe, albo poniżej przedziału cen w danym dniu (przy zakupie powyżej maksimum ceny przy sprzedaży poniżej minimum ceny);
- w tym samym czasie transakcja na walorze (długa albo krótka pozycja) i upublicznianie informacji, które mogą pchną ceny w korzystnym dla tego gracza kierunku.

4. Techniki śledztwa w przypadku przestępstw finansowych

Walka z przestępstwami finansowymi opiera się na następujących źródłach danych[50]: wywiadach ze świadkami i podejrzanymi, opiniach ekspertów, analizie poprzednich spraw, informacjach od informatorów, obserwacji fizycznych i wirtualnych miejsc, gdzie przestępcy się spotykają i gdzie realizowane są przestępstwa, analizie skonfiskowanych dokumentów, obserwacji (fizycznej i wirtualnej), niekiedy prowokacji, śledzeniu za pomocą kamer i innego sprzętu, podsłuchu i kontroli emaili, analizie fizycznych śladów typu odciski palców czy ślady biologiczne, analizie internetu, korzystaniu z policyjnych baz danych, informacjach od obywateli, roszczeniach ofiar oszustw, wymianie informacji z innymi instytucjami, informacjach z mediów, współpracy z organami nadzoru, bazach danych od firm i instytucji (udostępnianych na potrzeby śledztwa policji).

Na podstawie uzyskanych informacji tworzone są wzorce oszustw[51], które mogą pomóc znajdować miejsca kolejnych kradzieży (reguły zachowań[52]), trendy ewolucji danego oszustwa, powiązać je ze zmianami demograficznymi (stopa bezrobocia, poziom ubóstwa, inne), w końcu pozwalają dokładnie opisać, jak dane oszustwo działa i jakie elementy są z nim związane. Często dane oszustwo generuje określony rodzaj rynku na ukradzione aktywa – pieniądze trzeba wyprać i gdzieś schować, ktoś musi rozesłać e-maile phishingow, itd. Profilowanie pozwala także określić pewne cechy osobowe osób, które mogą

[50] P. Gottschalk, *Policing financial crime*, Brown Walker Press, Florida 2009, s. 136–140.
[51] Ibid.
[52] J. Leeuw, *Monitoring & Surveillance…*, op. cit.

popełnić dane przestępstwo, a także, jaką rolę poszczególne osoby odgrywają w grupie przestępców. Analiza zakończonych dochodzeń pozwala zidentyfikować błędy, ale także użyteczne działania i jak najlepiej i najszybciej daną sprawę w przyszłości doprowadzić do końca. Przypadki mogą być także porównywane ze sobą, aby znajdować podobieństwa między przestępstwami. Osoby nadzorujące poszukują także grup rachunków bankowych z podobną charakterystyką (ang. *peer-group*)[53].

Jeżeli dana transakcja zostanie zidentyfikowana jako podejrzana[54], wtedy dokonuje się analizy ryzyka, jakie niesie za sobą, każdym przypadkiem zarządza się w czasie rzeczywistym (coraz częściej podejrzane praktyki są identyfikowane w czasie rzeczywistym, czemu służą zautomatyzowane systemy nadzoru), stosuje się także narzędzia do zarządzania przepływem zadań (ang. *workflow management*), aby system automatycznie generował punkty kontrolne, zadania były zautomatyzowane oraz dokonywana była na bieżąco weryfikacja poprawności danych.

Przestępstwa finansowe, w zależności od ich rodzaju, mogą generować wokoło siebie cały rynek przestępczy[55], który obejmuje grupę przestępców działających razem, grupy konkurencyjne, klientów, dostawców, produkty konkurencyjne, poddostawców i podwykonawców. Aby skutecznie coś ukraść i skutecznie ukryć ukradziony majątek, trzeba pomocy i wiedzy wielu ekspertów. Na wypadek wykrycia potrzebni są zdolni prawnicy, doradcy, wsparcie finansowe (bo ukradzione środki i własny majątek mogą zostać zamrożone). Mogą być potrzebne sfałszowane dokumenty i karty. Na takim rynku potrzebna jest komunikacja, sposób rozliczeń finansowych, a także zabezpieczenia przed niepowołanymi osobami. Walka z przestępczością finansową to także poznawanie takich rynków i ich uczestników przez organy wymiaru sprawiedliwości i nadzoru[56]. Rynki te jednak rozwijają się jednak tak samo jak rynki legalne, np. w wyniku znoszenia barier przepływu kapitału i granic, a także w wyniku postępu technologicznego. Rynki z różnych krajów mogą obecnie tworzyć rynki ponadnarodowe, ale często w danym kraju występuje pewna specjalizacja (przynajmniej okresowa) na dany rodzaj przestępstw.

---

[53] Ibid.
[54] Ibid.
[55] P. Gottschalk, *Policing financial crime…*, op. cit., s. 144–145.
[56] Ibid.

Istotnym narzędziem walki z oszustwami finansowymi jest sprawna identyfikacja wszystkich szczegółów związanych z transakcją, w tym szczegółowych danych o osobach w nią zaangażowanych. W przypadku rachunków bankowych wymagane są przynajmniej następujące informacje: nazwa i adres klienta, numer identyfikacji podatkowej, jeżeli rachunek należy do firmy to dokumenty założycielskie, nazwa pod jaką dokonano rejestracji i wszystkie warianty tej nazwy, pełen opis, czym firma się zajmuje, referencje, dane osobowe dyrektorów i menedżerów. Banki powinny wysłać pracownika, aby ten sprawdził, czy firma działa pod adresem, który wskazała i czy podano prawdziwe dane, a także: zgromadzić sprawozdania finansowe firmy-klienta, badać powody brania pożyczek i kredytów, badać historię kredytową, sprawdzać możliwość spłaty kredytu, skontrolować, czy pożyczane środki są proporcjonalne do zasobów klienta[57].

5. Techniki walki z unikaniem podatków, uchylaniem się od opodatkowania i innymi formami nieprzestrzegania przepisów podatkowych

Do niedawna uwaga władz państwowych na świecie skupiona była głównie na wykrywaniu oszustw i karaniu podmiotów, obecnie zaś podejmowane są inicjatywy ukierunkowane na różne elementy, tj. wpływanie na postawy podatników i odczuwanie ryzyka wykrycia oszustwa, a także tworzenie zachęt do przestrzegania prawa. Stało się to zasadne, gdyż zauważono, że aby narzędzia prewencyjne były skuteczne, powinny być dostosowane do charakteru ucieczki od podatku. U podstaw zatem stosowanych współcześnie metod zapobiegających nieprawidłowościom leży koncepcja zakładająca klasyfikację ryzyka podatkowego. Jej filozofia sprowadza się do dostosowania narzędzi do rodzaju i rozmiarów nadużyć podatkowych, a także nieświadomie popełnianych błędów. Elementami o kluczowym znaczeniu w prowadzonej polityce jest bowiem nie tylko rozpoznanie i segmentacja ryzyka podatkowego, ale również podejmowanie ściśle określonych działań ukierunkowanych na jego minimalizację.

Stosowany przez kraje podstawowy model zarządzania ryzykiem podatkowym jest podobny, ale sposób wykorzystania narzędzi technicznych

[57] K.M. Kingsly, *Financial Crime Investigation…*, op. cit., s. 190.

i filozofia zarządzania są odmienne. Realizowane koncepcje różnią się także metodą identyfikowania i klasyfikowania ryzyka. Niektóre z nich skupiają się na indywidualnym podatniku i cechach związanych z prowadzoną przez niego działalnością[58]. Inne koncentrują się na konkretnych rodzajach błędów bądź segmentach podatników charakteryzujących się wysokim wskaźnikiem popełnianych błędów[59]. Typologia ryzyka podatkowego Komisji Europejskiej i OECD, a także Ministerstwa Finansów w Polsce, przedstawiona w tabeli 1, jest efektem strategii zarządzania ryzykiem podatkowym, propagowanej i realizowanej od co najmniej dekady[60].

Tabela 1. Mechanizmy zmniejszające dochody podatkowe w krajach UE i OECD – współczesne ujęcie

Obszary ryzyka podatkowego według Komisji Europejskiej i OECD
1. Ryzyko rejestracji (*register risk*) dotyczy podmiotów, które figurują we właściwym dla celów podatkowych rejestrze, ale nie mają do tego prawa. Są to np. podatnicy funkcjonujący w ramach karuzeli podatkowej, klasyczni oszuści podatkowi bądź podatnicy przestrzegający swoich obowiązków, którzy w wyniku błędu lub zaniedbania nie dokonują wyrejestrowania 2. Ryzyko to dotyczy także podmiotów, które powinny być zarejestrowane, lecz nie są. Obszar ten obejmuje działających w tzw. nieformalnej gospodarce
3. Ryzyko nieterminowego złożenia deklaracji (*filing risk*) – ryzyko, że wpływy podatkowe będą zaniżone z uwagi na brak zgłoszenia dochodów w określonym ustawowo terminie
4. Ryzyko płatności (*payment risk*) – ryzyko umniejszenia dochodów podatkowych o niezapłacone w terminie należne kwoty podatku
5. Ryzyko deklaracji (*declaration risk*) – ryzyko, że na wydajność podatku wpłyną, wykazane w deklaracji, nieprawidłowe kwoty wynikające z nieświadomego błędu podatnika bądź jego celowego działania
Katalog zachowań według Międzynarodowego Funduszu Walutowego
1. Przerzucanie dochodów za pomocą cen transferowych (*Transfer Mispricing*)
2. Przenoszenie własności patentu do kraju, w którym dochody są niżej opodatkowane (*Strategic Location of IP)*
3. Międzynarodowe przenoszenie długów (*International Debt Shifting*)

[58] W Wielkiej Brytanii segmentacja podmiotów opiera się na wysokości uzyskiwanych obrotów, złożoności spraw, profilu publicznym, rodzaju składanych zeznań podatkowych, posiadaniu osobowości prawnej lub jej braku. Duńskie władze fiskalne opierają się na koncepcji OECD. Natomiast, w Austrii podmioty kategoryzowane są według wysokości obrotów i liczby zatrudnianych pracowników, *Compliance Risk…*, op. cit., s. 19.

[59] *Pomarańczowa Księga. Zarządzanie ryzykiem – zasady i koncepcje*, Ministerstwo Skarbu JKM 2004. s. 7; *Compliance Risk…*, op. cit.; *Risk Management,* op. cit, s. 23; *Compliance Risk Management Guide for Tax Administrations*, Fiscalis Risk Management Platform Group, European Commission 2010, s. 97–104.

[60] *The Orange Book. Management of Risk – Principles and Concepts*, HM Treasury, London, 2004, s. 49; Compliance Risk, op. cit.; *Risk Management,* op. cit.

4. Wykorzystanie istniejących umów o unikaniu podwójnego opodatkowania do uzyskania korzyści finansowych w postaci zmniejszenia podatku zagranicznego (*Tax Treaty Shopping*)
5. Odraczanie podatku (*Tax Deferral*)
6. Zmiana siedziby firmy w celu zmniejszenia opodatkowania (*Corporate Inversions and HQ Location*)
Katalog zachowań według Ministerstwa Finansów w Polsce
1. Uczestnictwo podmiotów w transakcjach karuzelowych
2. Niewykazywanie do opodatkowania obrotu/przychodów z wystawionych rachunków/faktur VAT lub nieewidencjonowanie przychodów na kasach rejestrujących
3. Niewystawianie faktur lub wystawianie faktur w kwotach nieodpowiadających wielkościom faktycznym
4. Nieprawidłowe rozliczanie VAT w odniesieniu do nieściągalnych wierzytelności (tzw. ulga na „złe długi")
5. Zawyżanie kosztów uzyskania przychodów oraz podatku naliczonego związane z wykorzystaniem faktur, które nie dokumentują rzeczywistego przebiegu zdarzeń gospodarczych lub które dotyczą kosztów niestanowiących kosztów uzyskania przychodów
6. Nierealizowanie lub nieterminowe realizowanie obowiązków związanych z zapłatą podatku lub zaliczki na podatek
7. Niewywiązywanie się z obowiązku płatnika podatku dochodowego od osób fizycznych
8. Opodatkowanie sprzedaży usług według niewłaściwych stawek, w tym również poprzez błędne kwalifikowanie transakcji
9. Dokonywanie pozornych transakcji celem generowania fikcyjnych kosztów uzyskania przychodu oraz podatku naliczonego
10. Błędne stosowanie zryczałtowanej formy opodatkowania
11. Wykorzystywanie sieci podmiotów powiązanych do obniżenia zobowiązań podatkowych
12. Prowadzenie niezarejestrowanej działalności gospodarczej
Katalog zachowań opracowany przez Polski Instytut Ekonomiczny
1. Zawyżanie kosztów uzyskania przychodów poprzez dofinansowanie spółki przez wspólnika kapitałem dłużnym
2. Unikanie podwójnego opodatkowania poprzez wykorzystanie formy prawnej funduszu inwestycyjnego w połączeniu z transferami zagranicznymi
3. Zaniżanie dochodu do opodatkowania poprzez przenoszenie przychodów/kosztów między okresami podatkowymi
4. Rozliczanie podatków w korzystniejszej jurysdykcji poprzez zawyżanie cen produktów i usług nabywanych przez podmioty powiązane
5. Obniżanie dochodów do opodatkowania poprzez kreowanie straty, a także nabywanie spółek wykazujących straty oraz stosowanie niektórych instrumentów pochodnych
6. Obniżanie dochodu do opodatkowania poprzez sztuczne tworzenie podatkowych grup kapitałowych
7. Rejestrowanie spółek w miejscach nieuzasadnionych ekonomicznie, np. w rajach podatkowych
8. Sprzedaż towarów/usług bez paragonów i faktur
9. Zakładanie spółek zależnych w krajach związanych korzystną umową o unikaniu podwójnego opodatkowania
10. Transfer zysków poprzez sztuczne generowanie kosztów przez wykorzystanie wartości niematerialnych, fikcyjne zarządzanie założoną za granicą spółką kapitałową
11. Wykorzystanie zwolnienia podatkowego dywidend i podmiotów pośredniczących, w tym posiadających rezydencję podatkową w państwach o korzystnej jurysdykcji podatkowej, którym wypłacana jest dywidenda

Źródło: na podstawie: *Risk Management…*, op. cit.; *Compliance Risk Management: Managing and Improving Tax Compliance,* OECD Publishing, 2004; *Krajowy Plan Dyscypliny Podatkowej. Plan*

wdrożenia na 2005 r., Ministerstwo Finansów 2005; *Krajowy Plan Działań Administracji Podatkowej 2016 – główne założenia* oraz Załącznik nr 1 do Krajowego Planu Działań na 2016 r. – *Opis ryzyk związanych z podobszaramiryzyka*,http://mf-arch.mf.gov.pl/administracja-podatkowa/wiadomosci/aktualnosci/-/asset_publisher/2UWl/content/krajowy-plan-dzialan-administracji-podatkowej-2016-glowne-zalozenia/pop_up?_101_INSTANCE_2UWl_viewMode=print, dostęp: 12.07.2019; *Horyzont, op. cit.*, s. 13–14; S. Beer, R. Mooij, L. Liu, *International Corporate Tax Avoidance: A Review of the Channels, Magnitudes, and Blind Spots*, WP/w18/168, „IMW Working Papers" 2018.

Wymienione kanały ucieczki od podatku są jednakowe dla krajów Europy[61] i nie tylko, wiążą się ze wszystkimi podatkami centralnymi i dotyczą podmiotów o różnej wielkości, formie prawnej oraz zakresie działania. W stosunku do wytypowanych obszarów ryzyka stosuje się narzędzia prewencyjne i sankcyjne[62]. Z upływem czasu ciężar zwalczania ucieczki od podatku został dodatkowo przeniesiony na tworzenie warunków dla łatwiejszego wypełniania obowiązków podatkowych. Praktyka dowodzi, że cel ten osiągany jest poprzez świadczenie usług drogą elektroniczną[63], zachęcanie do współpracy[64],

[61] C.T. Czinege, *Risk management in order to enhance compliance of taxpayers in Hungary*, https://www.iota-tax.org/sites/default/files/documents/publications/IOTA_Papers/iota_paper_risk_analysis_in_hungary.pdf (dostęp: 8.8.2019); *Taxpayer Rating System in Latvia*, „Magazine of the Intra-European Organisation of Tax Administrations", 2019, z. 38, s. 21; I. Hansson, *Cash Sector initiatives in Swede*n, „Tax Tribune, Magazine of the Intra-European Organisationof Tax Administrations", 31th edition, 2014, s. 8.

[62] M. McKerchar, *Understanding and predicting taxpayers' behavioural responses to actions by tax administration*s, http://www.oecd.org/tax/administration/2789937.pdf (dostęp: 8.08.2019).

[63] W Danii, Francji i Niemczech wykorzystuje się mechanizm wstępnego wypełniania deklaracji i podkreśla się korzyści z tego płynące. Hiszpanie wykorzystują narzędzia SMS w dostarczaniu informacji podatnikowi. Dania i Hiszpania podejmują działania marketingowe w celu zwiększenia świadomości co do korzyści płynących z usług elektronicznych. Australia, Finlandia i Szwajcaria umożliwiają wydłużenie terminów jeśli podatnik wypełnia swoje obowiązki drogą elektroniczną. W Brazylii użytkownicy usług elektronicznych korzystają z możliwości szybszego otrzymania zwrotu podatku. W Chile, dla użytkowników usług elektronicznych przewidziana jest automatyczna redukcja kar i odsetek. W Kanadzie, Irlandii, Finlandii, Singapurze i Hiszpanii wprowadzono obowiązek korzystania z elektronicznych usług w zakresie np. podatku dochodowego oraz VAT dla wybranych grup podatników biznesowych. *Working smarter in structuring the administration, in compliance, and through legislation*, Information note, OECD Publishing 2012.

[64] W dokumencie OECD zatytułowanym „*Studia nad rolą pośrednictwa podatkowego*" przyznano, że istnieją możliwości dla nawiązania większej współpracy między podatnikami a organami podatkowymi, która pomaga w uzyskaniu wyższego poziomu dyscypliny podatkowej. Współpracę tę nazwano wzmocnieniem relacji (*enhanced relationship*) *Tax Compliance and Tax Accounting Systems*, Forum on Tax Administration, OECD 2010, s. 6; *Risk Management – Practice Note*, OECD Committee of Fiscal Affairs Forum on Strategic Management 1997, s. 7–8.

a także wykorzystywanie innych środków na rzecz ułatwienia przestrzegania prawa[65]. Od 2014 r. Agencja Podatkowa w Szwecji (*Swedish Tax Agency*, dalej STA) realizuje projekt zakupów testowych w Internecie w celu identyfikacji dostawców leków i narkotyków, a także graczy pokerowych, którzy nie deklarują dochodów do opodatkowania[66]. W kraju tym przez ostatnie 20 lat prowadzone są także bezpłatne wykłady na temat przepisów podatkowych dla nowo utworzonych firm oraz seminaria internetowe na żywo. Stosunkowo niedawno szwedzkie władze uruchomiły także podcast Szkoły podatkowej[67]. W Bułgarii zaś w 2012 r. został powołany zespół do spraw kontroli handlu elektronicznego, który koncentrował swe działania na nawiązaniu dobrych relacji z firmami kurierskimi. Do dziś wysyłane są oficjalne prośby do firm kurierskich o dostarczenie danych o zrealizowanych dostawach. W miejsce zespołu powstała obecnie wyspecjalizowana jednostka Departament „E-Audytu" w ramach struktur Krajowej Agencji Skarbowej (*National Revenue Agency*, dalej: NRA). Jednostka ta realizuje działania z zakresu: e-audytu, e-handlu, a w przyszłości także informatyki śledczej (*IT Forensic*)[68].

Z badania przeprowadzonego przez OECD wynika, że potencjał, który już wykorzystano, to restrukturyzacja administracji podatkowej. I tak np. Węgry zunifikowały dwie istniejące organizacje w jedną odpowiedzialną za pozyskiwanie wpływów z podatków, składek ubezpieczenia społecznego oraz opłat celnych. Restrukturyzacji dokonano także w Danii (w okresie 2005–2010), ale również w Niemczech czy we Francji w 2008 r.[69] W ten ogólnoświatowy

[65] Np. Loteria fakturowa w Portugalii, w Peru podatnicy przestrzegający przepisów są nagradzani rabatami podatkowymi i preferencyjnym traktowaniem. W Meksyku, podatnicy wypełniający swoje obowiązki podatkowego zgodnie z literą prawa są nagradzani otrzymując prezenty rzeczowe. W Argentynie, podatnicy otrzymują nagrody gotówkowe. P.B. Sousa, D.C. Wilks, J. Cruz, *Please give me an invoice": VAT evasion and the Portuguese tax lottery*, „International Journal of Sociology and Social Policy", 2019, nr 0144-3333x, s. 3.

[66] I. Berntsson, *The Swedish Approach To Identify Non-Filers On The Internet,* „Tax Tribune Magazine of the Inta-European Organisation of Tax Administrations", 35th edition 2016, s. 5–8.

[67] J. Persson, *The Swedish Tax School podcast*, „Tax Tribune Magazine of the Inta-European Organisation of Tax Administrations", 38th edition, 2019, s. 7.

[68] L. Timcheva, *Control Of E-Commerce In Bulgaria Courier Companies – Reliable Source Of Information On Cash On Delivery*, „Tax Tribune Magazine of the Intra-European Organization of Tax Administrations", 35th edition, 2016, s. 9–10.

[69] Aż 24 kraje przyznały restrukturyzacji największe znaczenie. A 53 kraje wskazały na przeprowadzone w tym celu inicjatywy. Tradycyjnie w wielu krajach organy podatkowe mają

trend wpisują się rozwiązania zaimplementowane do polskiego systemu prawnopodatkowego. Długookresowy i niezwykle kompleksowy proces stopniowych zmian w Polsce rozpoczął się w istocie w 2004 r.[70] i obejmuje[71] m.in.: wdrożenie koncepcji zarządzania ryzykiem i identyfikacji obszarów ryzyka podatkowego; konsolidację struktur administracji podatkowej; modernizację systemu informatycznego organów podatkowych i wykorzystanie analizy big data do identyfikacji nieprawidłowości (m.in. system OGNIVO, STIR, portal podatkowy[72]); rozwiązania ukierunkowane na zwalczanie uchylania się od podatku, a także działania wspierające dobrowolne wypełnianie obowiązków podatkowych (np. wstępnie wypełnione zeznanie, elektroniczna wysyłka deklaracji podatkowych, loteria paragonowa, obniżona stawka odsetek za zwłokę, list ostrzegawczy, objaśnienia podatkowe, opinie zabezpieczające, kampanie informacyjno-edukacyjne, a także powstanie instytucji Rzecznika Małych i Średnich Przedsiębiorców). Natomiast w odniesieniu do uchylania się od opodatkowania wprowadzono m.in. podwyższoną stawkę odsetek za zwłokę w zapłacie podatku, instytucję odpowiedzialności solidarnej, klauzulę przeciwko unikaniu opodatkowania i inne. Podobnie jak w Portugalii, Francji, Niemczech, Luksemburgu i Austrii podatnicy w Polsce zobowiązani są do składania Jednolitego Pliku Kontrolnego, odpowiednika *Standard Audit File for Tax* stworzonego przez OECD[73].

zdecentralizowaną strukturę. Tendencja zaś do centralizacji wpisuje się w rozwój technologii oraz realizację strategii zgodności (*compliance strategy*). Podkreśla się jednak, że fizyczna obecność organów podatkowych na szczeblu lokalnym jest nadal potrzebna, to jednak w znacznie mniejszym stopniu aniżeli dotychczas. *Working smarter…,* op. cit.

[70] W 2004 r. przyjęto do realizacji kilka strategii m. in. Strategię Zarządzania Ryzykiem Zewnętrznym, ale także Strategię Relacji z podatnikami, Strategię komunikacji i inne. *Strategia Zarządzania Ryzykiem Zewnętrznym. Polska Administracja Podatkowa*, Ministerstwo Finansów 2004, s. 54.

[71] *Działania…*, op. cit.

[72] OGNIVO – służy do poszukiwania rachunków bankowych dłużników. STIR – system teleinformatyczny izby rozliczeniowej umożliwiający monitoring i kontrolę operacji bankowych dokonywanych przez podmioty gospodarcze. *Działania…*, op. cit.

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.).

[73] *Guidance for the Standard Audit File – Tax*, Version 2.0:Appendix B: SAF-T Schema version 2.00, https://www.oecd.org/tax/administration/45167181.pdf (dostęp: 17.08.2019).

6. Metody ilościowe stosowane w wykrywaniu przestępstw finansowych

Metody ilościowe pozwalające na wykrywanie nadużyć finansowych zwykle bazują na klasyfikacji statystycznej. Jest to rodzaj zbioru technik i algorytmów statystycznych, które przydzielają obserwacje statystyczne do klas, bazując na atrybutach lub cechach tych obserwacji. Wśród aktualnie stosowanych metod oceny i identyfikacji przestępstw finansowych można wyróżnić sieci neuronowe, modele logitowe, metody wektorów nośnych, drzewa decyzyjne i losowe CART, algorytmy genetyczne, przeszukiwanie danych (data-mining) i tekstów (text-mining). Nowe metody obejmują grupy algorytmów zbiorowych operacji na danych, metodę powierzchni odpowiedzi, samoorganizujące się mapy, sztuczną inteligencję i uczenie głębokie, sieci bayesowskie i metody hybrydowe. Podsumowanie ograniczeń i mocnych stron każdej metody zawarto w tabeli 2.

Tabela 2. Mocne i słabe strony metod wykrywania przestępstw finansowych opartych na klasyfikacji statystycznej

Metoda	Zalety	Wady
Sieci neuronowe	Przydatna w przypadku niealgorytmicznych problemów z klasyfikacją binarną	Wymaga dużej mocy obliczeniowej do treningu i obsługi, nieodpowiednie do działania w czasie rzeczywistym. Nie są odporne na przeuczenie, dlatego wymagają ciągłego trenowania w celu dostosowania się do nowych metod oszustwa
Regresja logistyczna	Łatwa w implementacji	Niższa wydajność klasyfikacji niż inne metody eksploracji danych, trudność ze złożonością wykrywania oszustw
Wektory nośne	Wymagają niskiej mocy obliczeniowej, co daje potencjał do działania w czasie rzeczywistym	Trudno jest interpretować wyniki z powodu transformacji zestawu danych wejściowych
Drzewa i lasy decyzyjne	Łatwe w implementacji, wymagają niskiej mocy obliczeniowej, co daje potencjał do działania w czasie rzeczywistym	Wrażliwe na przeuczenie.
Algorytmy genetyczne	Łatwe w implementacji w przypadku niealgorytmicznych problemów z klasyfikacją binarną	Początkowa optymalizacja wymaga dużej mocy obliczeniowej
Text-mining/data-mining	Wykrywanie nadużyć na podstawie analizy tekstów sprawozdań finansowych	Subiektywny sposób klasyfikacji danych tekstowych. Konieczne jest zbudowanie właściwego słownika uwzględniającego zmianę znaczenia semantycznego

Metoda	Zalety	Wady
Metoda powierzchni reakcji	Proste w implementacji. Nadają się do nieliniowych problemów klasyfikacyjnych jak wykrywanie nadużyć w sprawozdaniach finansowych	Brak możliwości pełnej automatyzacji. Wymaga ingerencji audytora/walidatora
Samoorganizujące się mapy	Łatwość implementacji, przejrzysta wizualizacja danych	Wymaga zrozumienia rodzaju anomalii rynkowej
Sieci bayesowskie	Duża szybkość i efektywność obliczeniowa	Problem z klasyfikacją danych zaszumionych
Metody hybrydowe	Łączą zalety innych metod, łatwe w adaptacji do nowych rodzajów przestępstw	Brak możliwości zweryfikowania jakości wyników klasyfikacji ze względu na łączenie różnych pojęć

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

7. Skuteczność metod wykrywania oszustw i przestępstw finansowych

Jak wskazują wyniki badań KPMG z 2016 r.[74], w 24% przypadków nieprawidłowości wykryto na skutek skargi lub donosu innego niż gorąca linia. W 22% w czasie oceny pracy menedżerów, w 20% w wyniku zgłoszeń whistleblowerów, w 14% było to wynikiem przypadku, w 10% nieprawidłowości wykryli zwierzchnicy oszustów, w 7% zadziałała kontrola wewnętrzna, w 6% audyt wewnętrzny, w 3% było to zgłoszenie przez samego sprawcę i w kolejnych 3% analitycy rynkowi specjalizujący się w wykrywaniu takich nieprawidłowości[75].

Większość sprawców wykazywała przynajmniej jedno z zachowań wskazujących na ryzyko popełnienia oszustwa: nadmiernie kontrolowała podwładnych, zbyt bliskie relacje z dostawcami lub klientami, żyli na stopie przekraczającej ich możliwości finansowe, zachowanie wskazywało na problemy finansowe lub problemy rodzinne lub rozwód, ich zachowanie było oceniane jako kombinator[76]. Z raportu ACFE (ang. *Association of Certified Fraud Examiners*) z 2018 r.[77] wynika dodatkowo, że podstawowym powodem

[74] KPMG, *Profile of a fraudster*, 2016, KPMG.
[75] Ibid.
[76] Ibid.
[77] ACFE, *Report to the nations*, https://www.acfe.com/report-to-the-nations/2018/ (dostęp: 20.09.2019).

nieprawidłowości był brak kontroli lub możliwość ręcznego przejęcia nadzoru (obejścia kontroli wewnętrznej).

Systemy, które okazały się najskuteczniejsze w wykrywaniu i zapobieganiu, obejmowały: zarządzanie ryzykiem oszustwa, zgodne z prawem usługi lokalizacyjne, stosowanie technik kryminalistycznych i z zakresu cyberbezpieczeństwa, analizę danych, komercyjne usługi zewnętrzne związane z oceną ryzyka i jego zarządzaniem, *corporate intelligence*, dochodzenie w wykrytych sprawach, *whistleblowing*[78], a także programy wsparcia dla pracowników, niespodziewane audyty, obowiązkową rotacjęstanowisk, kodeks wymaganego zachowania[79].

Bibliografia

ACER, *Guidance on the application of Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency*, 4th Edition, https://acer.europa.eu/Official_documents/Other%20documents/4th%20Edition%20ACER%20Guidance%20REMIT%20-%204th%20Update.pdf

ACFE, *Report to the nations*, https://www.acfe.com/report-to-the-nations/2018/ (dostęp: 20.09.2019).

Beer S., Mooij R., Liu L., *International Corporate Tax Avoidance: A Review of the Channels, Magnitudes, and Blind Spots*, WP/w18/168, „IMW Working Papers" 2018.

Berntsson I., *The Swedish Approach To Identify Non-Filers On The Internet*, „Tax Tribune Magazine of the Inta-European Organisation of Tax Administrations", 35th edition 2016.

Compliance Risk Management: Managing and Improving Tax Compliance, OECD Publishing 2004.

Compliance Risk Management Guide for Tax Administrations, Fiscalis Risk Management Platform Group, European Commission 2010.

Czinege C.T., *Risk management in order to enhance compliance of taxpayers in Hungary*, https://www.iota-tax.org/sites/default/files/documents/publications/IOTA_Papers/iota_paper_risk_analysis_in_hungary.pdf, (dostęp: 8.8.2019).

DETECT Inc., *Red Flag Indicators of Fraud*, http://mcsip.org/wp-content/uploads/2016/11/MCSIP_Red_Flag_Indicators_of_Fraud.pdf

[78] KPMG, *Profile of a fraudster…*, op. cit.

[79] ACFE, *Report to the nations…*, op. cit.

Eren O., Depew B., Barnes S., *Test-based promotion policies, dropping out, and juvenile crime*, „Journal of Public Economics", 2017, nr 153, s. 9–31.

FATF Report, *Terrorist Financing Risk Assessment Guidance*, lipiec 2019, http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf (dostęp: 11.09.2019).

Gallaher M.P., Link A.N., Rowe B.R., *Cyber Security: Economic. Strategies and Public Policy Alternatives*, Cheltenham, Northampton 2008.

Górniok O., *Przestępczość gospodarcza i jej zwalczanie*, Wydawnictwo Naukowe PWN, Warszawa 1994.

Gottschalk P., *Policing financial crime*, Brown Walker Press, Floryda, 2009.

Guidance for the Standard Audit File – Tax, https://www.oecd.org/tax/administration/45167181.pdf (dostęp 8.08.2019).

Hansen I.I., *Corporate financial crime: social diagnosis and treatment*, „Journal of Financial Crime", 2009, nr 16, s. 28–40.

Hansson I., *Cash Sector initiatives in Sweden*, „Tax Tribune, Magazine of the Intra-European Organisation of Tax Administrations", 31th edition 2014.

Hardouin P., *Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing*, "Journal of Financial Crime", 2009, nr 16 (3), s. 199–209.

Horyzont optymalizacji – geneza, skala i struktura luki w podatku CIT, Polski Instytut Ekonomiczny 2019.

Kingsly K.M., *Financial Crime Investigation*, Christian Faith Publishing, Inc., New York.

Kojder A., *Korupcja i poczucie moralne Polaków*, w: *Kondycja moralna społeczeństwa polskiego*, red. J. Mariański, Wydawnictwo WAM, Kraków 2002, s. 233–252.

KPMG, *Profile of a fraudster*, 2016, KPMG.

Krajowy Plan Działań Administracji Podatkowej 2016 – główne założenia oraz Załącznik nr 1 do Krajowego Planu Działań na 2016 r. – Opis ryzyk związanych z podobszarami ryzyka, http://mf-arch.mf.gov.pl/administracja-podatkowa/wiadomosci/aktualnosci/-/asset_publisher/2UWl/content/krajowy-plan-dzialan-administracji-podatkowej-2016-glowne-zalozenia/pop_up?_101_INSTANCE_2UWl_viewMode=print

Krajowy Plan Dyscypliny Podatkowej. Plan wdrożenia na 2005 r., Departament Organizacji Skarbowości, Ministerstwo Finansów 2005.

Ksenia G., *Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective?*, „Journal of Financial Crime", 2008, nr 15 (2), s. 223–233.

Kubiczek A., *Przestępczość gospodarcza – czy można ją ograniczyć?,* „Nierówności społeczne a wzrost gospodarczy", 2015, nr 2 (42), s. 276.

Laudon K., *Management information systems: managing the digital firm*, Prentice Hall, New York 2010.

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

McKerchar M., *Understanding and predicting taxpayers' behavioural responses to actions by tax administrations*, http://www.oecd.org/tax/administration/2789937.pdf (dostęp: 8.08.2019).

Nelen H., Lankhorst F., *Facilitating organized crime: the role of lawyers and notaries*, w: D. Siegel, H. Nelen (eds), *Organized crime: Culture, Markets and Policies*, Springer, New York 2008, s. 127–142.

Pasternak-Malicka M., *Mentalność i moralność podatkowa a reakcje gospodarstw domowych na obowiązek podatkowy*, „Modern Management Review", 2013, nr 18 (20).

Persson J., *The Swedish Tax School podcast*, „Tax Tribune Magazine of the Intra-European Organisation of Tax Administrations", 38th edition 2019.

Peterson B., *Red Flags and Black Markets: Trends in Financial Crime and the Global Banking. Pomarańczowa Księga. Zarządzanie ryzykiem – zasady i koncepcje*, Ministerstwo Skarbu JKM 2004. s. 7.

Response, „Journal of Strategic Security", 2013, 6 (5), nr 3, s. 298–308.

Risk Management Guide for Tax Administrations, Fiscalis Risk Analysis Project Group, FPG/11, European Commission Directorate General Taxation and Customs Union 2006.

Risk Management–Practice Note, OECD Committee of Fiscal Affairs Forum on Strategic Management 1997.

Rogowski W., *Whistleblowing czyli czego się nie robi dla pozyskania zaufania inwestorów*, „Przegląd Corporate Governance", 2007, 2(10), https://www.pikw.pl/files/10/public/whistleblower/PCG_2_10_2007_Rogowski_Whistleblowing.pdf (dostęp: 1.09.2019).

Solska J., *Polacy coraz bardziej tolerancyjni wobec finansowych przekrętów*, „Polityka", 22.08.2019, https://www.polityka.pl/tygodnikpolityka/rynek/1716548,1,polacy-coraz-bardziej-tolerancyjni-wobec-finansowych-przekretow.read (dostęp: 1.09.2019).

Sousa P.B., Wilks D.C., Cruz J., *Please give me an invoice": VAT evasion and the Portuguese tax lottery*, „International Journal of Sociology and Social Policy" 2019, nr 0144-3333x, s. 3.

Strategia Zarządzania Ryzykiem Zewnętrznym. Polska Administracja Podatkowa, Ministerstwo Finansów 2004.*Tax Compliance and Tax Accounting Systems*, Forum on Tax Administration, OECD 2010, s. 6

Taxpayer Rating System in Latvia, „Tax Tribune. Magazine of the Intra-European Organisation of Tax Administrations", 2019, z. 38, s. 21.

The Orange Book. Management of Risk – Principles and Concepts, HM Treasury, London 2004.

The Specialist Property Law Regulator, *Anti-money laundering red flags*, https://www.clc-uk.org/wp-content/uploads/2018/07/180710-AML-red-flags.pdf (dostęp: 11.09.2019).

Timcheva L., *Control Of E-Commerce In Bulgaria Courier Companies – Reliable Source Of Information On Cash On Delivery*, „Tax Tribune Magazine of the Intra-European Organization of Tax Administrations", 35th edition 2016.

Trubarska J., *System antyterrorystyczny w Polsce – wybrane zagadnienia*, „Zeszyty Naukowe AON", 2016, nr 4 (105), s. 153–166.

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.).

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

Winiarska K. (red.), *Zakres zastosowań audytu wewnętrznego*, w: *Audyt wewnętrzny. Teoria i zastosowanie*, Difin, Warszawa 2017, s. 137–159.

Working smarter in structuring the administration, in compliance, and through legislation, Information note, OECD Publishing 2012.

Załącznik nr 1 do Krajowego Planu Działań na 2016 r. – *Opis ryzyk związanych z podobszaramiryzyka*, http://mf-arch.mf.gov.pl/administracja-podatkowa/wiadomosci/aktualnosci/-/asset_publisher/2UWl/content/krajowy-plan-dzialan-administracji-podatkowej-2016-glowne-zalozenia/pop_up?_101_INSTANCE_2UWl_viewMode=print (dostęp: 12.07.2019).

ROZDZIAŁ III

Zapobieganie kradzieży energii elektrycznej

ŁUKASZ WOJCIESZAK[1]

1. Wprowadzenie

Kradzież energii, najczęściej elektrycznej, stanowi niewątpliwie istotny problem, z którym starają się walczyć prawodawstwa różnych państw, w tym także Polski. Ponoszone przez dostawców energii straty pokrywane są przez obciążenie odpowiednią opłatą wszystkich odbiorców, co budzi ich zrozumiały sprzeciw i motywuje do wdrożenia skutecznych sposobów zapobiegania tego rodzaju czynom.

Istnieje wiele sposobów nielegalnego poboru energii, a zarazem można wskazać liczne środki mogące prowadzić do ograniczenia przestępczej działalności w tej dziedzinie, co jest zasadniczym celem tej pracy. Warto zaznaczyć, że kradzież energii elektrycznej pociąga za sobą konsekwencje o charakterze zarówno karnoprawnym, jak i cywilnoprawnym, choć w niniejszym opracowaniu zostały ukazane te pierwsze.

W pracy przedstawione zostały podstawy prawne kradzieży energii elektrycznej, specyfika tego rodzaju działalności, problematyka kontroli sposobu pobierania energii przez odbiorcę oraz sposoby zapobiegania istniejącemu zagrożeniu związanemu z popełnianiem tego rodzaju przestępstw. W odniesieniu do ukazanego problemu należy zadać pytanie o sposoby zapobiegania kradzieży energii elektrycznej, zwłaszcza o regulacje dotyczące kontroli oraz o metody zwalczania ubóstwa energetycznego, mogącego skutkować

[1] Doktor habilitowany nauk społecznych oraz doktor nauk prawnych. Profesor na Politechnice Świętokrzyskiej w Kielcach. Autor kilku książek oraz kilkudziesięciu artykułów naukowych. Główne zainteresowania badawcze: bezpieczeństwo energetyczne, prawo energetyczne, polityka wschodnia Polski i Unii Europejskiej.

ograniczeniem nielegalnego poboru energii. Osobny problem stanowi także kwestia wpływu wymiaru przewidzianych prawem kar na dokonywanie tytułowych przestępstw.

W opracowaniu zamieszczono najważniejsze kwestie dotyczące tytułowego zagadnienia, wskazując ich specyfikę na gruncie polskiego prawa i w realiach Polski. W opracowaniu została wykorzystana metoda językowo-logiczna typowa dla dogmatyki prawa. Zastosowanie znajduje też w pewnym stopniu również metoda socjologiczna, pomocna w ustaleniu, w jakim stopniu istniejące rozwiązania normatywne mogą okazać się skuteczne dla ograniczenia kradzieży energii elektrycznej.

2. Podstawy prawne kradzieży energii elektrycznej

Sposoby zachowań godzących w interesy przedsiębiorstw energetycznych można podzielić na dwie grupy:

a) nielegalny pobór niezwiązany z uprzednim zawarciem przez sprawcę umowy sprzedaży energii z przedsiębiorstwem energetycznym (podstawą odpowiedzialności karnej może być wówczas art. 278 § 5 k.k. regulujący przestępstwo kradzieży energii) oraz
b) nielegalny pobór energii funkcjonalnie powiązany z umową zawartą wcześniej z zakładem energetycznym (podstawą odpowiedzialności karnej może być albo wspomniany art. 278 § 5 k.k. albo określone w art. 286 k.k. przestępstwo oszustwa)[2].

W drugiej dekadzie XXI w. wykrywa się ponad 35 tys. nielegalnych pobrań, jednak trudno stwierdzić, jaka jest ich faktyczna liczba. Najczęstszym rodzajem kradzieży energii elektrycznej jest ingerencja dokonana w układ pomiarowo-rozliczeniowy (liczniki, instalacje elektryczne). W praktyce mają miejsca podłączenia do oświetlenia klatki schodowej, zatrzymanie tarczy licznika, podłączanie się do słupa energetycznego, odłączenie przewodu „N" i przykładanie magnesów neodymowych do inteligentnych liczników[3]. Za kradzież

[2] P. Kardas, *Przedsiębiorstwo energetyczne jako pokrzywdzony*, w: A. Walaszek-Pyzioł (red.), *Interdyscyplinarne problemy nielegalnego poboru energii*, Warszawa 2016, s. 242.

[3] *Co grozi za kradzież prądu?*, Enerad.pl, 25.05.2017, https://enerad.pl/aktualnosci/co-grozi-za-kradziez-pradu (dostęp: 21.08.2019). Kwestią sporną jest zasadność uznania kradzieży energii jako kradzieży z włamaniem, co zostanie ukazane w dalszej części opracowania.

energii uznaje się zatem wszelkie formy zachowania prowadzące do uzyskania dostępu do energii oraz możliwości jej wykorzystywania bez konieczności ponoszenia określonych prawem opłat[4].

Kradzież energii uregulowana została w rozdziale XXXV k.k. zawierającego przestępstwa przeciwko mieniu. Według art. 278 § 1 k.k. sprawca takiego czynu podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Przepisy dotyczące przestępstw związanych z kradzieżą rzeczy ruchomej stosowane są odpowiednio do kradzieży energii, co zawarte jest w § 5 tego artykułu. Warto zaznaczyć, że należy ten proceder zaliczyć do czynów przepołowionych, gdyż to przestępstwo ma swój odpowiednik w kodeksie wykroczeń – występkowi określonemu w art. 278 § 1 k.k. odpowiada wykroczenie określone w art. 119 § 1 k.w. Na podstawie tego przepisu skazany zostanie sprawca kradzieży mienia o wartości nie przekraczającej 500 zł[5]. Nowelizacja Kodeksu wykroczeń miała miejsce w 2018 r., wyznaczając próg, od którego kradzież przestaje już być wykroczeniem, stając się przestępstwem.

Kradzież energii elektrycznej jest możliwa przez dokonanie nieuprawnionego podłączenia kabla do kabla. Dopuszczenie się kradzieży energii elektrycznej w inny sposób nie jest *de facto* możliwe, gdyż nie są znane inne, np. bezprzewodowe, sposoby jej przesyłu. Istotny problem stanowi przy tym określenie, czy takie przestępstwo stanowi zwykłą kradzież, z powodu której sprawca mógłby ponosić odpowiedzialność w zależności od wartości zagarniętej energii albo na podstawie art. 278 § 1 i 5 k.k., albo na podstawie art. 119 k.w., czy też jest kradzieżą z włamaniem (art. 279 § 1 k.k.)[6]. Zdaniem Zygmunta Kukuły, chociaż pojęcie włamania rozumiane jest szeroko, to jednak do jego istoty należy wdarcie się do zamkniętego pomieszczenia i stąd nie może być mowy o kradzieży z włamaniem w wypadkach, gdy przedmiot wykonawczy jest położony wśród wolnej i nieograniczonej przestrzeni, a zarazem nie tworzy sobą zamkniętego, zabezpieczonego przed zaborem

[4] P. Kardas, *Przedsiębiorstwo energetyczne jako pokrzywdzony*…, op. cit., s. 247.

[5] J. Kędzierski, *Kradzieże prądu sprawiają problemy sądom*, „Rzeczpospolita", 30.11.2012, https://www.rp.pl/artykul/957109-Kradzieze-pradu-sprawiaja-problemy-sadom.html (dostęp: 25.09.2019). Co ważne, w myśl art. 130 kw, nie są czynami przepołowionymi inne przypadki kradzieży, takie jak kradzież broni, amunicji oraz materiałów i przyrządów wybuchowych, a ponadto rozbój i kradzież z włamaniem, a wymienione czyny zawsze są przestępstwami bez względu na wartość zagarniętego mienia, ibid.

[6] Ibid.

pomieszczenia[7]. Według Jacka Kędzierskiego kradzież energii elektrycznej z włamaniem musi polegać tylko na pokonaniu trwałego zabezpieczenia i niekoniecznie musi to być wtargnięcie do pomieszczenia zamkniętego, lokalu z instalacją elektryczną, lecz może też nastąpić poprzez np. otwarcie skrzynki z bezpiecznikami lub licznikiem, lub też otwarcie tzw. rozetki i podłączenie tam przewodu elektrycznego. Należy zgodzić się z poglądem, że przecięcie kabla podtynkowego, a następnie podłączenie z użyciem rozetki również będzie kradzieżą prądu z włamaniem[8].

Kwestia nielegalnego pobierania energii została zdefiniowana w ustawie – Prawo energetyczne. Według art. 3 pkt 18 tej ustawy jest to pobieranie energii bez zawarcia umowy, z całkowitym albo częściowym pominięciem układu pomiarowo-rozliczeniowego lub poprzez ingerencję w ten układ mającą wpływ na zafałszowanie pomiarów dokonywanych przez układ pomiarowo-rozliczeniowy[9]. Ponadto według art. 57. ust. 1 wspomnianej ustawy w razie nielegalnego pobierania paliw lub energii przedsiębiorstwo energetyczne może:

1) pobierać od odbiorcy, a w przypadku, gdy pobór paliw lub energii nastąpił bez zawarcia umowy, może pobierać od osoby lub osób nielegalnie pobierających paliwa lub energię opłatę w wysokości określonej w taryfie, chyba że nielegalne pobieranie paliw lub energii wynikało z wyłącznej winy osoby trzeciej, za którą odbiorca nie ponosi odpowiedzialności albo
2) dochodzić odszkodowania na zasadach ogólnych[10].

Warto zaznaczyć, ze w 2014 r. Trybunał Konstytucyjny podtrzymał w mocy rygorystyczne przepisy dotyczące kradzieży prądu. Kodeks karny kradzież energii elektrycznej traktuje jako przestępstwo, za którego popełnienie grozi

---

[7] Z. Kukuła, *Przestępstwo kradzieży energii – kontrowersje interpretacyjne*, „Wojskowy Przegląd Prawniczy" 2015, nr 3, https://pk.gov.pl/wp-content/uploads/2016/06/8df84ef7b5a-5e34e10415e1989774776.pdf (dostęp: 26.09.2019).

[8] J. Kędzierski, *Kradzieże prądu…* Ponadto odkręcenie żarówki z punktu świetlnego na korytarzu w budynku wielomieszkaniowym oraz wkręcenie w jej miejsce tzw. „złodziejki" umożliwiającej włożenie wtyczki z przewodem przeprowadzonym do lokalu mieszkalnego nie wyczerpuje znamion włamania. Jest tak, gdyż brak tu usunięcia trwałej przeszkody, zaś żarówka nie może być traktowana jako ta trwała przeszkoda i stałe zabezpieczenie przed dostępem energii elektrycznej. Nawet w przypadku odkręcenia przez sprawcę oprawki i uzyskania dostępu do przewodów i podłączenia do nich tych, które zostały przeprowadzone do mieszkania, nie byłaby to kradzież z włamaniem, lecz zwykła kradzież, ibid.

[9] *Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 2012 poz. 1059 z późn. zm.).*

[10] Ibid.

kara pozbawienia wolności do lat pięciu. Ustawa – Prawo energetyczne przewiduje nałożenie na sprawcę kradzieży kary w wysokości pięciokrotności wartości energii możliwej do zużycia, w związku z czym jeden z warszawskich sądów uznał, że jest to podwójne karanie za to samo przewinienie, a w dodatku sankcja finansowa jest nadmiernie represyjna. Trybunał Konstytucyjny nie podzielił jednak tych wątpliwości, uznając, że państwo karze za przestępstwo, natomiast wysoka opłata ma charakter cywilno-prawny i nalicza ją podmiot gospodarczy, a nie państwo. Dlatego też obie te kary można nadal stosować[11]. Według orzeczenia Trybunału Konstytucyjnego za kradzież energii elektrycznej można zostać ukaranym również na podstawie Kodeksu cywilnego, który podmiotowi okradzionemu otwiera drogę do uzyskania rekompensaty finansowej ustalanej na podstawie szacowanej skali kradzieży oraz prawa szczegółowego[12].

3. Wybrane aspekty związane z kradzieżą energii elektrycznej

Przez lata poważny problem stanowiła trudność ze wskazaniem odbiorcy, który dokonuje kradzieży energii elektrycznej. Dyskusyjne jest to, czy metodę wykrywania nielegalnego poboru (zastosowanego algorytmu postępowania) można uznać za swoiste know-how przedsiębiorstwa[13]. Zdaniem Eweliny Milan krąg osób odpowiedzialnych na podstawie Kodeksu karnego nie do końca pokrywa się z kręgiem osób, na które może być nałożona opłata z prawa energetycznego. W świetle ustawy – Prawo energetyczne odpowiedzialnością z tytułu nielegalnego pobierania energii może być objęty odbiorca nawet w sytuacji, gdy nielegalnego poboru energii dokonał nie on sam, ale osoba wykonująca na jego zlecenie i w jego lokalu określone czynności. W przypadku przestępstwa kradzieży odpowiedzialnością obarczony może być zaś tylko sprawca[14].

---

[11] *Surowe kary za kradzież prądu*, Dziennikpolski24.pl, 22.10.2014, https://dziennikpolski24.pl/surowe-kary-za-kradziez-pradu/ar/3617703 (dostęp: 26.08.2019).

[12] *Co grozi za kradzież prądu…*, op. cit.

[13] K. Billewicz, *Analityczne metody wykrywania kradzieży energii elektrycznej*, „Energetyka" – luty 2006, https://www.cire.pl/pliki/2/wykrywanie_kradziezy.pdf (dostęp: 22.08.2019).

[14] M. Kryszkiewicz, *Za kradzież prądu o jedną karę za dużo*, Gazetaprawna.pl, 12.02.2014, https://prawo.gazetaprawna.pl/artykuly/777251,za-kradziez-pradu-o-jedna-kare-za-duzo.html (dostęp: 4.09.2019).

Zjawisko nielegalnego pobierania energii elektrycznej wzmaga się zwłaszcza wówczas, gdy jej odbiorcy mają, wskutek istniejącej sytuacji ekonomicznej, gorsze warunki materialne swojej egzystencji. Zaprzestanie płacenia za pobraną energię, jak również pobieranie ich w sposób nielegalny, może oznaczać, że osoba, która tego dokonuje, znajduje się w skrajnie trudnym położeniu ekonomicznym. W związku z tym osoba taka jest nader często niewypłacalna, co stawia przedsiębiorstwo energetyczne na słabej pozycji w zakresie możliwości zrekompensowania straty poniesionej wskutek nielegalnego poboru (pomimo korzystnego rozstrzygnięcia sądowego windykacja okazuje się wręcz niemożliwa). Stąd też za sukces przedsiębiorstwa można uznać już sam fakt likwidacji nielegalnego poboru energii. Nielegalnego pobierania energii dopuszczają się niekiedy osoby majętne, które prowadzą działalność gospodarczą i swoje postępowanie motywują chęcią zmniejszenia nadmiernych kosztów generowanych zużywaniem energii elektrycznej. Inną grupą osób dokonujących nielegalnego poboru są ci, którzy zostali do takiej działalności nakłonieni przez nieuczciwych pracowników przedsiębiorstw energetycznych mających na celu oszukiwanie swoich pracodawców z chęci zysku[15].

Warte odnotowania jest zmniejszenie się poziomu ubóstwa energetycznego, do czego przyczyniło się m.in. wdrażanie licznych programów społecznych. Z raportu Instytutu Badań Strukturalnych pt. „Ubóstwo energetyczne 2012–2016" wynika, że odsetek osób ubogich energetycznie spada: obniżył się z on z 14,4% w 2012 r. do poziomu 12,2% w 2016 r. Oznacza to, że w tym okresie poprawiły się warunki życia prawie 880 tys. osób. W raporcie podkreślono, iż w tej grupie były głównie osoby, u których stwierdzono poprawę sytuacji dochodowej, największy zaś spadek rok do roku wystąpił pomiędzy 2015 a 2016 rokiem, co można wiązać z wprowadzeniem programu Rodzina 500 plus[16]. Można założyć, że znaczące ograniczenie skrajnego ubóstwa wpłynie zapewne na ograniczenie rozmiarów kradzieży energii elektrycznej.

Osobny problem stanowi kwestia odszkodowań za sprzeczny z prawem pobór energii. Zryczałtowane odszkodowanie z prawa energetycznego może

---

[15] A. Stankiewicz, M. Balwicka-Szczyrba, *Nielegalne pobieranie paliw lub energii. Aspekty prawne i zasady postępowania*, Gdańsk, wrzesień 2013, s. 7.

[16] P. Bednarz, *Miliony Polaków mają problem z ogrzaniem swoich domów. 500 plus poprawia jednak sytuację*, businessinsider.com.pl, 31.01.2018, https://businessinsider.com.pl/twoje-pieniadze/ubostwo-energetyczne-w-polsce-na-czym-polega/d8rdmnn (dostęp: 7.09.2019).

być wyższe od faktycznej szkody i ma funkcje represyjną oraz odstraszającą, ale podobna sytuacja dotyczy np. kary umownej z Kodeksu cywilnego. Tymczasem zdaniem sądu rejonowego rozpatrującego sprawę rozważania o cywilnoprawnym charakterze opłaty są w pełni uzasadnione tylko w przypadku, „gdy nielegalny pobór polega na poborze przez odbiorcę, który zawarł umowę z dostawcą, ale dokonuje poboru z całkowitym albo częściowym pominięciem układu pomiarowo-rozliczeniowego lub poprzez ingerencję w ten układ mającą wpływ na zafałszowanie pomiarów dokonywanych przez układ pomiarowo-rozliczeniowy”[17].

Zdaniem sądu rejonowego, który zainicjował postępowanie przed Trybunałem Konstytucyjnym, można uznać, że opłata za nielegalny pobór energii elektrycznej ma charakter opłaty, którą można określić mianem opłaty ustawowej. Według sądu, choć prawo nie nakłada obowiązku, to niemal wszystkie przedsiębiorstwa określiły opłaty w takiej właśnie maksymalnej wysokości. Sąd przeanalizował pod tym kątem 20 taryf stosowanych przez różne elektrownie, zwracając uwagę na to, że wysokość rekompensaty dla elektrowni wydaje się nieadekwatna do rzeczywistych strat, jakie poniosła na skutek kradzieży prądu. Jak wskazał, już nawet jednokrotność stawek taryfowych z nawiązką rekompensowałaby elektrowni wartość skradzionej energii. Stąd też opłata w wysokości pięciokrotności stawek taryfowych powinna być odczytywana jako opłata o charakterze sankcji mającej za cel nie tylko naprawienie szkody wyrządzonej za sprawą nielegalnego poboru, ale także represję wobec podmiotu, który się tego dopuścił, posiadając również walor odstraszający[18].

Warto też zaznaczyć, że posiadanie nielegalnej instalacji elektrycznej w nieruchomości otrzymanej w darowiźnie nie przesądza o winie odbiorcy – należy wykazać celowe wprowadzenie w błąd sprzedawcy prądu i osiągnięcie z tego tytułu korzyści. W wielu przypadkach nielegalny pobór energii elektrycznej wiąże się z uszkodzeniem instalacji w budynku, co może być częstą przyczyną pożarów bądź porażenia prądem elektrycznym nie tylko osób nielegalnie pobierających energię elektryczną, lecz również osób mieszkających w sąsiedztwie. Interesujący wyrok w kwestii nielegalnego poboru energii zapadł w 2013 r. w Sądzie Rejonowym w Opolu w II Wydziale Karnym.

---

[17] M. Kryszkiewicz, *Za kradzież…*, op. cit.

[18] Ibid.

Przedsiębiorstwo energetyczne oskarżyło odbiorcę, że w bliżej nieustalonym okresie pomiędzy 11 października 2001 r. a 14 kwietnia 2012 r. dokonywał on zaboru w celu przywłaszczenia energii elektrycznej z pominięciem układu pomiarowo-rozliczeniowego[19].

4. Problematyka kontroli

Zagadnienie kontroli sposobu pobierania energii przez odbiorcę stanowi przedmiot licznych analiz wiążących się z kwestią zwalczania nielegalnych działań w tym obszarze. Jak stanowi art. 6 ust. 1. ustawy – Prawo energetyczne, przedsiębiorstwo energetyczne wykonujące działalność gospodarczą w zakresie przesyłania lub dystrybucji paliw lub energii przeprowadza kontrolę legalności pobierania paliw lub energii, kontrolę układów pomiarowo-rozliczeniowych, dotrzymania zawartych umów oraz prawidłowości rozliczeń[20]. Kontrola ta, wykonywana na podstawie upoważnienia udzielonego przez przedsiębiorstwo energetyczne, może obejmować nie tylko odbiorców, lecz także inne podmioty. Jak ponadto stwierdzają Anna Walaszek-Pyzioł i Wojciech Pyzioł, zasadniczo udzielenie upoważnienia do prowadzenia kontroli powoduje powstanie obowiązków do poddania się kontroli po stronie klientów przedsiębiorstw sektora energetycznego[21].

Szczególne zasady przeprowadzania przez przedsiębiorstwa energetyczne kontroli określa Rozporządzenie w sprawie przeprowadzania kontroli przez przedsiębiorstwa energetyczne. W dokumencie tym określono w szczególności, co obejmuje kontrola oraz uprawnienia kontrolujących. Jak stanowi § 4, kontrole przeprowadza przedsiębiorstwo energetyczne z własnej inicjatywy lub na wniosek odbiorcy. Według § 5.1. kontrole są przeprowadzane przez upoważnionych przedstawicieli przedsiębiorstw energetycznych. Jednym

[19] T. Jurczak, *Kradzież energii trzeba udowodnić, a nie domniemywać*, Gazetaprawna.pl, 18.06.2015, https://serwisy.gazetaprawna.pl/energetyka/artykuly/877964,kradziez-energii-trzeba-udowodnic-a-nie-domniemywac.html (dostęp: 13.08.2019).

[20] *Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. 2012 poz. 1059 z poźn. zm.).*

[21] A. Walaszek-Pyzioł, W. Pyzioł, *Prawo energetyczne. Komentarz*, Warszawa 1998, s. 34, za: M. Szewczyk, *Charakter prawny upoważnień do przeprowadzania kontroli przez przedsiębiorstwa energetyczne*, w: A. Walaszek-Pyzioł (red.), *Interdyscyplinarne problemy nielegalnego poboru energii*, Warszawa 2016, s. 175.

z celów nadzoru, wskazanym w tymże akcie prawnym, jest ustalenie, czy miało miejsce pobieranie energii bez zawarcia umowy albo z częściowym lub całkowitym pominięciem układu pomiarowego[22].

Jak stanowi art. 6b. ust. 1., przedsiębiorstwo energetyczne wykonujące działalność gospodarczą w zakresie przesyłania lub dystrybucji paliw gazowych lub energii może wstrzymać, z zastrzeżeniem art. 6c niniejszej ustawy, dostarczanie paliw gazowych lub energii, jeżeli:

1) w wyniku przeprowadzonej kontroli stwierdzono, że nastąpiło nielegalne pobieranie paliw lub energii;
2) odbiorca zwleka z zapłatą za świadczone usługi, co najmniej przez okres 30 dni po upływie terminu płatności.

Trzeba dodać, że w wyniku przeprowadzonego postępowania Prezes URE rozstrzyga, czy wstrzymanie dostaw będące następstwem nielegalnego poboru było uzasadnione[23]. W przeszłości pewnym problemem był brak postępowań karnych, które zakończyłyby się wyrokami skazującymi dla osób odpowiedzialnych za nielegalny pobór energii elektrycznej. Pociągało to za sobą brak skutku w postaci prewencji ogólnej i szczegółowej, a osoby, które dokonały nielegalnego poboru albo które zamierzały go dokonać, mogły czuć się niemal bezkarne, gdyż większość postępowań przygotowawczych kończyła się postanowieniami o umorzeniu wobec niewykrycia sprawcy[24].

W przypadku ujawnienia poboru energii elektrycznej z pominięciem wskazań licznika pobierane są przez dostawcę energii opłaty sanacyjne, które należy uznać za wysokie. Są one obliczane według obowiązującej taryfy. Warto zauważyć, że w przypadku przeciętnego gospodarstwa domowego lub niewielkiego przedsiębiorstwa opłaty sanacyjne dalece przewyższają korzyści uzyskane z podjętego działania. Z uwagi na to należy analizować także postępowanie dostawcy energii wobec jej odbiorcy oraz ujawniać nieprawidłowości w działaniu tego pierwszego – wysokość opłat sankcyjnych

---

[22] *Rozporządzenie Ministra Gospodarki z dnia 11 sierpnia 2000 r. w sprawie przeprowadzania kontroli przez przedsiębiorstwa energetyczne (Dz.U. 2000 Nr 75 poz. 866).*

[23] Z. Muras, *Prawno-regulacyjne aspekty nielegalnego poboru paliw i energii*, w: A. Walaszek-Pyzioł (red.), *Interdyscyplinarne problemy nielegalnego poboru energii*, Warszawa 2016, s. 160.

[24] A. Stankiewicz, M. Balwicka-Szczyrba, *Nielegalne pobieranie…*, op. cit., s. 54.

może skłaniać pracowników dostawcy energii do działań „stymulujących" przypadki poboru energii z pominięciem licznika[25].

5. Możliwości działań prewencyjnych

Według Anny Górskiej kradzież energii elektrycznej można ograniczyć, stosując nowoczesne rozwiązania techniczne, takie jak mierniki zabezpieczone przed manipulacją przez osoby niepowołane, metody zarządzania – kontrolę oraz monitorowanie, a w niektórych przypadkach restrukturyzację własności i regulację systemów elektroenergetycznych. Z przedstawionymi przestępstwami wiąże się kwestia ubóstwa energetycznego łączącego się z ubóstwem społecznym, mniejszymi dochodami, stosunkowo wyższymi wydatkami na energię. Problem ten determinuje możliwość kradzieży energii elektrycznej i manipulacji przy nośnikach energii. Warto zaznaczyć, że duże znaczenie w walce z ubóstwem energetycznym ma poprawa efektywności energetycznej. Dla działań prewencyjnych istotne jest wydawanie aktów prawnych zabezpieczających interesy przedsiębiorstw tracących znacznie środki z powodu działalności przestępczej[26].

Należy wspomnieć o nakazaniu państwom członkowskim UE zapewnienia odbiorcom wrażliwym niezbędnych dostaw energii, a także zastosowania zintegrowanego podejścia, które zawierałoby w sobie polityki socjalne oraz poprawę efektywności energetycznej w mieszkalnictwie. Można wskazać wiele środków pomocy odbiorcom wrażliwym, do których należy rozłożenie zaległych płatności na raty, prolongatę terminu płatności, odstąpienie od naliczania odsetek za nieterminowe wniesienie opłaty, zaniechanie naliczania odsetek prze określony czas, przyjęcie w miejsce odsetek ustawowych – odsetek umownych o określonej wartości, a także wstrzymanie windykacji lub nieprzeprowadzenie windykacji w określonych porach roku, podczas świąt

[25] J. Grudnicki, *Roszczenia związane z kradzieżą energii elektrycznej*, Krynica-Zdrój 2012, s. 81.

[26] A. Górska, *Relacja między ubóstwem energetycznym a przestępstwem kradzieży energii elektrycznej – sposoby prewencji*, Ł. Wojcieszak, B. Oręziak, M. Wielec (red.), *Rynek energetyczny. Zapobieganie przyczynom przestępczości*, Warszawa 2019, s. 105.

lub przed dniami wolnymi od pracy, umarzanie zaległości, instalowanie przedpłatowego układu pomiarowo-rozliczeniowego[27].

Działalność legislacyjna, prowadzona zwłaszcza od 2015 r., przyczynia się do zmniejszenia ubóstwa społecznego. To zaś może wpływać na zmniejszenie się liczby przestępstw. Samo zminimalizowanie poziomu ubóstwa energetycznego zapewniłoby odbiorcom większą uczciwość wobec dostawców energii, w tym energii elektrycznej. Istotne są przy tym techniczne problemy liczników, które powinny być regulowane prawnie, zabezpieczając również interesy obywateli. Należy podkreślić, że liczniki nierzadko psują się, ingerencja zaś pracowników przedsiębiorstw energetycznych oraz celowe ich uszkadzanie na niekorzyść klientów generują nowe formy przestępstw na rynku energetycznym. Trudno również stwierdzić, czy i ile energii pobierał konsument, świadomie popełniając przestępstwo[28].

Na fakt, iż co roku wzrasta liczba wykrywania kradzieży prądu, wpływ ma kilka czynników: przede wszystkim prowadzone są wspólne szkolenia pomiędzy policją, pracownikami spółek dystrybuujących oraz zarządcami nieruchomości. Następuje również wzrost świadomości społeczeństwa, w związku z czym klienci stali się istotnym wsparciem. Społeczeństwo w coraz większym stopniu zdaje sobie sprawę z tego, że nielegalny pobór energii stanowi kradzież. Istotne znaczenie ma również upowszechnienie się zawiadomień zgłaszanych zarządcy budynku, policji lub dystrybutorowi energii elektrycznej. Niebagatelne znaczenie ma fakt, iż zgłoszenia są anonimowe[29].

Warto zaznaczyć, że w szczególności przedsiębiorstwo TAURON na dużą skalę prowadzi kontrolę – w 2016 r. ponad 85 tys. przeprowadzonych kontroli wykazało ponad 6 tys. przypadków nielegalnego poboru energii, natomiast rok wcześniej prawie 90 tys. kontroli przyniosło wykrycie ponad 7 tys. nielegalnych podłączeń. Jest to przykład niewątpliwie skutecznej walki z kradzieżą prądu elektrycznego, której rezultatem jest spadek liczby przypadków nielegalnego poboru energii elektrycznej i wzrost ich wykrywalności obserwowany w przedsiębiorstwie TAURON. Poza kompleksowymi działaniami kontrolnymi prowadzone są również akcje prewencyjne i edukacyjne.

---

[27] Ł. Wojcieszak, *Pozycja odbiorcy wrażliwego w polskim prawie gazowym*, w: M. Minta, W. Śledzik (red.), *Energetyka. Wyzwania prawno-instytucjonalne*, Poznań 2016, s. 230.

[28] A. Górska, *Relacja między…*, op. cit., s. 106.

[29] *Co grozi za kradzież prądu…*, op. cit.

Wykrywanie i eliminacja nielegalnego poboru energii są ważne dla spółki nie tylko ze względów ekonomicznych, ale również dlatego, że poprawiają bezpieczeństwo klientów przedsiębiorstwa. Warto zaznaczyć, że kradzież prądu, kiedy dochodzi do manipulacji przy liczniku lub w instalacji elektrycznej, generuje ryzyko wypadków, porażeń i pożaru. Zagrożenie to dotyczy to nie tylko osób bezpośrednio zaangażowanych w kradzież, ale też często ich rodzin czy sąsiadów[30].

Jak stwierdził Leszek Wojtachnio, Dyrektor ds. Technicznych w TAURON Dystrybucja, stale rozwijane są narzędzia do wykrywania i zwalczania kradzieży energii. Co ważne, dużym wsparciem w procesie likwidowania nielegalnych podłączeń są klienci, którzy zaniepokojeni podejrzanymi instalacjami proszą o ich sprawdzenie. Każde zgłoszenie jest sprawdzane, a osoba zgłaszająca pozostaje anonimowa. W przedsiębiorstwie od lat działa Telefon Bezpieczeństwa – Linia Antykradzieżowa, można dzwonić pod określony numer oraz podzielić się swoimi podejrzeniami związanymi z zauważonymi przeróbkami i prowizorkami. Wszystkie zgłoszenia są wnikliwie sprawdzane, a pracownicy przedsiębiorstwa TAURON posiadają upoważnienie do przeprowadzenia czynności kontrolnych oraz legitymację służbową pracowników. Na każdym upoważnieniu wydanym przez przedsiębiorstwo znajduje się imienna pieczątka z podpisem oraz numerem kontaktowym do osoby wystawiającej upoważnienie[31].

6. Podsumowanie

Problem kradzieży energii elektrycznej jest niewątpliwie zjawiskiem poważnym. Jak wskazano, uwzględniając polskie uwarunkowania i ich specyfikę, można wskazać sposoby zmniejszenia tego rodzaju przestępczej działalności. Jak zaznaczono, w Polsce istnieje wiele problemów związanych z kradzieżą energii elektrycznej. Jednym z nich jest słaba wykrywalność, choć co roku wzrasta liczba ujawnianych kradzieży prądu. Polepszenie się tej sytuacji jest

[30] *Coraz lepsza wykrywalność nielegalnego poboru energii*, Elektroinfo.pl, 27.03.2017, http://www.elektro.info.pl/aktualnosc/id7723,coraz-lepsza-wykrywalnosc-nielegalnego-poboru-energii (dostęp: 14.09.2019).

[31] Ibid.

wynikiem wzrostu świadomości społecznej, szkoleń czy upowszechnienie się zawiadomień.

Dla zwalczania kradzieży energii elektrycznej duże znaczenie ma właściwa kontrola, która została uregulowana w prawie polskim. Szczególnie istotna jest możliwość wstrzymania dostarczania energii, a także nakładanie opłat sanacyjnych, które należy uznać za wysokie. Istotny jest tu zatem odstraszający charakter przewidzianych prawem sankcji. Skuteczność kontroli, przedstawiona na przykładzie przedsiębiorstwa TAURON, znacznie zmniejsza ryzyko dokonywania czynów przestępczych.

Zasadnicze znaczenie ma zwłaszcza zwalczanie ubóstwa energetycznego. Sposoby walki z tym zjawiskiem są zróżnicowane, a uwagę zwraca rola wsparcia socjalnego, obserwowanego zwłaszcza w drugiej dekadzie XXI w. Działania prospołeczne pomimo obciążeń dla budżetu państwa pozwalają, poprzez wsparcie socjalne, zmniejszyć rozmiar ubóstwa energetycznego, a co za tym idzie, zapewne także liczbę popełnianych kradzieży energii.

Jak wykazano, pomimo stosunkowo wysokich kar grożących za kradzież energii elektrycznej przestępstwo to wciąż pozostaje poważnym problemem. Pożądany skutek odnoszą za to wskazane w opracowaniu działania o charakterze prewencyjnym i społecznym, nie zaś groźba poniesienia wysokich kosztów, w szczególności w wyniku uiszczenia opłat sankcyjnych. Przewidywany przez Prawo energetyczne wymiar możliwej do nałożenia na sprawcę kradzieży kary, mający charakter odstraszający, nie przyczynił się w zadowalający sposób do zmniejszenia liczby przestępstw.

W świetle przedstawionych rozważań należy stwierdzić, że skuteczne zapobieganie kradzieży energii elektrycznej może być rezultatem zarówno ścisłej kontroli i wskazanych wcześniej działań prewencyjnych, lecz nie należy także lekceważyć znaczenia czynnika, jakim jest bogacenie się społeczeństwa, choć warto zaznaczyć, że potrzeba jeszcze czasu, aby stwierdzić, jak (i czy) w istocie uruchomione programy społeczne wpłynęły na ograniczenie zjawiska kradzieży energii elektrycznej.

Bibliografia

Bednarz P., *Miliony Polaków mają problem z ogrzaniem swoich domów. 500 plus poprawia jednak sytuację*, businessinsider.com.pl, 31.01.2018, https://businessinsider.com.pl/twoje-pieniadze/ubostwo-energetyczne-w-polsce-na-czym-polega/d8rdmnn (dostęp: 7.09.2019).

Billewicz K., *Analityczne metody wykrywania kradzieży energii elektrycznej*, „Energetyka" – luty 2006, https://www.cire.pl/pliki/2/wykrywanie_kradziezy.pdf (dostęp: 22.08.2019).

Co grozi za kradzież prądu?, Enerad.pl, 25.05.2017, https://enerad.pl/aktualnosci/co-grozi-za-kradziez-pradu (dostęp: 21.08.2019).

Coraz lepsza wykrywalność nielegalnego poboru energii, Elektroinfo.pl, 27.03.2017, http://www.elektro.info.pl/aktualnosc/id7723,coraz-lepsza-wykrywalnosc-nielegalnego-poboru-energii (dostęp: 14.09.2019).

Górska A., *Relacja między ubóstwem energetycznym a przestępstwem kradzieży energii elektrycznej – sposoby prewencji*, w: Ł. Wojcieszak, B. Oręziak, M. Wielec (red.), *Rynek energetyczny. Zapobieganie przyczynom przestępczości*, Warszawa 2019.

Grudnicki J., *Roszczenia związane z kradzieżą energii elektrycznej*, Krynica-Zdrój 2012.

Jurczak T., *Kradzież energii trzeba udowodnić, a nie domniemywać*, Gazetaprawna.pl, 18.06.2015, https://serwisy.gazetaprawna.pl/energetyka/artykuly/877964,kradziez-energii-trzeba-udowodnic-a-nie-domniemywac.html (dostęp: 13.08.2019).

Kardas P., *Przedsiębiorstwo energetyczne jako pokrzywdzony*, w: A. Walaszek-Pyzioł (red.), *Interdyscyplinarne problemy nielegalnego poboru energii*, Warszawa 2016, s. 233–258.

Kędzierski J., *Kradzieże prądu sprawiają problemy sądom*, „Rzeczpospolita", 30.11.2012, https://www.rp.pl/artykul/957109-Kradzieze-pradu-sprawiaja-problemy-sadom.html (dostęp: 25.09.2019).

Kryszkiewicz M., *Za kradzież prądu o jedną karę za dużo*, Gazetaprawna.pl, 12.02.2014, https://prawo.gazetaprawna.pl/artykuly/777251,za-kradziez-pradu-o-jedna-kare-za-duzo.html (dostęp: 4.09.2019).

Kukuła Z., *Przestępstwo kradzieży energii – kontrowersje interpretacyjne*, „Wojskowy Przegląd Prawniczy" 2015, nr 3, https://pk.gov.pl/wp-content/uploads/2016/06/8df84ef7b5a5e34e10415e1989774776.pdf (dostęp: 26.09.2019).

Muras Z., *Prawno-regulacyjne aspekty nielegalnego poboru paliw i energii*, w: A. Walaszek-Pyzioł (red.), *Interdyscyplinarne problemy nielegalnego poboru energii*, Warszawa 2016, s. 151–166.

Rozporządzenie Ministra Gospodarki z dnia 11 sierpnia 2000 r. w sprawie przeprowadzania kontroli przez przedsiębiorstwa energetyczne (Dz.U. 2000 Nr 75 poz. 866).

Stankiewicz A., Balwicka-Szczyrba M., *Nielegalne pobieranie paliw lub energii. Aspekty prawne i zasady postępowania*, Gdańsk, wrzesień 2013.

Surowe kary za kradzież prądu, Dziennikpolski24.pl, 22.10.2014, https://dziennikpolski24.pl/surowe-kary-za-kradziez-pradu/ar/3617703 (dostęp: 26.08.2019).

Szewczyk M., *Charakter prawny upoważnień do przeprowadzania kontroli przez przedsiębiorstwa energetyczne*, w: A. Walaszek-Pyzioł (red.), *Interdyscyplinarne problemy nielegalnego poboru energii*, Warszawa 2016.

Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 2012 poz. 1059 z późn. zm.).

Walaszek-Pyzioł A., Pyzioł W., *Prawo energetyczne. Komentarz*, Warszawa 1998.

Wojcieszak Ł., *Pozycja odbiorcy wrażliwego w polskim prawie gazowym*, w: M. Minta, W. Śledzik (red.), *Energetyka. Wyzwania prawno-instytucjonalne*, Poznań 2016, s. 217–232.

ROZDZIAŁ IV

Propozycje poprawy skuteczności metod zapobiegania przestępczości w ubezpieczeniach komunikacyjnych

JOLANTA STANIENDA[1]

1. Wprowadzenie

Gwałtowny rozwój procesu globalizacji oraz liberalizacji rynków finansowych, komunikacji, przemieszczania się ludzi i kapitału oprócz pozytywnych skutków ma swoje odbicie również w przemianach zachodzących w sferze przestępczości, a w szczególności w zorganizowanych grupach przestępczych, których struktury, jak i zakres działania przybierają coraz bardziej charakter międzynarodowy. Nie tylko rozszerzają one zakres terytorialny swojej bytności, ale coraz częściej są w stanie prowadzić nielegalną działalność daleko od miejsca swojej podstawowej lokalizacji. Organy ścigania stoją przed ogromnym wyzwaniem, aby nie tylko zidentyfikować, ale również doprowadzić do ukarania głównych przestępców przebywających często poza granicami kraju popełnienia przestępstwa[2].

Przestępstwa ubezpieczeniowe w sposób istotny utrudniają właściwy rozwój rynku ubezpieczeniowego i są jaskrawym przykładem zagrożenia związanego z umową ubezpieczenia mogącą wpływać negatywnie na prawa lub obowiązki ubezpieczonych, gdyż ostatecznie działania lub zaniechania mające na celu wyłudzenie odszkodowania uderzają w interesy konsumentów

[1] Doktor; adiunkt w Katedrze Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

[2] J. Talarek, *Przestępczość w ubezpieczeniach komunikacyjnych w Polsce na tle wybranych krajów europejskich*, Gazeta ubezpieczeniowa on-line, http://www.gu.com.pl/index.php?option=com_content&view=article&id=1578&catid=124:ubezpieczenia-majtkowe&Itemid=154 (dostęp: 21.08.2019).

poprzez wzrost składki oraz obsługę i stosunek zakładów ubezpieczeń do osób poszkodowanych[3].

W związku z tym **konieczne jest wskazanie podstawowych zagrożeń, zakresu zjawiska przestępczości ubezpieczeniowej oraz metod przeciwdziałania. Celowi temu służyć ma niniejsze opracowanie dotyczące przestępczości w ubezpieczeniach komunikacyjnych oparte na literaturze przedmiotu, aktach prawnych oraz wzbogacone o studium przypadku.**

W opracowaniu dokonano analizy problematyki przestępczości w ubezpieczeniach komunikacyjnych oraz zaproponowano wprowadzenie metod zapobiegania im w kontekście koncepcji „Improving Performance". Opracowanie uwzględnia dwa ujęcia problemu przestępczości na rynku ubezpieczeniowym: ujęcie osobowe i instytucjonalne, które są ze sobą nierozerwalnie związane. Równocześnie przedstawione zagadnienia zaprezentowano z punktu widzenia prawnego, gospodarczego oraz technologicznego. Skoncentrowano się głównie na aspekcie ekonomiczno-społecznym.

Dla realizacji celu opracowania, jakim jest wskazanie innowacyjnych i skutecznych metod zapobiegania przestępczości w ubezpieczeniach komunikacyjnych, postawiono następujące pytania badawcze:

1. Czym determinowane jest zjawisko wyłudzeń nienależnych odszkodowań w ubezpieczeniach?
2. Jaka jest skala przestępczości w ubezpieczeniach komunikacyjnych?
3. Jakie istnieją sposoby wyłudzania nienależnych odszkodowań w ubezpieczeniach komunikacyjnych?
4. Jakimi metodami w sposób skuteczny można zwalczać przestępczość w ubezpieczeniach komunikacyjnych?

Metodą badawczą, jaką wykorzystano do realizacji postawionego celu opracowania i odpowiedzi na sformułowane pytania badawcze, było dowodzenia dedukcyjne. Struktura opracowania obejmuje wstęp, trzy części oraz podsumowanie. W pierwszej części zaprezentowano istotę, przyczyny oraz skalę zjawiska przestępczości na rynku ubezpieczeń komunikacyjnych.

[3] T. Wróblewski, *Przestępczość ubezpieczeniowa – metody działania oraz sposoby zapobiegania w świetle ankiety Rzecznika Ubezpieczonych,* https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Tomasz_Wroblewski_-_Przestepczosc_ubezpieczeniowa_-_metody_dzialania_oraz_sposoby_zapobiegania_w_swietle_ankiety_Rzeczni__145 (dostęp: 21.08.2019).

Przedstawiono również strukturę skarg na zakłady ubezpieczeniowe w Polsce w sprawie ubezpieczeń komunikacyjnych. Część druga poświęcona jest sposobom wyłudzeń w ubezpieczeniach komunikacyjnych oraz likwidacji szkody komunikacyjnej jako studium przypadku. Ostatnia część prezentuje metody zapobiegania wyłudzeniom odszkodowań w ubezpieczeniach komunikacyjnych. Zakończeniem opracowania są postulaty (propozycje) poprawy skuteczności metod zapobiegania przestępczości w ubezpieczeniach komunikacyjnych.

2. Przestępczość na rynku ubezpieczeń komunikacyjnych – skala zjawiska

Rozmiary przestępczości ubezpieczeniowej mogą być rozpatrywane w ujęciu osobowym i instytucjonalnym, dlatego można przedstawić następujące kategorie tego zjawiska[4]:

1. Przestępczość ubezpieczeniowa rzeczywista – wszystkie przestępstwa polegające na uzyskaniu korzyści majątkowej kosztem zakładu ubezpieczeń (w szczególności nienależnego odszkodowania bądź świadczenia ubezpieczeniowego) i jednocześnie łączące się z wykorzystaniem stosunku ubezpieczeniowego, które zostały popełnione w danym czasie i na określonym terenie.
2. Przestępczość ubezpieczeniowa ujawniona – wszystkie czyny, o których informacje uzyskały organy ścigania i w związku z tym wszczęły postępowanie przygotowawcze w sprawie podejrzenia popełnienia przestępstwa ubezpieczeniowego. Przestępczość ujawniona nazywana jest również przestępczością pozorną, gdyż nie wszystkie czyny, które zostały zakwalifikowane jako przestępstwa w momencie wszczęcia postępowania przygotowawczego, są faktycznie przestępstwami. W przypadku przestępstw ubezpieczeniowych sytuacja taka nie będzie należała wcale do rzadkości – przykładowo zakłady ubezpieczeń nie mają podstaw prawnych do aktywnego wykrywania przestępstw ubezpieczeniowych i zgłaszając podejrzenie popełnienia takiego przestępstwa, opierają się najczęściej jedynie na własnych

[4] J. Talarek, *Przestępczość w ubezpieczeniach komunikacyjnych*…, op. cit.

informacjach, co może w efekcie doprowadzić do mylnych wniosków i wysunięcia podejrzeń w stosunku do niewinnych osób.

3. Przestępczość ubezpieczeniowa stwierdzona – wszystkie czyny, które w wyniku postępowania przygotowawczego zostały potwierdzone jako przestępstwa ubezpieczeniowe.
4. Przestępczość ubezpieczeniowa osądzona – wszystkie czyny, których charakter jako przestępstw ubezpieczeniowych został potwierdzony w wyniku postępowania sądowego i które zostały osądzone wyrokiem skazującym.

Jednym z najistotniejszych aktów prawnych, który wpływa na rozwój rynku ubezpieczeń jest przyjęta przez Parlament Europejski i Radę UE dyrektywa w sprawie dystrybucji ubezpieczeń (tzw. dyrektywa IDD)[5], zastąpiła ona dotychczas obowiązującą dyrektywę IMD2[6]. Dyrektywa IDD została zaimplementowana do polskiego systemu prawnego w ustawie o dystrybucji ubezpieczeń[7], w ustawie o działalności ubezpieczeniowej i reasekuracyjnej[8], ustawie o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym[9] oraz w ustawie o nadzorze ubezpieczeniowym i emerytalnym[10]. Cele dyrektywy zostały zawarte w jej preambule i dotyczą zapewnienia wyższego poziomu ochrony klienta poprzez nałożenie na dystrybutorów ubezpieczeniowych wiele nowych obowiązków, m.in.[11]: rzetelnego informowania o cechach produktu, opłatach, zasadach wynagradzania pośredników przez towarzystwa ubezpieczeń. Istotą jest dokładne i rzetelne

[5] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń* (wersja przekształcona).

[6] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2002/92/WE z dnia 9 grudnia 2002 r. w sprawie pośrednictwa ubezpieczeniowego, (Dz. Urz. L9).*

[7] *Ustawa z dnia 15 grudnia 2017 roku o dystrybucji ubezpieczeń (Dz.U. 2017 poz. 2486).*

[8] *Ustawa z dnia 11 września 2015 roku o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. 2015 poz. 1844 z późn. zm.).*

[9] *Ustawa z dnia 5 sierpnia 2015 roku o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym (Dz.U. 2015 poz. 1348 z późn. zm.).*

[10] *Ustawa z dnia 22 maja 2003 roku o nadzorze ubezpieczeniowym i emerytalnym (Dz.U. 2003 Nr 124 poz. 1153 z późn. zm.).*

[11] Zapisane w preambule Dyrektywy IDD, pkt.: 63, *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń* (wersja przekształcona).

analizowanie przez dystrybutorów potrzeb klienta i przedstawianie mu najbardziej korzystnej oferty.

Wynika z tego, że głównym beneficjentem przepisów dyrektywy IDD są konsumenci, których pozycja na ryku ubezpieczeń poprzez uzyskanie większych uprawnień oraz ochronę w ramach zawieranych umów ubezpieczenia powinna się wzmocnić.

Najważniejszymi aktami prawnymi w Polsce regulującymi rynek ubezpieczeń komunikacyjnych są: ustawa o działalności ubezpieczeniowej i reasekuracyjnej[12], ustawa o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych[13] oraz ustawa o dystrybucji ubezpieczeń[14]. Zawierają one najważniejsze regulacje porządkujące rynek ubezpieczeń komunikacyjnych.

Wielkość tego rynku jest trudna do oszacowania, co wynika z przyjętej metodologii oficjalnych danych statystycznych, choć wielkość tego rynku zależy od liczby pojazdów. W Polsce na 1000 mieszkańców przypada ok. 380 samochodów osobowych[15].

Skala zjawiska przestępczości na rynku ubezpieczeń komunikacyjnych jest duża i ma tendencję rosnącą, podobnie jak na bardziej rozwiniętych rynkach ubezpieczeń w Europie i na świecie[16]. Przyczyn takiej skali zjawiska jest bardzo wiele, wśród nich przede wszystkim motywy o charakterze: ekonomicznym (uzyskanie korzyści majątkowych) oraz społecznym (m.in. przyzwolenie społeczne na zachowania nieetyczne). Potwierdzeniem są wyniki raportu o moralności finansowej Polaków, przedstawiające m.in. poziom akceptacji

---

[12] *Ustawa z dnia 11 września 2015 roku o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. 2018 poz. 999 z późn. zm.).*

[13] *Ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. 2018, poz. 473 z późn. zm.).*

[14] *Ustawa z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń (Dz.U. 2017 poz. 2486 z późn. zm.).*

[15] *Raport z badania rynku ubezpieczeń komunikacyjnych*, Urząd Ochrony Konkurencji i Konsumentów, Departament Analiz Rynku, Warszawa 2018, s. 5.

[16] P. Majewski, *Analiza danych dotyczących przestępstw ujawnionych w 2016 roku w związku z działalnością zakładów ubezpieczeń- członków Polskiej Izby Ubezpieczeń,* Polska Izba Ubezpieczeń, Warszawa 2017, s. 25.

nieetycznych zachowań finansowych (tzw. moralnego permisywizmu)[17]. Wielkość nadużyć dokonywanych przez konsumentów pokazuje, że instytucje finansowe, państwo czy też inne osoby powinny zachować ostrożność w relacjach z klientami, ponieważ co piąty z nich jest gotowy zaakceptować nieetyczne zachowania finansowe[18]. Na pytanie zadane Polakom: „Czy można usprawiedliwić, gdy ktoś zawyża wartość poniesionych szkód, aby uzyskać nienależne odszkodowanie?", aż 20% respondentów odpowiedziało, że: czasem, często lub zawsze (tabela 1). Wśród powodów usprawiedliwiania zawyżania wartości poniesionych szkód dla uzyskania nienależnego odszkodowania aż 71% respondentów jest przekonanych o braku uczciwości ubezpieczycieli, dlatego stwierdza, że można dopuszczać się otrzymania nienależnego odszkodowania, prawie 16% badanych usprawiedliwia taką sytuację małymi dochodami osoby, a 13% ankietowanych stwierdza, że wiele osób tak robi, czyli wskazuje na społeczny standard takiego zachowania[19] (tabela 2).

Tabela 1. System normatywny dotyczący nadużyć konsumentów w obszarze finansów w Polsce w 2018 r.

Czy można usprawiedliwić, gdy ktoś:	Częstość (w %)				
	Nigdy	Czasem	Często	Zawsze	Rok badania
Posługuje się cudzym dokumentem tożsamości, by uzyskać kredyt?	98,8	0,9	0,3	0,0	2018
	97,2	2,2	0,1	0,5	2017
	98,5	0,5	0,5	0,5	2016
Nie zwraca uwagi kasjerowi, który pomylił się na własną niekorzyść?	81,0	15,0	2,1	1,9	2018
	74,6	15,4	3,9	6,1	2017
	80,6	11,8	2,8	4,8	2016
Zawyża wartość poniesionych szkód, by uzyskać nienależne odszkodowanie?	79,3	17,6	2,5	0,6	2018
	85,1	11,6	2,0	1,3	2017
	85,7	10,6	2,2	1,5	2016
Zmienia często rachunki bankowe, by uniknąć zajęcia środków przez komornika?	77,0	19,3	2,7	1,0	2018
	78,4	18,6	1,6	1,4	2017
	76,8	19,2	2,7	1,3	2016

[17] A. Lewicka-Strzałecka, *Moralność finansowa Polaków – raport z badań III edycja*, Gdańsk–Warszawa 2018, http://www.pte.pl/pliki/2/21/moralnosc_2018.pdf (dostęp: 13.08.2019).

[18] Ibid.

[19] Ibid.

Czy można usprawiedliwić, gdy ktoś:	Częstość (w %)				
	Nigdy	Czasem	Często	Zawsze	Rok badania
Zataja informacje uniemożliwiające wzięcie kredytu?	74,6	21,8	2,2	1,4	2018
	81,9	14,3	1,5	2,3	2017
	83,2	13,6	1,8	1,4	2016
Przepisuje majątek na rodzinę, by uciec przed wierzycielem?	72,2	22,9	3,8	1,1	2018
	73,6	21,7	3,0	1,7	2017
	71,2	22,5	3,2	2,6	2016
Płaci gotówką bez rachunku, by uniknąć płacenia VAT?	70,5	24,4	2,1	3,0	2018
	75,1	19,2	2,6	3,1	2017
	67,0	23,2	5,6	4,2	2016
Pracuje na czarno, by uniknąć ściągania długów z pensji?	70,2	24,6	3,5	1,7	2018
	70,6	24,1	3,3	2,0	2017
	64,4	26,9	6,4	2,3	2016
Zaciąga kredyt, nie zapoznając się dokładnie z warunkami spłaty?	67,3	26,0	4,2	2,5	2018
	68,5	25,5	3,3	2,7	2017
	64,1	26,6	6,1	3,2	2016
Indeks Akceptacji Nieetycznych Zachowań Finansowych*	23,2				2018
	21,7				2017
	23,2				2016

*średni odsetek odpowiedzi czasem, często lub zawsze na pytanie o możliwość usprawiedliwiania poszczególnych działań

Źródło: A. Lewicka-Strzałecka, *Moralność finansowa Polaków – raport z badań III edycja*, Gdańsk–Warszawa 2018, http://www.pte.pl/pliki/2/21/moralnosc_2018.pdf (dostęp: 13.08.2019), s. 10

Najbardziej wyraźną prawidłowością przeprowadzonych badań jest to, że wymagania moralne dotyczące kwestii finansowych rosną wraz z wiekiem. Starsze osoby w mniejszym stopniu są skłonne usprawiedliwiać konsumenckie nadużycia niż młodsi. Może to być konsekwencją naturalnego procesu moralnego rozwoju lub efektem różnicy między pokoleniami, spowodowanej funkcjonowaniem w odmiennych systemach gospodarczych. Przeprowadzone badania pozwalają stwierdzić, że również płeć jest zmienną trwale różnicującą respondentów ze względu na poziom moralnego permisywizmu, który w wyższym stopniu przejawiają mężczyźni niż kobiety[20].

[20] Ibid.

Tabela 2. Struktura odpowiedzi respondentów o rodzajach usprawiedliwień zawyżania wartości poniesionych szkód, by uzyskać nienależne odszkodowanie

Jeżeli uważa Pan/i, że czasem (często lub zawsze) można usprawiedliwiać, gdy ktoś zawyża wartość poniesionych szkód, by uzyskać niezależne odszkodowanie, to dlatego że:	Procent badanych, którzy uznali, że można usprawiedliwiać, gdy ktoś zawyża wartość poniesionych szkód, by uzyskać niezależne odszkodowanie
Ta osoba ma małe dochody	15,9
Ubezpieczyciele nie zawsze są uczciwi wobec klientów	71,0
Wiele osób tak robi	13,1

Źródło: A. Lewicka-Strzałecka, *Moralność finansowa Polaków…*, op. cit., s. 18.

Przekonanie o braku uczciwości ubezpieczycieli (tabela 2) zapewne w znacznej części klientów kształtowane jest poprzez wiedzę potoczną, czerpaną z osobistych doświadczeń i otoczenia, jak i informacji opartych na przekazie medialnym. Obejmują one wiadomości o wielomilionowych nadużyciach popełnianych przez globalnych graczy, a także liczne przypadki codziennych oszustw, polegające na namawianiu do zakupu nieodpowiednich lub wręcz niebezpiecznych produktów finansowych, ukrywaniu w umowach niekorzystnych warunków, bagatelizowaniu ryzyka, posługiwaniu się oszukańczą lub zwodniczą reklamą itp[21]. Postrzeganie konsumenta jako ofiary instytucji finansowych kształtuje swoistą moralność retrybutywną, usprawiedliwiającą popełnianie nadużyć dążeniem do wyrównania rachunków. Tego typu usprawiedliwienie jest szczególnym przejawem funkcjonowania reguły wzajemności, zidentyfikowanej i opisywanej przez psychologów społecznych. Silnie zakorzeniona w kulturze reguła wzajemności nakazuje w wersji negatywnej złem odpłacać za doznane zło. W relacjach z instytucjami finansowymi zło nie musiało być doświadczone osobiście, ale jego poczucie jest przenoszone i utrwalane przez prawdziwy lub fałszywy, ale przede wszystkim sensacyjny przekaz[22].

W związku z tym istotny jest zapis preambuły dyrektywy IDD, że: należy zwiększyć poziom zaufania klientów i bardziej ujednolicić przepisy regulujące

[21] Dyrektywa IDD, preambuła pkt. 63 zawiera sformułowanie o konieczności zapewnienia efektu odstraszającego w stosunku do ogółu społeczeństwa poprzez informowanie uczestników rynku o zachowaniach uznawanych za szkodliwe dla klientów, decyzje (organów) powinny być publikowane.

[22] A. Lewicka-Strzałecka, *Moralność finansowa Polaków…*, op. cit. s. 29.

dystrybucję produktów ubezpieczeniowych, aby zapewnić odpowiedni poziom ochrony klientów w całej Unii[23].

Zawyżanie wartości poniesionych szkód po to, by uzyskać nienależne odszkodowanie w przypadku ubezpieczeń komunikacyjnych, odbywa się w różny sposób, jednym z nich jest powiększanie zakresu uszkodzeń, do których doszło w wyniku kolizji, podciąganiu pod stratę uszkodzeń dokonanych jeszcze przed wypadkiem, podobnie jest z wypłatą odszkodowań za utratę uszczerbku na zdrowiu czy utratą „fikcyjnego" mienia w wyniku kradzieży mieszkania, pożaru czy zalania. Okazuje się, że świadome powiększenie roszczenia związanego z autentyczną szkodą (tzw. *opportunistic fraud*) bywa bardziej kosztownym rodzajem przestępstwa dla niektórych ubezpieczycieli niż to, które polega na celowym sfingowaniu całego zdarzenia. Tego typu działanie jest skorzystaniem z nadarzającej się okazji, więc może budzić mniej oporów moralnych niż intencjonalne zaaranżowanie przestępstwa[24].

3. Struktura skarg na zakłady ubezpieczeniowe w Polsce w sprawie ubezpieczeń komunikacyjnych

Rzecznik Finansowy przestawił sprawozdanie ze swojej działalności za 2018 rok[25], z którego wynika, że liczba skarg dotyczących ubezpieczeń OC i AC, które wysłali do niego klienci zakładów ubezpieczeń i osoby poszkodowane, jest wysoka[26].

W 2018 r. wpłynęło do niego 14 043 wniosków zgłaszanych w indywidualnych sprawach z zakresu problematyki ubezpieczeń gospodarczych. Wniosków w zakresie ubezpieczeń na życie (dział I) odnotowano łącznie 4835 (34,4%). Natomiast wniosków z zakresu problematyki pozostałych ubezpieczeń osobowych oraz majątkowych (dział II) w przedstawianym okresie sprawozdawczym odnotowano łącznie 9176 (65,3%)[27].

---

[23] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń* (wersja przekształcona), preambuła, pkt. 10.

[24] A. Lewicka-Strzałecka, *Moralność finansowa Polaków…*, op. cit., s. 17.

[25] Sprawozdanie Rzecznika Finansowego za 2018 r., https://rf.gov.pl/files/22980__5328__Sprawozdanie_Rzecznika_Finansowego_za_2018_r_.pdf (dostęp: 14.08.2019).

[26] Ibid.

[27] Ibid., s. 16.

Najliczniejsza grupa wniosków odnosiła się do problematyki ubezpieczeń komunikacyjnych – 4843 wnioski (34,5%). Wśród nich najwięcej odnotowano na obowiązkowe ubezpieczenie OC p.p.m. – 3784 wnioski (26,9%)[28]. Natomiast liczba wniosków odnoszących się do ubezpieczeń AC, to 681 (4,8%). W przedstawianym okresie sprawozdawczym drugie miejsce zajmowały sprawy dotyczące nieprawidłowości w dziale I – 4835 wniosków (34,4%). Trzecie miejsce w tym okresie sprawozdawczym przypisane było sprawom obejmującym problematykę ubezpieczeń OC (poza OC p.p.m. i OC rolników) – 1634 wnioski (11,6%). Kolejne miejsce w omawianym okresie zajmowały wnioski odnoszące się do ubezpieczenia mienia od kradzieży z włamaniem, od ognia i innych zdarzeń losowych – 855 wniosków (6,1%), w tym ubezpieczenia mienia osób fizycznych – 772 wnioski (5,5%)[29].

W tabeli 3 przedstawiono liczbę skarg dotyczących ubezpieczeń komunikacyjnych z udziałem rynkowym poszczególnych zakładów ubezpieczeń, dla celów porównawczych liczba skarg została przeliczona na 1% udziału rynkowego każdego ubezpieczyciela.

Tabela 3. Struktura skarg na zakłady ubezpieczeniowe w 2018 r. w Polsce (ubezpieczenia komunikacyjne)*

Nazwa ubezpieczyciela	Liczba skarg w sprawie ubezpieczeń komunikacyjnych (od 01.01.2018 do 31.12.2018)	Udział rynkowy mierzony wartością składki przypisanej brutto (wynik dla polis komunikacyjnych od 01.01.2018 do 31.12.2018)	Liczba skarg przypadająca na 1% udziału rynkowego
TUiR WARTA S.A.	358	10,5%	22
Pocztowe TUW	11	0,4%	31
STU Ergo Hestia S.A.	549	15,9%	35
TUiR Allianz Polska S.A.	194	5,4%	36
Gothaer TU S.A.	85	2,0%	43
PZU S.A.	1 513	33,6%	45
Concordia Polska TUW	25	0,5%	46
TU INTERRISK S.A. VIG	102	2,2%	46
TU Compensa S.A. VIG	224	4,4%	51
UNIQA TU S.A.	158	2,6%	61

[28] Ibid., s. 17.
[29] Ibid., s. 20.

Nazwa ubezpieczyciela	Liczba skarg w sprawie ubezpieczeń komunikacyjnych (od 01.01.2018 do 31.12.2018)	Udział rynkowy mierzony wartością składki przypisanej brutto (wynik dla polis komunikacyjnych od 01.01.2018 do 31.12.2018)	Liczba skarg przypadająca na 1% udziału rynkowego
AXA Ubezpieczenia TUiR S.A.	331	5,3%	62
Generali TU S.A.	240	3,9%	62
TUW TUW	130	1,9%	70
Link 4 TU S.A.	323	4,0%	81
AVIVA TU Ogólnych S.A.	61	0,7%	83
TUZ TUW	59	0,6%	104

* w tabeli uwzględniono zakłady ubezpieczeń z siedzibą w Polsce

Źródło: Ubea.pl, http://www.gu.com.pl/index.php?option=com_content&view=article&id=69049:ubeapl-skargi-a-udzia-w-rynku&catid=107:rynek-ubezpiecze&Itemid=106 (dostęp: 3.09.2019).

Z przedstawionych danych w tabeli 3 wynika, że najwięcej skarg polis komunikacyjnych dotyczyło działalności PZU S.A., gdzie zostało skierowanych 1513 wniosków od ubezpieczonych proszących o interwencję w sprawie produktów oferowanych przez tego ubezpieczyciela. Największy udział PZU S.A. na rynku ubezpieczeń majątkowych (33,6%) uzasadnia największą liczbę skarg. Jednak biorąc pod uwagę udział reklamacji w ogólnej liczbie polis komunikacyjnych udzielonych przez PZU SA, tak jak to liczy Ubea.pl, wynik osiągnięty przez to towarzystwo (45 skarg) jest bardzo dobry[30].

Najrzadziej zaskarżane polisy dotyczyły produktów oferowanych przez Wartę (do rzecznika wpłynęło 358 skarg), której udział w rynku stanowił 16,5%. Oznacza to, że na 1% udziału rynkowego Warty przypadały w 2018 r. tylko 22 skargi. Podobnie zaskarżane były w 2018 r. polisy: Pocztowe TUW, gdzie na 1% udziału rynkowego przypadło 31 skarg, STU Ergo Hestia – na 1% udziału rynkowego było 35 skarg, TUiR Allianz Polska – na 1% udziału rynkowego było 36 skarg, Gothaer TU na 1% udziału rynkowego było 43 skargi oraz Concordia Polska TUW i InterRisk – na 1% udziału rynkowego było 46 skarg.

[30] *Skargi na polisy komunikacyjne. Na których ubezpieczycieli skarżyliśy się najczęściej*, https://www.rp.pl/Ubezpieczenia/190519725-Skargi-na-polisy-komunikacyjne-Na-ktorych-ubezpieczycieli-skarzylismy-sie-najczesciej.html (dostęp: 14.08.2019).

Natomiast największa liczba skarg przypadająca na 1% udziału rynkowego dotyczyła TUZ TUW, w przypadku którego na 1% udziału rynkowego przypadły aż 104 skargi na oferowane polisy AC i OC, AVIVA TU Ogólnych S.A. z liczbą skarg 83 na 1% udziału oraz Link 4 TU S.A. z 81 skargami na 1% udziału rynkowego.

Niezwykle istotną kwestią na rynku ubezpieczeń komunikacyjnych wskazanych także w sprawozdaniu Rzecznika Finansowego jest sposób likwidacji szkody i zgłaszanie do tego uwag przez poszkodowanych. Najczęściej poszkodowani zgłaszali sporo uwag do sposobu likwidacji szkody poprzez nieuprawnione kwalifikowanie jej jako całkowitej. Tym samym skarżący wskazywali, że ubezpieczyciele często zaniżają wartość pojazdu w stanie sprzed szkody, a zawyżają wartość pozostałości, przez co odszkodowanie nie wystarcza na rekompensatę poniesionych strat.

Zgłaszane problemy dotyczyły również zwrotu kosztów najmu pojazdu zastępczego, zasadności stosowania amortyzacji części, odszkodowania z tytułu utraty wartości handlowej pojazdu, żądania przedstawienia faktur źródłowych stwierdzających rodzaj i źródło nabycia części zamiennych stosowanych przy naprawie pojazdu oraz obniżania stawek za roboczogodziny.

Poszkodowani skarżyli się też na zbyt niskie wypłaty za szkody osobowe, czyli np. zaniżanie procentu uszczerbku na zdrowiu, zbyt niskie kwoty zadośćuczynień, zaniżenie bądź odmowę wypłaty zadośćuczynienia za doznaną krzywdę dla najbliższych członków rodziny[31].

Jednym z najszybciej rozwijających się przestępstw ubezpieczeniowych są kradzieże aut. Według statystyki Policji (ustawa o statystyce publicznej[32] jak również Rozporządzenie Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2019[33] nakłada na Policję obowiązki w zakresie gromadzenia danych statystycznych w Systemie Analitycznym[34]), liczba kradzionych samochodów z roku na rok spada (tab. 4), jednak wzrasta

[31] *Sprawozdanie Rzecznika Finansowego…*, op. cit., s. 55.

[32] *Ustawa z dnia 29 czerwca 1995 roku o statystyce publicznej (Dz.U. 2019 poz. 649 i 730).*

[33] *Rozporządzenia Rady Ministrów z dnia 14 września 2018 roku w sprawie programu badań* statystycznych *statystyki* publicznej *na rok 2019 (Dz.U. 2018 poz. 2103).*

[34] Kradzież samochodu, http://statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-kryminalne/7-wybranych-kategorii-p/kradziez-cudzej-rzeczy/kradziez-samochodu/122278,Kradziez-samochodu.html (dostęp: 25.09.2019).

wartość kradzionych pojazdów. Oznacza to, że złodzieje dokonują kradzieży droższych modeli aut, ponieważ są one bardziej „opłacalne", a ryzyko podejmowania kradzieży jest takie samo jak w przypadku samochodu tańszego. Wykrywalność przestępstw związanych z kradzieżą pojazdów rosła w latach 2015–2018 (tabela 4).

Tabela 4. Dane dotyczące kradzieży samochodów w Polsce w latach 2015–2018

Kradzieże samochodów	2015 rok	2016 rok	2017 rok	2018 rok
Przestępstwa wszczęte	12 141	11 220	9 823	8816
Przestępstwa zakończone	12 190	11 769	10 287	9123
Przestępstwa stwierdzone	12 036	11 448	10 047	8745
% wykrycia*	21,9	18,3	21,9	23,8
Podejrzani	1 260	1194	1 089	1 056

* Wskaźnik wykrywalności jest to iloraz liczby przestępstw wykrytych (łącznie z wykrytymi podjęciu z umorzenia) przez ogólną liczbę przestępstw stwierdzonych powiększoną o liczbę przestępstw wykrytych po podjęciu postępowań umorzonych w roku ubiegłym lub latach poprzednich – wyrażony w procentach.

Źródło: opracowanie własne na podstawie: http://statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-kryminalne/7-wybranych-kategorii-p/kradziez-cudzej-rzeczy/kradziez-samochodu/122278,Kradziez-samochodu.html (dostęp: 25.09.2019)

Współczesne samochody wyposażone są w elektronikę, która poprawia komfort jazdy, ale jednocześnie daje duże możliwości jej wykorzystania przez przestępców. Przykładem jest szybko rozwijająca się kradzież aut z systemem bezkluczykowym na tzw. walizkę. Metoda ta polega na wykorzystaniu umieszczonego w walizce sprzętu wzmacniającego sygnał emitowany przez kluczyk do auta. Wystarczy, że złodziej wyposażony we wzmacniacz zbliży się do kierowcy, który ma przy sobie kluczyk. Po przywróceniu sygnału wysyłany jest on do podobnego urządzenia, w jaki wyposażony jest wspólnik stojący przy aucie, który otwiera samochód i odjeżdża.

4. Sposoby wyłudzeń w ubezpieczeniach komunikacyjnych – studium przypadku

Ubezpieczenia komunikacyjne należą do grupy produktów najbardziej popularnych na rynku ubezpieczeń, co wynika z raportu „Badania rynku

ubezpieczeń komunikacyjnych, przeprowadzonych przez Urząd Ochrony Konkurencji i Konsumentów". Wyłudzenia odszkodowań są ciągle na rynku polskim istotnym problemem, na którym tracą rzetelni klienci. Dlatego też ubezpieczyciele coraz więcej uwagi poświęcają na walkę z przestępczością ubezpieczeniową, wprowadzając innowacyjne rozwiązania, które podnoszą skuteczność wychwytywania przestępstw.

Dokładne dane dotyczące wyłudzeń w ubezpieczeniach komunikacyjnych są trudne do oszacowania, ponieważ nie każde z nich udaje się wykryć. Na pewno można stwierdzić, że im więcej jest nieuczciwych klientów, tym więcej pojawia się metod i sposobów wyłudzeń. Według pracownika instytucji ubezpieczeniowej (wywiad z pracownikiem multiagencji z 10-letnim doświadczeniem) najczęściej występują dwa typy wyłudzeń w ubezpieczeniach komunikacyjnych:

- **wyłudzenia na małą skalę**, polegające np. na zdarzeniu zderzenia się dwóch pojazdów na umówionych warunkach. Jeden z pojazdów miał wcześniej pewne uszkodzenia, które najczęściej były szkodami parkingowymi. Właściciel tego pojazdu nie posiadał polisy AC (autocasco), a chciałby naprawić samochód z ubezpieczenia. W tym celu za ustaloną wcześniej opłatą umawia się z kierowcą innego auta, żeby zlikwidować powstałą szkodę z jego polisy OC;
- **wyłudzenia na dużą skalę**, dotyczą zazwyczaj drogich samochodów, np. marki Audi, BMW, Mercedes o wartości 300–600 tys. zł. Wtedy z zagranicy sprowadzane są uszkodzone pojazdy (aby nie można było sprawdzić ich historii szkodowej), zakupione za ok. 100–200 tys. zł i zgłaszane są fikcyjne szkody do ubezpieczyciela. Ten typ wyłudzeń dotyczy zorganizowanych grup przestępczych, które traktują to jako zawód zapewniający wysokie dochody.

Wśród sposobów wyłudzeń zakłady ubezpieczeń zauważają powrót oszustów do tradycyjnych, pozornie zapomnianych metod[35]. Jedną z nich jest metoda polegająca na celowym spowodowaniu szkody. Jej częstą odmianą, stosowaną przez wyspecjalizowanych sprawców, są szkody na rondach i roz-

[35] *Raport Polskiej Izby Ubezpieczeń o przestępczości ubezpieczeniowej w 2016 roku,* https://piu.org.pl/wp-content/uploads/2016/10/Raport-roczny-PIU-2016-w-wersji-PDF.pdf (dostęp: 20.08.2019).

budowanych skrzyżowaniach dużych miast (np. wyreżyserowane szkody na rondach). Proceder polega na wielokrotnym pokonywaniu ronda samochodem aż do momentu, gdy nadarzy się okazja „złapania" tzw. „dawcy polisy". Sprawcy kolizji wykorzystują błędy i dekoncentrację innych kierowców i celowo doprowadzają do kolizji w taki sposób, aby być stroną poszkodowaną. Następnie samochody – generatory szkód – są prowizorycznie naprawiane i ponownie wykorzystywane do tego procederu wyłudzeń.

Znane w Polsce wyłudzenia nienależnych odszkodowań miały miejsce w latach 2009–2016 w Polsce południowej i polegały na seryjnych kolizjach drogowych. Sprawcy takich zdarzeń używali do tego tanich samochodów zarejestrowanych w Polsce oraz pojazdów drogich marek zarejestrowanych i ubezpieczonych w Niemczech, należących do osób pochodzących z Polski. Kierowca kierujący tanim samochodem, zarejestrowanym w Polsce, był sprawcą takiej upozorowanej kolizji. Przyznawał się policji do spowodowania kolizji, a wtedy właściciel pojazdu zarejestrowanego w Niemczech występował do ubezpieczyciela o odszkodowanie. W ten sposób przestępcy zarabiali na zawyżaniu wartości spowodowanej szkody.

Co istotne, osoby kierujące takimi procederami są najczęściej osobami, które pośredniczą w likwidacji szkód i przewodzą zorganizowanej grupie przestępczej, składającej się z przedsiębiorców prowadzących warsztaty mechaniki pojazdowej, blacharstwa, lakiernictwa, holowników i dostawców części. Zadaniem takiej grupy jest uczestniczenie w pozorowanych kolizjach i szukanie tzw. „słupów", które będą chciały „wypożyczyć" swój samochód do pozorowanej kolizji.

Grupy przestępcze do celowych kolizji pojazdów o drogich częściach zamiennych bez możliwości zastosowania zamienników masowo wykorzystują pojazdy luksusowe sprowadzone zza granicy (np. z USA) w stanie całkowitego zniszczenia (np. po pożarze lub poważnym wypadku). Taki pojazd poddawany jest rzekomej naprawie, aby ponownie wprowadzić go do obrotu i następnie wykorzystać jako generator roszczeń.

Nowe metody wyłudzania odszkodowań komunikacyjnych określane są następującymi pojęciami:

- **car for crash** (samochód potrzebny do spowodowania zdarzenia faktycznego);

- **slash for crash** (miganie światłami) i wymuszenie na osobie kierującej pojazdem wyjazdu np. na rondzie czy drodze podporządkowanej, aby ostatecznie uderzyć w jej pojazd. Nawet obecność policji na miejscu zdarzenia uniemożliwia ustalenie faktycznego sprawcy wypadku, ponieważ wymuszający zdarzenie daje sygnał kierowcy światłami pod pretekstem wpuszczania kierowcy, aby ostatecznie uderzyć w jego pojazd. W takiej sytuacji trudno jest udowodnić wymuszenie zdarzenia i stanowisko policji na miejscu zdarzenia jest jednoznaczne, czyli osoba, która wyjechała popełniła wykroczenie i jest karana mandatem.

Kolejna metoda wyłudzania odszkodowań z ubezpieczeń komunikacyjnych związana jest z panującym w Polsce trendem, że drogie samochody nabywają głównie młode osoby, które w momencie kupowania pojazdu nie biorą pod uwagę, że zdarzenie może mieć miejsce i dlatego nie wykupują ubezpieczenia AC. Dlatego jak wydarzy się wypadek, poszukują osoby, która będzie w stanie napisać oświadczenie o spowodowaniu takiego zdarzenia i wtedy dorabiana jest cała historia zaistniałej sytuacji według dwóch możliwości:

1. Zdarzenie miało miejsce jako szkoda kontaktowa polegająca na upozorowanym uderzeniu w samochód, ale z dużo mniejszą siłą (mniejsza odległość, mniejsza prędkość), dla wykazania korelacji pomiędzy pojazdami.
2. Szkoda bezkontaktowa polegająca na zajechaniu, czyli wymuszeniu manewru obronnego kierowcy i następnie uderzeniu np. w drzewo, budynek, ogrodzenie. Tego typu szkody mają charakter wątpliwy i obejmuje je skomplikowana ścieżka likwidacji.

Jako przykład w przeprowadzonym wywiadzie z pracownikiem multiagencji podano nieuczciwych klientów, których suma szkód wszystkich zdarzeń wnosiła 200 tys zł. i była pozorowana na rondach. W ocenie ubezpieczyciela było to zjawisko regularne, traktowane przez nich jako stałe źródło dochodu. W związku z tym informacja została skierowana do organów ścigania.

Kolejnym zjawiskiem, które dotyczy większości Towarzystw Ubezpieczeniowych, jest sytuacja, kiedy zachodzi faktyczne zdarzenie drogowe i do sprawców zdarzenia docierają pełnomocnicy, którzy prowadzą kancelarie specjalizujące się w dochodzeniu roszczeń w imieniu klientów. Informacje o zaistnieniu zdarzenia docierają do takich kancelarii najczęściej ze szpitali, od kierowców karetek pogotowia itd. Jako przykład można podać zdarzenie,

kiedy ubezpieczony nie zachowuje ostrożności i wjeżdża pod nadjeżdżający pociąg. Po zdarzeniu zostały zgłoszone przez pełnomocników dwie szkody osobowe np. o łącznej wartości 60 tys. zł. W toku postepowania likwidacyjnego ubezpieczyciel przedstawił nagranie monitoringu z wnętrza pociągu oraz z tego, co działo się na zewnątrz pociągu. Przedstawiony monitoring jest podstawą udowodnienia przez ubezpieczyciela, że szkoda osobowa nie mogła mieć miejsca, gdyż pociąg hamował bardzo delikatnie. Zaistniała także dodatkowa sprzyjająca dla ubezpieczyciela okoliczność ujęta w monitoringu, że w czasie hamowania jedna z osób podróżująca pociągiem korzystała z telefonu komórkowego, który położyła na kolanie i telefon nie upadł. W związku z tym stwierdzono, że nie mogła zadziałać żadna siła, która mogła spowodować uszkodzenie np. odcinka kręgosłupa szyjnego czy innej części ciała – jakie podawane było przez poszkodowanego.

Ubezpieczyciele informują o szybkim wzroście wartości szkód osobowych. Dotyczy to powiększania deklarowanego zakresu uszkodzeń ciała w przypadku urazów, symulowania stanów psychicznych wynikających z rzekomo doznanego szoku pourazowego i powiększania liczby poszkodowanych w wypadku poprzez składanie fałszywych deklaracji. Najpopularniejsze dolegliwości wymieniane w roszczeniach związane są z uszkodzeniem szyjnego odcinka kręgosłupa, bólami głowy, depresjami powypadkowymi.

Sposoby markowania zdarzeń, aby wyłudzić nienależne odszkodowania, są coraz bardziej inteligentne. Jednak wielu ze sprawców nie bierze pod uwagę, że łatwo jest je wykryć. Na przykład w przypadku samochodu, który ma ściśle określone właściwości, określoną strukturę, co wpływa na łatwość odtworzenia wzajemności uszkodzeń pomiędzy pojazdami. Jednym ze sposobów umożliwiających prawdziwą rekonstrukcję zdarzenia pojazdów jest korzystanie ze specjalnego programu komputerowego, który jest w stanie wskazać, w jaki sposób samochody przemieszczały się w czasie wypadku. Oprócz tego wyłudzający odszkodowania muszą mieć świadomość, że samochód ma pewne wymiary, koła są w określonych miejscach względem nadwozia, dlatego łatwo jest stwierdzić, czy ślady, jakie są na pojeździe, są śladami związanymi ze zdarzeniem czy z innym faktem.

Kolejną metodą wyłudzeń nienależnych odszkodowań jest celowe uszkodzenia drogich elementów szklanych w pojazdach, np. szyb czołowych. Najczęściej dokonuje się to przy współudziale likwidatora dokonującego

oględziny i polega na wykorzystaniu kawałka cienkiego mydła z ostrą krawędzią, którym wykonuje się cienką rysę na szybie. Następnie wykonywane są zdjęcia szkody – pęknięcia szyby i w ostateczności wymiana szyby.

Jednym z najczęściej wykrywanych przestępstw ubezpieczeniowych jest p**owiększanie szkód po wypadku** przez właścicieli auta, którzy celowo niszcząc swój samochód (uderzenia w karoserię, rozbicie szyby, urywanie elementów zewnętrznych, np. lusterek), próbują zawyżyć wysokość odszkodowania. Oprócz tego niektórzy z kierowców dopisują do oświadczenia strat elementy, które zostały uszkodzone jeszcze przed wypadkiem, jak telefon komórkowy. W ten sposób liczą na dodatkowe środki finansowe z odszkodowania. Rzeczoznawcy ubezpieczeniowi mają jednak duże doświadczenie w rozpoznawaniu uszkodzeń. Większość prób oszustwa związanych z powiększeniem szkody udaje się wykryć na wczesnym etapie postępowania likwidacyjnego.

Sposobem wyłudzenia nienależnych odszkodowań jest także fałszowanie dokumentów – np. faktur za likwidację szkody. W związku z tym zakłady ubezpieczeń nierzadko przyznają wiarygodność i uczciwość autoryzowanym serwisom naprawczym, względem zaś serwisów nieautoryzowanych stosują domniemanie winy. Efektem tego jest wymóg udowodnienia przez roszczącego, że wybrany przez niego serwis naprawczy nie prowadzi działalności przestępczej i nie próbuje wyłudzić nienależnych mu kwot. Dzieje się tak, mimo iż roszczący nie ma ku temu żadnych narzędzi, a samo żądanie zakładu ubezpieczeń w tym zakresie nie posiada co do zasady umocowania prawnego[36]. Dlatego też nierzadko zdarza się, że wobec niedostarczenia faktur źródłowych, pomimo niewykazania przez ubezpieczyciela faktu użycia do naprawy innych części niż wskazane w fakturze naprawy, zakład ubezpieczeń wypłaca jednak kwoty niższe, tj. ustalone po dokonaniu korekt tej faktury. W ostatecznym rozrachunku praktyki te prowadzą do pokrzywdzenia osób uprawnionych do odszkodowania poprzez jego pomniejszenie. Nieuznawanie bowiem przez zakład ubezpieczeń pełnej kwoty należnej warsztatowi oznacza *de facto* przerzucenie na poszkodowanego części kosztów związanych

[36] T. Młynarski, *Żądanie przez zakłady ubezpieczeń w związku z likwidacją szkód komunikacyjnych faktur źródłowych zakupu części zamiennych,* https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Tomasz_Mlynarski___Zadanie_przez_zaklady_ubezpieczen_w_zwiazku_z_likwidacja_szkod_komunikacyjnych_faktur_zrodlowych_zaku__20749 (dostęp: 21.08.2019).

z likwidowaniem poniesionej przez niego szkody, gdyż zakłady naprawcze, wobec pokrycia przez ubezpieczyciela jedynie części tych kosztów, występują do samych poszkodowanych o zapłatę reszty należności. W przypadku obowiązkowego ubezpieczenia OC posiadaczy pojazdów mechanicznych wartość wszelkich czynności, których podjęcie jest niezbędne w procesie dokonywania naprawy, powinna odzwierciedlać ceny faktycznie obserwowane na rynku lokalnym, gdyż dopiero wówczas odszkodowanie będzie równe poniesionej szkodzie. Orzeczenie Sądu Najwyższego z dnia 16 czerwca 2003 r. (sygn. akt III CZP 32/03)[37] jasno stwierdza, iż nie można w tym kontekście mówić o cenach uśrednionych, lecz stosowanych w indywidualnej naprawie dokonywanej w wybranym przez poszkodowanego zakładzie naprawczym. Tymczasem ceny zawarte w systemach takich jak Eurotax, czy Audatex, będących podstawą wyliczeń dokonywanych przez ubezpieczycieli – w tym korekt faktur stwierdzających koszt naprawy – są właśnie cenami uśrednionymi. W przypadku zaakceptowania przez ubezpieczyciela zasadności i sposobu dokonania naprawy ubezpieczyciel nie powinien kwestionować wysokości tych kosztów. Jest to także równoznaczne z przyznaniem poszkodowanemu prawa do swobodnego wyboru zakładu naprawczego, z którego usług chce skorzystać. Praktyka zakładów ubezpieczeń polegająca na kwestionowaniu kosztów naprawy opartych na domniemaniu próby wyłudzenia jest krzywdząca zarówno dla zakładów naprawczych, jak i poszkodowanych, i w ostateczności jest przyczyną naruszenia zawartej w art. 361 § 2 k.c. zasady pełnego odszkodowania[38].

Kolejnym sposobem fałszowania dokumentów jest proceder dotyczący przedłużania ubezpieczenia OC, ponieważ brak jego ciągłości jest bardzo surowo karany. Zgodnie z obowiązującymi przepisami[39] **polisę ubezpieczeniową musi posiadać każdy zarejestrowany samochód**. Maksymalna

[37] Uchwała z dnia 13 czerwca 2003 r., III CZP 32/03, http://www.sn.pl/sites/orzecznictwo/Orzeczenia1/III%20CZP%2032-03.pdf (dostęp: 1.09.2019).

[38] E. Kiziewicz, *Żądanie przez zakład ubezpieczeń od poszkodowanych lub właścicieli warsztatów faktur stwierdzających rodzaj i źródło nabycia części zamiennych stosowanych przy naprawie pojazdu,* https://rf.gov.pl/najczestsze-pytania-i-odpowiedzi/Zadanie_przez_zaklad_ubezpieczen_od_poszkodowanych_lub_wlascicieli_warsztatow_faktur_stwierdzajacych_rodzaj_i_zrodlo_nab__20881 (dostęp: 21.08.2019).

[39] *Ustawa z dnia 22 maja 2003 roku o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. 2003 Nr 124 poz. 1152).*

wysokość kary dla samochodu osobowego wynosi w 2019 r. 4500 zł[40]. Wielu kierowców zapominając o konieczności przedłużenia ubezpieczenia OC, próbuje wymusić na ubezpieczycielu dokonanie ubezpieczenia z datą wstecz, aby ciągłość była zachowana.

Innym nadużyciem w ubezpieczeniach komunikacyjnych jest korzystanie z krótkoterminowej polisy OC (na okres nie krótszy niż 30 dni), która wystawiana jest w szczególnych okolicznościach, określonych w ustawie o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych[41]. Zgodnie z ustawą nie dotyczy ona osób czy firm, które mają normalny pojazd (nie historyczny i nie wolnobieżny), zarejestrowany na stałe w Polsce. Polisa może być zawarta np. wtedy, gdy sprowadzany jest samochód z zagranicy i należy go zarejestrować w polskim urzędzie – na tę procedurę jest przeznaczone 30 dni. Szczególne możliwości, jeżeli o chodzi o krótkoterminowe polisy OC, mają komisy samochodowe, gdyż dotyczą one m.in. ochrony aut pozostawionych w komisach i są znacznie tańsze od standardowej polisy OC. Natomiast nie można jej wykorzystywać jako sposobu na obniżenie składki za normalny pojazd (średni koszt takiego „komisowego" ubezpieczenia to ok. 50 zł miesięcznie). Taka niska kwota wynika z tego, że ten rodzaj polisy jest przeznaczony dla podmiotów prowadzących działalność komisową, a nie osób fizycznych (ubezpieczyciele nie uwzględniają historii szkodowej właściciela samochodu). W ciągu roku w taki sposób można „zaoszczędzić" nawet kilka tysięcy złotych. Jeżeli pojawiają się sytuacje, w których pośrednik sprzedaje ubezpieczenie krótkoterminowe osobie nieuprawnionej, czyli z takiego OC korzysta zwykły kierowca (zwłaszcza mający wysoką szkodowość na swoim koncie), a nie komis samochodowy, to oznacza poświadczenie nieprawdy (zgodnie z art. 271 k.k.[42] za tego typu działanie grozi kara od trzech miesięcy do pięciu lat pozbawienia wolności).

[40] Ubezpieczeniowy Fundusz Gwarancyjny, www.ufg.pl (dostęp: 2.09.2019).

[41] *Ustawa z dnia 22 maja 2003 roku o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. 2003 Nr 124 poz. 1152).*

[42] *Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny (Dz.U. 1997 Nr 88 poz. 553).*

5. Przykład likwidacji szkody przez ubezpieczyciela – studium przypadku (wywiad z właścicielem auta biorącego udział w zdarzeniu)

W czasie wyjazdu służbowego na trasie Polska-Węgry, na autostradzie w Czechach miało miejsce zdarzenie z udziałem polskiego kierowcy samochodu marki audi A4, który jadąc za półciężarówką, najechał na leżący na drodze plastik. Pod wpływem przejeżdżającej półciężarówki został on poderwany w górę, co spowodowało dostanie się go pod nadkole samochodu audi. Kierowca samochodu audi A4 nie zatrzymał się na miejscu zdarzenia na autostradzie, ponieważ sądził, że nic się nie stało i mógł dalej jechać. Zatrzymał się na najbliższym parkingu i wtedy dokonał oględzin auta oraz wykonał zdjęcia uszkodzeń samochodu. W ich wyniku okazało się, że w samochodzie jest wygięty błotnik oraz wyrwany z gniazda halogen w zderzaku, uszkodzona została klatka wentylacyjna. W związku z tym, nie znając sprawcy zdarzenia, kierowca zgłosił do ubezpieczyciela szkodę online, podając parametry samochodu i przesyłając zrobione zdjęcia szkody. Zachował się więc zgodnie z zapisami ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych[43], według których osoba objęta ubezpieczeniem obowiązkowym, uczestnicząca w zdarzeniu nim objętym, jest obowiązana m.in. do niezwłocznego powiadomienia o zdarzeniu zakładu ubezpieczeń, udzielając mu niezbędnych wyjaśnień i przekazując posiadane informacje. Zawiadomienie ubezpieczyciela o zajściu zdarzenia losowego objętego ochroną ubezpieczeniową (wypadku ubezpieczeniowego) rozpoczęło tzw. postępowanie likwidacyjne prowadzone przez zakład ubezpieczeń. Celem tego postępowania było ustalenie stanu faktycznego zdarzenia, zasadności zgłoszonych roszczeń i wysokości świadczenia.

Zakład Ubezpieczeń na podstawie zgłoszenia i załączonych zdjęć dokonał wyceny likwidacji tej szkody, ustalając kosztorys na kwotę 2500 zł. Najprawdopodobniej szkoda została wyceniona, biorąc pod uwagę, że do jej naprawy posłużą używane części zamienne, bez względu na kolor auta i jego lata. W takiej sytuacji kierowca mógł odebrać gotówkę i we własnym zakresie

[43] *Ustawa z dnia 22 maja 2003 roku o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. 2003 Nr 123 poz. 1152)* (art. 16 ust. 2).

dokonać usunięcia szkody w dowolnym warsztacie. Niektórzy kierowcy korzystają z takiej formy likwidacji szkody, kiedy mają możliwość naprawienia jej we własnym zakresie. Może to być w takim przypadku tańsze, a nawet część środków od ubezpieczyciela może pozostać u poszkodowanego.

Natomiast w tym przypadku właściciel auta zdecydował o likwidacji szkody w sposób bezgotówkowy w autoryzowanym serwisie, ponieważ zależało mu na jakości wykonanej usługi (jest to czteroletnie auto). Ze względu na to, że auto jest w leasingu w Idea Getin Leasing, to firma leasingowa po zgłoszeniu szkody, wskazała konkretny serwis likwidacji szkody, który dokonał oględzin samochodu przy współudziale właściciela i stwierdził, że koszt likwidacji szkody będzie dużo wyższy niż wycena dokonana przez ubezpieczyciela. Autoryzowany serwis sporządził kosztorys likwidacji szkody i wysłał go do ubezpieczyciela. Ostatecznie ubezpieczyciel dokonał akceptacji kosztorysu na wskazaną wyższą kwotę, uwzględniając demontaż uszkodzonych elementów samochodu. Właściciel auta oczekuje informacji od autoryzowanego serwisu o propozycji terminu naprawy auta.

W przedstawionej sytuacji istnieje możliwość dokonania przez autoryzowany serwis zawyżenia kosztorysu likwidacji szkody o kwotę dodatkowych napraw, jakie wskaże kierowca, bądź zawyżenia jej o kwotę, która może „pozostać" w serwisie. Z całą pewnością w przypadku wykazania przez zakład ubezpieczeń próby wyłudzenia ze strony serwisu-warsztatu zakład ubezpieczeń powinien zawiadomić o tym fakcie prokuraturę. Oprócz tego, gdy zaistnieje uzasadnione podejrzenie udziału w tym procederze także poszkodowanego, zawiadomienie powinno obejmować również i tę okoliczność. Jednak przedstawienie ubezpieczycielowi kosztorysu do akceptacji jest formą weryfikacji poprawności i zasadności wyceny likwidacji szkody.

6. Metody zapobiegania wyłudzeniom odszkodowań w ubezpieczeniach komunikacyjnych

Wyłudzenia odszkodowań są istotnym problemem na polskim rynku, dlatego ubezpieczyciele podejmują działania na walkę z przestępczością ubezpieczeniową, wprowadzając nowoczesne rozwiązania, które podnoszą skuteczność wykrywania przestępstw. Rozróżnienie między innowacjami procesowymi

i produktowymi w usługach ubezpieczeniowych jest skomplikowane ze względu na istotę usług. Przyjmuje się, że innowacją produktową jest doskonalenie lub wprowadzenie nowej usługi ubezpieczeniowej na rynek, innowacją procesową zaś rozwój nowego sposobu dostarczania usług ubezpieczeniowych[44]. Wśród metod zapobiegania przestępczości w obszarze ubezpieczeń komunikacyjnych można wymienić innowacje produktowe o charakterze inkrementalnym, czyli doskonalącym i poszerzającym istniejące rozwiązania, lub o charakterze transformacyjnym, dotyczące zmian i nowości bardziej radykalnych, oraz innowacje procesowe, np. poprzez wprowadzenie likwidacji szkód przez Internet.

W obliczu cyfrowej transformacji (czwartej rewolucji przemysłowej) wykorzystanie nowoczesnych technologii, zarówno jeśli chodzi o lepsze szacowanie ryzyka, jak i nowe kanały komunikacji z klientem, przyczyni się do zapobiegania przestępczości w obszarze ubezpieczeń komunikacyjnych. Wśród innowacji produktowych i procesowych można wymienić:

1. Stworzenie w instytucjach ubezpieczeniowych komórek (przynajmniej 1–2 osoby) do spraw zwalczania przestępczości.
2. Stworzenie banku danych (wzorem rozwiązania skandynawskiego i amerykańskiego) o mandatach, przeglądach technicznych pojazdów, co umożliwi lepszą ocenę ryzyka i zróżnicowanie składek dla poszczególnych kierowców.
3. Stworzenie produktu ubezpieczeniowego w taki sposób, aby wprowadzić zależności korelacyjne pomiędzy np. płaconymi mandatami czy niebezpieczną jazdą, a wysokością składki ubezpieczeniowej. Może to mieć także dodatkowy efekt w postaci poprawy bezpieczeństwa na drogach.
4. Zautomatyzowanie przekazywania informacji o kierowcach i pojazdach, co zapewni m.in. łatwiejsze wykrycie kierowców jeżdżących bez obowiązkowego ubezpieczenia OC.
5. Zwiększenie poziomu wykorzystania wymiany informacji, analiz statystycznych i dostępnych danych o korzystających z ubezpieczeń komunikacyjnych, gdyż nie jest on jeszcze na polskim rynku satysfakcjonujący.

[44] T.H. Bednarczyk, A. Jańska, *Innowacje produktowe i procesowe w obszarze ubezpieczeń majątkowych dla osób fizycznych,* „Oeconomia" 2015, nr 4, s. 47.

6. Wypracowanie modelu współpracy zakładów ubezpieczeń, organów ścigania i innych podmiotów i instytucji rynku ubezpieczeniowego oraz państwa w obszarze zmniejszenia, bądź likwidacji zjawiska przestępczości ubezpieczeniowej (obecnie nie ma współpracy, jest rywalizacja np. pomiędzy zakładami ubezpieczeń – walka o klienta)[45]. Wspólne działanie wszystkich jest konieczne.
7. Wykorzystanie nowoczesnych i szybkich kanałów komunikacji z klientem, np. czat, który jest kanałem tanim, ale za to szybkim. Może on wspierać inne kanały komunikacji m.in. e-mail. Kanały komunikacji potrzebne są, gdy ubezpieczyciel chce skontaktować się z klientem (np. e-mail), a inne (np. (telefon, wideoczat, spotkanie z agentem), gdy klient ma problem i zgłasza się do ubezpieczyciela.
8. Skuteczne napiętnowanie osób i instytucji dokonujących procederów wyłudzeń polegające m.in. przekazywaniu przez ubezpieczyciela, który wykrył wyłudzenia danej osoby, informacji do odpowiednich organów i instytucji. W takiej sytuacji wyłudzający może mieć problem np. z otrzymaniem kredytu, a kolejne ubezpieczenie dla niego powinno kosztować dwa razy więcej.
9. Stworzenie dostępnego dla każdego obywatela rejestru wyłudzających ubezpieczenia (dla zlikwidowania akceptacji społecznej takiego zachowania) – zagrożenie utratą czci i dobrego imienia.
10. Ujawnianie sposobów, schematów, modeli działań przestępczych, podejrzanych zdarzeń czy sieci powiązań między zdarzeniami w branży ubezpieczeń komunikacyjnych przez Ośrodek Informacji Ubezpieczeniowego Funduszu Gwarancyjnego w celu ułatwienia zakładom ubezpieczeń i organom ścigania prowadzenia postępowań w tym zakresie.
11. Zapobieganie przestępczości ubezpieczeniowej w zakresie fałszowania faktur likwidacji szkody poprzez ściślejszą współpracę zakładów

[45] Dyrektywa IDD – preambuła pkt. 37: „Dla ochrony klientów oraz zapewnienia prawidłowej działalności ubezpieczeniowej i reasekuracyjnej na rynku wewnętrznym zasadnicze znaczenie ma współpraca i wymiana informacji między właściwymi organami. Zarówno w procesie rejestracji, jak i w bieżących działaniach należy w szczególności wspierać wymianę informacji dotyczących dobrej reputacji oraz wiedzy zawodowej i kompetencjach zawodowych osób odpowiedzialnych za prowadzenie działalności dystrybutora ubezpieczeń lub reasekuracji".

ubezpieczeń z Policją i Prokuraturą, jak również organami kontroli podatkowej i skarbowej.

12. Edukacja społeczna poprzez podnoszenie świadomości ubezpieczeniowej, ponieważ występują duże deficyty w tym obszarze zarówno wśród klientów, pracowników zakładów ubezpieczeń, pośredników, pracowników prokuratury, jak i policji.

7. Podsumowanie

W opracowaniu przedstawiono wybrane rodzaje nadużyć dokonywane w ubezpieczeniach komunikacyjnych. Zaprezentowano również metody, które mogłyby tym procederom zapobiec bądź je ograniczyć. Jednak należy stwierdzić, że pokusa nadużyć w ubezpieczeniach jest coraz bardziej powszechna ze względu na możliwość zdobycia łatwych środków finansowych. Aby powstały warunki, w których może pojawić się pokusa nadużycia, potrzebne jest zawarcie umowy między dwiema stronami, z których jedna nie ponosi pełnej odpowiedzialności za swoje zachowanie ani nie jest w pełni kontrolowana, oraz kolejny warunek w postaci asymetrii informacji między stronami, czyli jedna nie wie, jak się zachowuje ta druga, więc nie może natychmiast przeciwstawić się nieuczciwym działaniom, które jej szkodzą. Oznacza to, że strona, która ma przewagę informacyjną, zaczyna dążyć do maksymalizacji własnych korzyści, kosztem drugiej strony, która jest niczego nieświadoma[46].

Zatem wszystkie metody, które mogą zapobiec procederom nadużyć dokonywanym w ubezpieczeniach komunikacyjnych oraz innych rodzajach ubezpieczeń, mogą być mało skuteczne, jeżeli korzystający z ubezpieczenia oraz ubezpieczyciel nie będą postępować uczciwie.

[46] P. Rosik, *Pokusa nadużyć spowszechniała*, „Obserwator Finansowy", 09.08.2018, https://www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/pokusa-naduzyc-spowszechniala/ (dostęp: 3.09.2019).

Bibliografia

Bednarczyk T.H., Jańska A., *Innowacje produktowe i procesowe w obszarze ubezpieczeń majątkowych dla osób fizycznych,* „Oeconomia", 2015, nr 4, s. 46–55.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń (wersja przekształcona).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2002/92/WE z dnia 9 grudnia 2002 r. w sprawie pośrednictwa ubezpieczeniowego (Dz. Urz. L9).

http://statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-kryminalne/7-wybranych-kategorii-p/kradziez-cudzej-rzeczy/kradziez-samochodu/122278, Kradziez-samochodu.html

Kiziewicz E., *Żądanie przez zakład ubezpieczeń od poszkodowanych lub właścicieli warsztatów faktur stwierdzających rodzaj i źródło nabycia części zamiennych stosowanych przy naprawie pojazdu,* https://rf.gov.pl/najczestsze-pytania-i-odpowiedzi/Zadanie_przez_zaklad_ubezpieczen_od_poszkodowanych_lub_wlascicieli_warsztatow_faktur_stwierdzajacych_rodzaj_i_zrodlo_nab__20881

Lewicka-Strzałecka A., *Moralność finansowa Polaków – raport z badań III edycja*, Gdańsk–Warszawa 2018, http://www.pte.pl/pliki/2/21/moralnosc_2018.pdf

Majewski P., *Analiza danych dotyczących przestępstw ujawnionych w 2016 roku w związku z działalnością zakładów ubezpieczeń- członków Polskiej Izby Ubezpieczeń,* Polska Izba Ubezpieczeń, Warszawa 2017.

Młynarski T., *Żądanie przez zakłady ubezpieczeń w związku z likwidacją szkód komunikacyjnych faktur źródłowych zakupu części zamiennych,* https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Tomasz_Mlynarski___Zadanie_przez_zaklady_ubezpieczen_w_zwiazku_z_likwidacja_szkod_komunikacyjnych_faktur_zrodlowych_zaku__20749

Raport z badania rynku ubezpieczeń komunikacyjnych, Urząd Ochrony Konkurencji i Konsumentów, Departament Analiz Rynku, Warszawa 2018.

Raport Polskiej Izby Ubezpieczeń o przestępczości ubezpieczeniowej w 2016 roku, https://piu.org.pl/wp-content/uploads/2016/10/Raport-roczny-PIU-2016-w-wersji-PDF.pdf

Rosik P., *Pokusa nadużyć spowszechniała*, „Obserwator Finansowy", 09.08.2018, https://www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/pokusa-naduzyc-spowszechniala/

Rozporządzenia Rady Ministrów z dnia 14 września 2018 roku w sprawie programu badań statystycznych *statystyki* publicznej *na rok 2019 (Dz.U. 2018, poz. 2103).*

Sprawozdanie Rzecznika Finansowego za 2018 r., https://rf.gov.pl/files/22980__5328__Sprawozdanie_Rzecznika_Finansowego_za_2018_r_.pdf

Talarek J., *Przestępczość w ubezpieczeniach komunikacyjnych w Polsce na tle wybranych krajów europejskich*, Gazeta ubezpieczeniowa on-line. http://www.gu.com.pl/

index.php?option=com_content&view=article&id=1578&catid=124:ubezpieczenia-majtkowe&Itemid=154
Ubea.pl, http://www.gu.com.pl/index.php?option=com_content&view=article&id=69049:ubeapl-skargi-a-udzia-w-rynku&catid=107:rynek-ubezpiecze&Itemid=106
Uchwała z dnia 13 czerwca 2003 r., III CZP 32/03, http://www.sn.pl/sites/orzecznictwo/Orzeczenia1/III%20CZP%2032-03.pdf
Ustawa z dnia 11 września 2015 roku o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. 2015 poz. 1844 z późn. zm.).
Ustawa z dnia 15 grudnia 2017 roku o dystrybucji ubezpieczeń (Dz.U. 2017 poz. 2486).
Ustawa z dnia 22 maja 2003 roku o nadzorze ubezpieczeniowym i emerytalnym (Dz.U. 2003 Nr 124 poz. 1153 z późn. zm.).
Ustawa z dnia 5 sierpnia 2015 roku o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym (Dz.U. 2015 poz. 1348 z późn. zm.).
Ustawa z dnia 29 czerwca 1995 roku o statystyce publicznej (Dz.U. 2019 poz. 649 i 730).
Ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. 2018 poz. 473 z późn. zm.).
Ubezpieczeniowy Fundusz Gwarancyjny, www.ufg.pl
Wróblewski T., *Przestępczość ubezpieczeniowa – metody działania oraz sposoby zapobiegania w świetle ankiety Rzecznika Ubezpieczonych,* https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Tomasz_Wroblewski_-_Przestepczosc_ubezpieczeniowa_-_metody_dzialania_oraz_sposoby_zapobiegania_w_swietle_ankiety_Rzeczni__145

ROZDZIAŁ V

Czyny zabronione w zarządzaniu przedsiębiorstwem w kontekście relacji pracownik–pracodawca. Wybrane aspekty

MAREK BIELECKI[1]

1. Wprowadzenie

Proces zarządzania przedsiębiorstwem niesie wiele wyzwań zarówno dla pracodawców, jak i dla podmiotów pełniących ich rolę. Relacje panujące w stosunkach podwładny–przełożony odgrywają niebagatelną rolę w pozycji, jaką zajmuje dany zakład w stosunku do innych konkurencyjnych firm, jak również decydują o jego wewnętrznej „kondycji gospodarczej". Wzajemna koegzystencja podmiotów odpowiedzialnych za kierowanie przedsiębiorstwem oraz osób stanowiących tzw. „siłę roboczą" realizowana jest na wielu płaszczyznach. W grę wchodzą m.in.: relacje interpersonalne, uwarunkowania formalnoprawne czy interes ekonomiczny. W zależności od kontekstu każda z powyższych przesłanek może odgrywać kluczową rolę, decydującą o ostatecznym sukcesie realizowanego przedsięwzięcia.

W niniejszym opracowaniu analizie zostanie poddany każdy z wymienionych obszarów. Przedmiotem prowadzonych rozważań będzie głównie sytuacja jednostek tworzących strukturę danej zbiorowości, analizowana w kontekście interesu całej firmy. Punktem odniesienia dla prowadzonych badań będą m.in. przesłanki, które doprowadzają wszystkie podmioty występujące w strukturze przedsiębiorstwa do popełniania przestępstw. Z uwagi na zakres tematu opracowania w grę wchodzić będą przede wszystkim te występujące po stronie osób odpowiedzialnych za zarządzanie przedsiębiorstwem. Zostanie również zaprezentowany katalog czynów niedozwolonych, których

[1] Doktor habilitowany, profesor w Instytucie Prawa Akademii Sztuki Wojennej w Warszawie.

mogą dopuścić się zarówno pracodawcy, jak i pracownicy. Z uwagi zaś na rozwój technologiczny i pojawiające się w związku z tym nowe możliwości monitorowania i przeciwdziałania niepożądanym postawom ze strony pracowników omówienia wymaga ich sytuacja prawna w kontekście uprawnień przysługujących pracodawcy.

Przedstawione zostaną również propozycje, które mogą spowodować usprawnienie procesu kierowania przedsiębiorstwem pod kątem wyeliminowania potencjalnych przestępców i ich negatywnego postępowania.

2. Uwagi terminologiczne

Zanim zostaną poddane analizie szczegółowe zagadnienia, wyjaśnienia wymagają podstawowe pojęcia, które zostały użyte w tytule niniejszej pracy i ich zakres. Najwaniejszą kwestią, wokół której będą koncentrować dalsze ustalenia, jest wyjaśnienie zakresu określenia **czyn zabroniony**. Na gruncie obowiązujących regulacji pod tym pojęciem będą rozumiane przestępstwa oraz wykroczenia przeciwko prawom pracownika. Zarówno jedna, jak i druga kategoria wykazują typowe cechy, które warunkowane są istnieniem stosunku pracy. Po pierwsze swoisty jest przedmiot czynów zabronionych, którym z zasady są uprawnienia pracowników, głównie z zakresu indywidualnego prawa pracy. Wyjątek stanowią układy zbiorowe pracy. Ponadto regulacje dotyczące tych kategorii czynów zawarte są w ustawodawstwie z zakresu prawa pracy[2]. Należy podkreślić, że obowiązujący Kodeks karny (dalej k.k.) nie zawiera definicji przestępstwa. Można jednakże ją wyinterpretować na podstawie poszczególnych przepisów[3]. Na użytek niniejszego opracowania za **przestępstwo** należy uznać czyn (działanie, zaniechanie) człowieka, zabroniony przez ustawę pod groźbą kary jako zbrodnia lub występek, zawiniony umyślnie lub nieumyślnie oraz społecznie szkodliwy w stopniu wyższym niż znikomy[4]. Z kolei **wykroczenie przeciwko** prawom pracowniczym to czyn człowieka, bezprawny, karygodny, karalny i zawiniony, którego przedmiotem

[2] E. Wiszowata, *Wykroczenia przeciwko prawom pracownika*, Warszawa 2012, s. 7–9.

[3] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn.: Dz.U. z 2018 poz. 1600 ze zm.)*

[4] L. Gardocki, *Pojęcie przestępstwa i podziały przestępstw w polskim prawie karnym*, „Annales Universitatis Mariae Curie-Skłodowska", 2013, nr 2, s. 30.

ochrony są uprawnienia pracownicze. Może być popełniony tylko przez określone podmioty, z udziałem inspektora pracy[5]. **Niniejsze opracowanie w głównej mierze dotyczyć będzie przestępstw, które będą charakteryzować się m.in. znamionami określonymi w 218 § 1 a k.k.** Doprecyzowania wymaga również samo pojęcie zarządzania przedsiębiorstwem. Proces ten utożsamiany jest z kierowaniem zasobami ludzkimi, które **oznacza całokształt działań związanych z dysponowaniem posiadanymi zasobami ludzkimi przez daną organizację, podejmowanych dla osiągnięcia jej celów[6]. W procesie zarządzania zasobami ludzkimi można wyodrębnić m.in.: pozyskiwanie i dobór pracowników, motywację pracowników, edukację i rozwój pracowników, ocenę kwalifikacji i wyników pracowników oraz outplacment pracowników (monitorowane zwalniania pracowników)**[7].

Interesujący nas proces zarządzania zasobami ludzkimi dokonuje się w obrębie przedsiębiorstwa, pod określeniem którego kryje się podmiot gospodarczy, prowadzący na własny rachunek działalność produkcyjną lub usługową ukierunkowaną w celu osiągnięcia zysku[8]. Przedsiębiorstwa mogą przybierać różnorodne formy organizacyjno-prawne. Można wyodrębnić m.in. firmy jednoosobowe, spółki, przedsiębiorstwa państwowe oraz spółdzielnie. Z kolei spółki dzielą się na osobowe (jawne, partnerskie, komandytowe, komandytowo-akcyjne) i kapitałowe (z ograniczoną odpowiedzialnością, akcyjne).

Dla tematyki podejmowanej w niniejszym opracowaniu kluczowe znaczenie ma dookreślenie pracownika i pracodawcy, które to podmioty mogą dopuszczać się czynów zabronionych. **Definicja pracownika** została zawarta w art. 2 Kodeksu pracy (KP). Zgodnie z dyspozycją wyrażoną w tym przepisie jest to osoba zatrudniona na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę[9]. Należy jednakże zauważyć, że powyższe określenie nie koresponduje ze zwrotami, jakimi

---

[5] E. Wiszowata, *Wykroczenia przeciwko prawom pracownika…*, op. cit., s. 8.

[6] W. Golnau, M. Kalinowski, J. Litwin, *Zarządzanie zasobami ludzkimi*, Warszawa 2002, s. 19–21.

[7] A. Leleń, *Zarządzanie zasobami ludzkimi przedsiębiorstwa*, „Bezpieczeństwo i Technika Pożarnicza", 2011, nr 2, s. 31–42.

[8] T. Buczyńska, *Mikroekonomia*, Warszawa–Łódź 2017, s. 189.

[9] *Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn.: Dz.U. 2019 poz. 1040 ze zm.).*

posługuje się obowiązujący k.k., który w rozdziale XXVIII reguluje przestępstwa przeciwko prawom osób wykonujących pracę zarobkową. Jest to szersza kategoria w porównaniu z zakresem art. 2 KP z tego względu, że w jej obręb wchodzą również osoby zatrudnione na podstawie umów cywilno-prawnych. W niniejszym opracowaniu czyny niedozwolone, których może dopuścić się pracodawca lub osoba działająca w jego imieniu, będą odnoszone do podmiotów zatrudnionych na podstawie przepisów KP. Czynów niedozwolonych wobec osób wykonujących pracę zarobkową w procesie zarządzania przedsiębiorstwem może dopuścić się zarówno pracodawca, jak i osoba działająca w jego imieniu. Zgodnie z art. 3 KP **pracodawcą** jest jednostka organizacyjna, choćby nie posiadała osobowości prawnej, a także osoba fizyczna, jeżeli zatrudnia pracowników. Ponadto, jak stanowi art. 3 (1) § 1–2 KP, za pracodawcę czynności z zakresu prawa pracy dokonuje osoba lub organ zarządzający tą jednostką albo inna wyznaczona do tego osoba.

Jak podkreśla Sąd Najwyższy w jednym ze swoich orzeczeń, w odniesieniu do osób zarządzających konieczne jest stwierdzenie występowania dwóch elementów: uprawnienia do dokonywania czynności w sprawach z zakresu prawa pracy i pierwotny charakter tego uprawnienia[10]. Nie ma ponadto przeszkód, by osoba zarządzająca była jednocześnie zatrudniona na podstawie stosunku pracy lub umowy cywilnoprawnej[11]. Żeby działanie można było uznać za skuteczne, z oświadczenia pracodawcy musi jednoznacznie wynikać zakres upoważnienia, a osoba zainteresowana powinna wyrazić zgodę[12]. Sama forma oświadczenia uzależniona jest od wewnętrznych regulacji przyjętych w danej jednostce organizacyjnej. Dokonywanie czynności z zakresu prawa pracy przez pracodawcę, będącego jednostką organizacyjną, przez osobę lub organ zarządzający tą jednostką albo inną wyznaczoną osobą może nastąpić w każdy sposób, dostatecznie ujawniający wolę reprezentowanego pracodawcy i nie jest uzależnione od udzielenia takiej osobie pisemnego pełnomocnictwa[13]. Przez **czynności z zakresu prawa pracy**, które realizowane są przez

[10] Wyrok Sądu Najwyższego z dnia 3 kwietnia 2008 r. (II PK 288/07).

[11] Wyrok Sądu Najwyższego z dnia 25 listopada 2004 r. (I PK 42/04).

[12] Wyrok Sądu Najwyższego z dnia 20 września 2005 r. (II PK 412/04 – OSNP 2006/13-14/210).

[13] Wyrok Sądu Najwyższego z dnia 2 lutego 2001 r. (I PKN 226/00 – OSNAPIUS z 2002/20, poz. 488); Wyrok Sądu Najwyższego z dnia 7 grudnia 2012 r. (II PK 121/12 LEX nr 1284747).

pracodawcę oraz osobę występującą w jego imieniu, należy uznać wszystkie czynności prawne określone w przepisach regulujących stosunek pracy, a więc nawiązywanie i rozwiązywanie stosunku pracy, zmiany w umowach oraz ustalanie regulaminów pracy. Wyznaczenie w rozumieniu art. 3 (1) § 1 KP ma charakter generalny, a wyznaczona osoba może udzielać pełnomocnictwa innym osobom do poszczególnych czynności w zakresie prawa pracy[14].

Należy również zauważyć, że prawodawca przewiduje możliwość dokonywania czynności i ponoszenia z tego tytułu odpowiedzialności w imieniu tzw. podmiotów zbiorowych. Zgodnie z art. 2 ustawy o *odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary*, podmiotem zbiorowym jest osoba prawna, jednostka organizacyjna niemająca osobowości prawnej, której odrębne przepisy przyznają zdolność prawną, z wyłączeniem Skarbu Państwa, jednostek samorządu terytorialnego i ich związków, spółek handlowych z udziałem Skarbu Państwa, jednostek samorządu terytorialnego lub związku takich jednostek, spółek kapitałowych w organizacji, podmiotów w stanie likwidacji oraz przedsiębiorców niebędących osobami fizycznymi, a także zagranicznych jednostek organizacyjnych[15].

3. Korelacje praw i obowiązków pracownika i pracodawcy w procesie zarządzania przedsiębiorstwem

Relacje między pracownikiem, również osobą wykonującą pracę zarobkową, a pracodawcą bądź podmiotem reprezentującym go w procesie zarządzania opierają się na podstawowych zasadach zawartych zarówno w KP, jak i innych aktach normatywnych w szczególności w obowiązującej ustawie zasadniczej i prawie Unii Europejskiej.

Ich charakter dookreśla art. 22 § 1 KP, zgodnie z którym przez nawiązanie stosunku pracy, pracownik zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem w miejscu i czasie wyznaczonym przez pracodawcę. Pracodawca zaś ma zapewnić wynagrodzenie pracownikowi. Z kolei w umowie o dzieło przyjmujący zamówienie

[14] Ibid.

[15] *Ustawa z dnia 28 października 2008 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (tekst jedn.: Dz.U. 2019 poz. 628 ze zm.).*

zobowiązuje się do wykonania oznaczonego dzieła, a zamawiający do zapłaty (art. 627 k.c.)[16]. Przy umowie–zleceniu przyjmujący zobowiązuje się do dokonania określonej czynności prawnej dla dającego zlecenie (art. 734 § 1 k.c.).

Z uwagi na ograniczony zakres przewidziany dla niniejszego opracowania w głównej mierze należy zwrócić uwagę na podstawowe prawa i obowiązki stron zaangażowanych w proces zarządzania przedsiębiorstwem, które opierają się na regulacjach dotyczących stosunku pracy. **Nie sposób omawiać wszystkich zasad prawa pracy, dlatego też poniższy wybór będzie dotyczył tych, których nieprzestrzeganie wiąże się z możliwością popełniania czynów niedozwolonych związanych z zarządzaniem przedsiębiorstwem.**

Punktem wyjścia dla dalszych rozważań powinna stać się m.in. dyspozycja wyrażona w art. 218 § 1a k.k., zgodnie z którą: „Kto, wykonując czynności w sprawach z zakresu prawa pracy i ubezpieczeń społecznych, złośliwie lub uporczywie narusza prawa pracownika wynikające ze stosunku pracy lub ubezpieczenia społecznego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Zgodnie z prezentowanym w doktrynie poglądem złośliwe zachowanie w stosunku do pracownika ma mieć na celu: wyrządzenie mu przykrości, poniżenie go, dokuczenie mu, zlekceważenie go bądź wyrządzenie krzywdy, której nie można racjonalnie uzasadnić[17]. Z kolei, żeby zostało spełnione znamię uporczywości, muszą zaistnieć dwa elementy. Po pierwsze jest to zła wola sprawcy. Po drugie to długotrwałość jego działania[18]. Żeby działanie wyczerpywało znamię długotrwałości powinno trwać przynamniej przez okres 3 miesięcy[19]. Osoba, która uporczywie narusza prawa pracownicze, cechuje się szczególnym nastawieniem psychicznym, które wyraża się w nieustępliwości, chęci postawienia na swoim oraz podtrzymywaniu własnego stanowiska na przekór ewentualnym próbom jego zmiany. Z kolei popełnienie wykroczeń przeciwko prawom pracowników regulują przepisy zawarte w art. 281–283 KP.

---

[16] *Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (tekst jedn.: Dz.U. 2018 poz. 1025 ze zm.)*.

[17] Wyrok Sądu Najwyższego z dnia 17 stycznia 2017 r. (WA 18/16 LEX nr 2203539).

[18] Wyrok Sądu Najwyższego z dnia 17 stycznia 2017 r. (WA 18/16 – LEX 2203539).

[19] Wyrok Sądu Okręgowego w Rzeszowie z dnia 24 października 2014 r. II KA 434/14 – LEX nr 1860417).

Z uwagi na to, że stosunek pracy jest stosunkiem zobowiązaniowym między pracownikiem i pracodawcą, w momencie zawarcia umowy o pracę powstają między stronami wzajemne prawa i obowiązki. Cechą charakterystyczną owego zobowiązania jest istnienie określonej dobrowolnej więzi prawnej, wyrażającej się w kierowniczej roli pracodawcy, determinującej w znacznym stopniu pozycję prawną pracownika, który pracując pod jego kierownictwem korzysta z szeregu uprawnień[20].

Pracodawca korzystając ze swoich uprawnień, może wydawać pracownikowi polecenia dotyczące pracy, które służą konkretyzacji obowiązków pracownika. Tadeusz Zieliński i Ludwik Florek wyodrębniają m.in. polecenia: określające zadania, jakie pracownik powinien wykonać; określające sposób, miejsce i termin wykonania przydzielonych zadań oraz konkretyzujące czas świadczenia pracy[21]. Powyższym uprawnieniom odpowiadają obowiązki pracownika określone w art.100 § 1 KP, zgodnie z którym pracownik zobowiązany jest stosować się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa. **Zarówno w literaturze przedmiotu, jak i w orzecznictwie, najwięcej kontrowersji wzbudza kwestia dopuszczalności odmowy przez pracownika wykonywania poleceń, które zostały wydane z naruszeniem przepisów prawa[22].** Tomasz Duraj omawia orzecznictwo Sądu Najwyższego (SN), w którym z jednej strony przyjmuje się, że pracownik odmawiający wykonania polecenia spełniającego wymogi określone w art. 100 § 1 KP naraża się na odpowiedzialność porządkową i materialną, a ponadto takie zachowanie może być podstawą wypowiedzenia umowy o pracę lub rozwiązania umowy bez wypowiedzenia[23]. W podobnym duchu wypowiada się Sąd Najwyższy, kiedy stwierdza, że wynikający z art. 100 KP obowiązek pracownika nie może być rozumiany w ten sposób, że jego krytyczny stosunek do wydanych mu poleceń służbowych zwalnia go z powinności ich wykonania. Ocena bowiem, czy zadanie objęte poleceniem służbowym jest

[20] J. Stelina (red.), *Stosunek pracy*, w: *Leksykon prawa pracy. 100 podstawowych pojęć*, Warszawa 2008, s. 268.

[21] L. Florek, L. Zieliński, *Prawo pracy*, Warszawa 1997, s. 142–143.

[22] T. Duraj, *Granice uprawnień kierowniczych pracodawcy w stosunku pracy*, „Zeszyty Prawnicze" 2013, nr 13 (2), s. 114 (s. 101–130) i przywołana tam literatura.

[23] Ibid., autor przywołuje m.in.: wyrok Sądu Najwyższego z dnia 15 października 1999 r. (I PKN 309/99 – OSNP 5/2001, poz. 147).

w interesie pracodawcy, zależy od kierownictwa zakładu. Odmienny pogląd prowadziłby do dezorganizacji pracy zakładu[24]. W wypowiedziach SN można również spotkać się ze stanowiskiem, że bezkrytyczne wykonywanie przez pracownika bezprawnych poleceń przełożonego może uzasadniać wypowiedzenie umowy o pracę[25].

W procesie zarządzania przedsiębiorstwem może dochodzić do sytuacji, kiedy polecenia wydawane przez pracodawcę lub osobę działającą w jego imieniu mogą wzbudzić u pracowników kontrowersje pod względem ich zgodności z prawem. Wydaje się, że w takich sytuacjach pracownik nie tylko ma prawo, ale wręcz ciąży na nim obowiązek wykonania polecenia, które ewidentnie narusza obowiązujące przepisy prawne. W szczególności należy zwrócić uwagę na te czynności, których wykonanie spowoduje popełnienie przestępstwa bądź wykroczenia. Niemniej jednak z taką sytuacją ma się do czynienia, jeżeli jest to ewidentne działanie *contra legem*. **W sytuacjach wątpliwych należałoby przewidzieć mechanizm polegający na tym, że pracownik przed wykonaniem zadania ma możliwość zwrócenia się do pracodawcy i zgłoszenia mu swoich obaw. Fakt ten powinien zostać odpowiednio udokumentowany na wypadek potencjalnych przyszłych oskarżeń kierowanych przeciw pracownikowi.**

Treść stosunku pracy obok możliwości wydawania pracownikowi wiążących poleceń determinuje również określone obowiązki, jakie spoczywają na pracodawcy, które korespondują z uprawnieniami pracowniczymi. Zgodnie z dyspozycją wyrażoną w art. 22 KP na pracodawcy spoczywa obowiązek zatrudnienia pracownika oraz wypłacenia mu wynagrodzenia za pracę. Zatrudnianie pracownika powinno dokonywać się zgodnie z jego kwalifikacjami i predyspozycjami do wykonywania zawodu. Pracodawca bądź inny podmiot zarządzający procesem produkcji nie może w związku z tym za wszelką cenę dążyć do obsadzania wolnych stanowisk. W sytuacji, kiedy zatrudnia się daną osobę bez sprawdzenia chociażby jej predyspozycji zdrowotnych, może dojść do tragedii. W dobie „braku rąk do pracy" pracodawca może celowo pomijać kwestie zdolności pracownika do wykonywania

[24] Wyrok Sądu Najwyższego z dnia 14 października 1977 r. (I PRN 136/77 – LEX nr 14431), tekst orzeczenia za: T. Duraj, *Granice uprawnień kierowniczych*…, op. cit.

[25] Wyrok Sądu Najwyższego z dnia 19 września 1997 r. (I PKN 244/87 – OSNP 12/98, poz. 358).

określonego zawodu. Należy zauważyć, że z powyższym obowiązkiem pracodawcy koresponduje prawo pracownika do wykonywania rodzaju pracy określonej w umowie. Dlatego też z jego strony powinno dojść do ewentualnego sprzeciwu wobec pracodawcy, który chce powierzyć mu do wykonania zadanie nieodpowiednie do jego predyspozycji. Przy zatrudnianiu pracownika na określonym stanowisku może również zaistnieć taka ewentualność, że to sam pracownik w procesie rekrutacji do danej firmy przedstawia fałszywe dokumenty potwierdzające jego przydatność do danej profesji. Ciężko wymagać od pracodawcy, aby szczegółowo analizował każdy przypadek, niemniej jednak, jeżeli chodzi o wykonywanie zawodu, w którym narażone może być zdrowie bądź życie pracownika, w razie jakichkolwiek wątpliwości powinien dołożyć wszelkich starań w ich wyjaśnieniu.

Obowiązek wypłacenia wynagrodzenia za pracę jest istotą stosunku pracy. Każdy pracodawca winien jest regularnie w ustalonych odstępach czasowych i w zależności od przyjętego sposobu wynagradzania wywiązać się z owej powinności. Korzystanie z pracy nieodpłatnej jest zabronione, a odmienne postanowienia umowne są nieważne. Również pracownik, którego podstawowym prawem jest otrzymywanie wynagrodzenia za pracę, nie może z niego zrezygnować[26].

Rodzaj podstawowych obowiązków pracodawcy, których nieprzestrzeganie może doprowadzić do popełniania przestępstw i innych czynów niedozwolonych, został określony w rozdziale II KP dotyczącym podstawowych zasad pracy. W procesie zarządzania przedsiębiorstwem może najczęściej dochodzić do naruszania następujących zasad: poszanowania godności i innych dóbr osobistych pracownika (art. 11 (1) KP); respektowania równych praw pracowników z tytułu jednakowego wypełnienia takich samych obowiązków, ze szczególnym uwzględnieniem równego traktowania mężczyzn i kobiet (art. 11 (2) KP); zakazu dyskryminacji w zatrudnieniu (art. 11 (3) KP); zapewnienia pracownikowi godziwego wynagrodzenia (art. 13 KP); respektowania prawa pracownika do wypoczynku (art. 14 KP); obowiązku zapewnienia pracownikom bezpiecznych i higienicznych warunków pracy (art. 15 KP). Nie jest to pełny katalog zasad zawartych w przepisach KP, jednakże ze względu na ograniczone rozmiary opracowania, konieczne było wskazanie tych, których

[26] L. Florek, L. Zieliński, *Prawo pracy*…, op. cit., s. 143.

nieprzestrzeganie, zdaniem autora, najczęściej doprowadza do popełniania przestępstw.

Pierwszą, a zarazem najtrudniejszą do sprecyzowania, jest **zasada respektowania godności pracownika i respektowania innych dóbr osobistych**. Poszanowanie godności pracownika jest następstwem regulacji zawartych w obowiązującej ustawie zasadniczej, która chroni wolności i prawa każdej istoty ludzkiej. Zgodnie z art. 30 Konstytucji przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Przyrodzoność owego prawa oznacza, że przynależy ona każdej jednostce niezależnie od jakichkolwiek okoliczności. Zatem pracownik, niezależnie od tego w jakiej sytuacji życiowej się znajduje, ma prawo do jej respektowania przez podmiot zarządzający jego pracą. W grę mogą wchodzić chociażby sytuacje zatrudniania osób, które pracują w okresie odbywania kary pozbawienia wolności. Poszanowanie i ochrona tego prawa jest obowiązkiem władz publicznych. Godność jest pojęciem nienormatywnym i zdecydowanie łatwiej wskazać jest przykłady, kiedy można ją naruszyć, niż dookreślić czym ona jest. Wedle stanowiska wymiaru sprawiedliwości godność utożsamiana jest z czcią wewnętrzną człowieka. Konkretyzuje się w poczuciu własnej wartości i oczekiwaniu szacunku ze strony innych ludzi. Naruszenie godności polega na ubliżeniu komuś lub na obraźliwym zachowaniu wobec niego[27]. Aby w procesie zarządzania zostało zapewnione poszanowanie godności pracowników, pracodawca bądź podmiot działający w jego imieniu powinien bezwzględnie reagować na wszelkie próby poniżania czy innego naruszania godności swoich podwładnych, zarówno ze strony ich przełożonych, jak i współpracowników. Obecnie problem ów zyskuje na aktualności w związku z zatrudnianiem w przedsiębiorstwach osób należących do różnych nacji czy religii. Wydaje się, że działania zarządzających powinny pójść nie tylko w kierunku bezwzględnego respektowania praw pracowników, ale również organizowania różnych form wzajemnej integracji. W przypadku zatrudniania osób reprezentujących różne kultury w zakładach powinna być wyodrębniona komórka, która będzie organizowała przedsięwzięcia polegające na zacieśnieniu relacji na wszystkich poziomach organizacyjnych przedsiębiorstwa.

[27] Wyrok Sądu Okręgowego w Koszalinie z dnia 11 lutego 2010 r. (I C 639/09 – LEX nr 1713915).

Zasada poszanowania godności pracownika koresponduje z **koniecznością ochrony jego dóbr osobistych**. W art. 23 Kodeksu cywilnego (k.c.), Ustawodawca przedstawia przykładowy katalog tych wartości, do których zalicza m.in.: zdrowie, wolność, cześć, swobodę sumienia, nazwisko lub pseudonim, wizerunek czy tajemnicę korespondencji. W procesie zarządzania przedsiębiorstwem może dochodzić do ich naruszenia zarówno na płaszczyźnie relacji wertykalnych (pracownik-pracodawca), jak i horyzontalnych (pracownik-pracownik). Nie sposób jest się odnieść w niniejszym tekście do wszystkich kategorii, jakie wymienia prawodawca w art. 23 k.c., niemniej jednak niektórym z nich należy poświęcić nieco więcej uwagi z powodu możliwości występowania potencjalnych zagrożeń dla praw pracowniczych.

Niewątpliwie poczynione powyżej spostrzeżenia, odnoszące się do odrębności kulturowej pracowników, zachowują swoją aktualność w procesie ochrony ich dóbr osobistych. W pierwszej kolejności mogą one stanowić przesłankę **do naruszenia ich wolności sumienia i religii, określanego również szerszym pojęciem wolności religijnej**. Zgodnie bowiem z art. 7 ustawy *o gwarancjach wolności sumienia wyznania* (u.g.w.s.w.). cudzoziemcy i bezpaństwowcy, przebywający na terytorium Rzeczypospolitej Polskiej, korzystają ze swych praw w tym zakresie na równi z obywatelami polskimi[28]. Podobnie jak godność osoby ludzkiej, tak również wolność religijna jest kategorią konstytucyjną. Ustrojodawca w art. 53 ust. 1 stanowi, że jest to prawo przysługujące każdej jednostce ludzkiej. Ponadto z uprawnień w tym zakresie mogą korzystać rodzice (art. 53 ust. 3), kościoły i inne związki wyznaniowe o uregulowanej sytuacji prawnej (art. 53 ust. 4) oraz dzieci w zależności od stopnia dojrzałości (art. 48 ust. 1). Z norm konstytucyjnych wynika, że wolność religijna obejmuje dwa aspekty: pozytywy, traktowany jako prawo do określonych zachowań, jak również aspekt negatywny – jako wolność od zachowań innych podmiotów. W aspekcie pozytywnym wolność religii obejmuje m.in.: „wolność wyznawania lub przyjmowania religii według własnego wyboru oraz uzewnętrzniania indywidualnie lub z innymi, publicznie lub prywatnie, swojej religii przez uprawianie kultu, modlitwę, uczestniczenie w obrzędach, praktykowanie i nauczanie. Wolność religii obejmuje także

[28] *Ustawa z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania (tekst jedn.: Dz.U. 2017 poz. 1153).*

posiadanie świątyń i innych miejsc kultu w zależności od potrzeb ludzi wierzących oraz prawo osób do korzystania z pomocy religijnej tam, gdzie się znajdują" (art. 53 ust. 2). Z kolei aspekt negatywny dotyczy zakazu zmuszania kogokolwiek do uczestniczenia albo do nieuczestniczenia w praktykach religijnych (art. 53 ust. 6) oraz zakazu zmuszania kogokolwiek przez organy władzy publicznej do ujawniania swojego światopoglądu, przekonań religijnych lub wyznania (art. 53 ust. 7). Jak zauważa Artur Mezglewski, wolność religijna należy przede wszystkim do świadomości ludzkiej. Same zaś przekonania religijne rodzą się i kształtują w sferze wewnętrznej człowieka, jednakże w głównej mierze dotyczą także sfery zewnętrznej i w tej płaszczyźnie się realizują i konkretyzują[29]. Z oczywistych względów przekonania religijne pracowników nie mogą zakłócać procesu zarządzania przedsiębiorstwem, jednakże mogą zdarzyć się sytuacje, że pracodawca narusza prawa pracownika. W kraju takim jak Polska, gdzie dominuje wyznanie rzymsko-katolickie, największe święta kościelne są jednocześnie dniami wolnymi od pracy. Pracodawca powinien również zadbać o to, aby osoby zatrudnione w jego zakładzie i należące do innych wyznań, miały również możliwość celebrowania swoich świąt. Zgodnie bowiem z art. 2 ust. 2a u.g.w.s.w., korzystając z wolności sumienia i wyznania pracownicy zgodnie z zasadami swojego wyznania mogą uczestniczyć w czynnościach i obrzędach religijnych oraz wypełniać obowiązki religijne i obchodzić święta religijne. Podobnie rzecz przedstawia się z zakazem pracy w określone dni, który bezwzględnie respektowany jest przez przedstawicieli określonych wyznań, oraz spożywania w zakładowych stołówkach określonych potraw. Respektowanie powyższych praw jest konieczne jedynie w sytuacji, gdy pracownik sam zgłosi pracodawcy przy nawiązywaniu stosunku pracy, że przynależy do określonego wyznania, którego zasady religijne determinują jego zachowania. Pracodawca sam nie może wykazywać inicjatywy w tym przedmiocie, chociażby miał uzasadnione podejrzenia co do religii, jaką wyznaje określona grupa pracowników z uwagi na prawo do zachowania milczenia w sprawach swojej religii lub przekonań (art. 2 ust. 5 u.g.w.s.w.). Jest to praktyczny wymiar realizowania negatywnego aspektu wolności religijnej, który dodatkowo realizuje się

[29] A. Mezglewski, *Uzewnętrznienie przekonań religijnych*, w: A. Mezglewski, H. Misztal, P. Stanisz, *Prawo wyznaniowe*, Warszawa 2006, s. 86.

w **zakazie zmuszania do niebrania udziału w czynnościach lub obrzędach religijnych ani do udziału w nich (art. 6 ust. 2 u.g.w.s.w. w zw. z art. 53 ust. 6 Konstytucji)**. W procesie zarządzania problem ten może występować szczególnie w instytucjach publicznych, których pracownicy bardzo często uczestniczą w uroczystościach patriotyczno-religijnych. Aby nie narażać ich na ewentualne niedogodności, pracodawca nie powinien ich do tego zmuszać. Przykład dobrych praktyk w tym zakresie może stanowić chociażby Ceremoniał Sił Zbrojnych Rzeczypospolitej Polskiej, gdzie stwierdza się, że: „Dowódcy jednostek wojskowych przy typowaniu żołnierzy do udziału w nich postępują zgodnie z regulaminami, kierując się poszanowaniem zasad wolności sumienia i wyznania. Indywidualne uczestnictwo żołnierzy w tych uroczystościach odbywa się na zasadzie dobrowolności"[30].

Osoba odpowiedzialna za zarządzanie przedsiębiorstwem nie może ignorować powyższych uprawnień wolnościowych osób zatrudnionych w przedsiębiorstwie, w przeciwnym razie naraża się na popełnienie przestępstwa stypizowanego w art. 194 k.k. Zgodnie z treścią przywoływanej regulacji: „Kto ogranicza człowieka w przysługujących mu prawach ze względu na jego przynależność wyznaniową albo bezwyznaniowość, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

Do dóbr osobistych, które szczególnie narażone są na naruszenie w procesie zarządzania przedsiębiorstwem, należy zaliczyć wolność pracowników. Przy kierowaniu przedsiębiorstwem szczególnej analizy wymagają sytuacje związane **z kontrolowaniem pracowników przy użyciu tzw. nowych technologii**. W grę wchodzi przede wszystkim zjawisko monitorowania ich zachowań. Ewa Suknarowska wskazuje warunki, które muszą zaistnieć, aby ten proces był możliwy. Po pierwsze pracodawca musi mieć usprawiedliwiony cel, który można wykazać w razie ewentualnego sporu. Drugim warunkiem jest zastosowanie proporcjonalnych środków do zakładanego celu. Po trzecie pracownicy powinni być informowani o zakresie kontroli, chyba że jej celem jest wykrycie sprawców popełnianych przestępstw. Czwartym warunkiem jest

[30] Ceremoniał Wojskowy Sił Zbrojnych Rzeczypospolitej Polskiej wprowadzony do użytku służbowego decyzją Ministra Obrony Narodowej nr 392/Mon z dnia 30 września 2014 r., Warszawa 2015 s. 21.

stosowanie przepisów o ochronie danych osobowych i zakazie dyskryminacji[31]. Naruszenia praw pracowników poddawanych kontroli mogą wystąpić w kilku sytuacjach. Chodzi m.in. o sprawdzanie e-maili służbowych (dopuszczalne, jeżeli pracownik wyraził zgodę), stosowanie podsłuchu treści rozmów czy kontroli smsów, nadużywania instalowania kamer – poza sytuacjami wpływającymi na zapobieganie popełnianiu przestępstw czy wykroczeń[32].

Wejście w życie 25 maja 2018 r. rozporządzenia 2016/679[33] zrewolucjonizowało kwestię przetwarzania danych osobowych pracowników, a tym samym zmieniono zasady monitorowania ich zachowań w miejscu pracy[34].

W tekście samego rozporządzenia nie odnajdzie się przepisów dotyczących monitoringu, niemniej jednak zgodnie z dyspozycją wyrażoną w art. 88 (Przetwarzanie w kontekście zatrudnienia) przewidziano możliwość wprowadzenia przez państwa członkowskie przepisów szczególnych dotyczących przetwarzania danych osobowych w zatrudnieniu[35]. W związku z powyższą dyspozycją polski prawodawca skonkretyzował w KP zasady monitoringu wizyjnego (art. 22 (2) KP) oraz monitorowania poczty elektronicznej (art. 22(3) KP). Ustawa formułuje przesłanki warunkujące możliwość wprowadzenia w zakładzie pracy monitoringu wizyjnego. Zgodnie z treścią art. 22(2) § 1 KP: „Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia, lub kontroli produkcji, lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu". Nie jest wymagane, aby przesłanki zostały spełnione kumulatywnie. Wystarczy, że wystąpi jeden z czynników określonych w dyspozycji przywołanego przepisu. Trzy spośród czterech wymienionych przesłanek dotyczą

---

[31] E. Suknarowska-Drzewiecka, *Godność pracownika pod ochroną prawną. Komentarz praktyczny*, ABC, https://sip.lex.pl/#/publication/469915847/suknarowska-drzewiecka-ewa-godnosc-pracownika-pod-ochrona-prawa?cm=URELATIONS (dostęp: 17.06.2019).

[32] Ibid.

[33] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (Dz. Urz UE L 119/L 4/5/2016).*

[34] J. Cur, *Monitorowanie pracowników po 25.5.2018*, „Kwartalnik Edukacja Prawnicza", nr 2(173) rok akademicki 2018/2019, s. 17 (17–21).

[35] Szerzej na ten temat: ibid., s. 17–21.

zabezpieczenia interesów pracodawcy, a tylko jedna odnosi się do interesów pracownika. **Jednakże to właśnie przesłanka bezpieczeństwa osób zatrudnionych w zakładzie pracy może** stwarzać pole do wprowadzania nadużyć. Pojęcie bezpieczeństwa jest niezmiernie szeroką kategorią, która może być wykorzystywana przez pracodawców. Ustawodawca nie precyzuje bowiem, czy w grę wchodzą realne zagrożenia skonkretyzowane w momencie uruchomienia monitoringu, czy też potencjalne, bliżej nieokreślone, mogące zaistnieć w przyszłości. Nie jest wiadome także, z czyjej strony ma pochodzić zagrożenie. Czy chodzi więc o sytuację panującą w zakładzie pracy, czy też mogące „przyjść" z zewnątrz. Nie można również uznać, że przepisy dotyczące obowiązujących zasad BHP, zawarte w KP – art. 207, wyczerpująco formułują przesłanki, w których może dojść do zagrożenia bezpieczeństwa. Zatem można przyjąć, że zasady bezpiecznych i higienicznych warunków pracy zawarte w KP określają jedynie pewien obszar przypadków zagrażających prawom pracownika. Zgodnie z treścią art. 22 (2) § 6 KP: „cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. **Wydaje się uzasadnione, aby zarządzający zakładem pracy, powołując się na przesłankę zagrożenia bezpieczeństwa pracowników, wraz z nimi, np. po konsultacji z zakładową organizacją związkową, podejmował decyzję o uruchomieniu monitoringu.**

Niezrozumiała wydaje się być regulacja **odnosząca się do zakazu monitorowania pomieszczeń sanitarnych, szatni, stołówek oraz palarni (art. 22 (2) § 2 KP). Prawodawca zakazuje w tych miejscach monitorowania, chyba że jest to niezbędne do realizacji celu określonego w art. 22(2) § 1 KP. W powyższej normie brakuje logiki z tego względu, że cele określone w art. 22(2) § 1 warunkują w ogóle możliwość zastosowania monitoringu w całym zakładzie pracy.** Dodatkowa przesłanka dotycząca zakazu naruszenia godności oraz innych dóbr osobistych pracownika, pomimo że niezwerbalizowana wyraźnie w art. **22(2) § 1 KP, również powinna być spełniona niezależnie od miejsca, w którym monitoruje się zachowania pracowników**.

O ile w przypadku monitoringu wizyjnego wątpliwości interpretacyjne powstają w związku z przesłanką bezpieczeństwa pracowników, to w sytuacji monitorowania poczty elektronicznej pole do ewentualnych nadużyć zdaje

się być jeszcze szersze. Zgodnie z art. 22(3) § 1 KP istnieje możliwość kontrolowania służbowej poczty elektronicznej pracownika, jeżeli jest to niezbędne do zapewnienia organizacji pracy, umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. W zasadzie ciężko sobie wyobrazić, jakie zachowanie pracownika w procesie realizowania obowiązków wynikających z zawartej umowy nie jest ukierunkowane na spełnianie powyższych przesłanek. Jednakże wydaje się, że jeżeli zostaną spełnione wszelkie warunki, m.in.: powiadomienie pracowników z odpowiednim wyprzedzeniem, fakt kontrolowania poczty służbowej zdaje się być uzasadniony dla zapewnienia większej efektywności działania. Słuszny zdaje się być postulat zawarty w wypowiedziach doktryny, że **pominięto w tym przepisie możliwości stosowania monitoringu poczty elektronicznej w przypadku podejrzenia naruszenia tajemnicy informacji przedsiębiorstwa. Z uwagi na to, że tego typu naruszenia mogą mieć miejsce w przypadku, np. przesyłania przez nieuczciwych pracowników wiadomości mailowych**[36].

Warto zwrócić uwagę na dyspozycję wyrażoną w art. 22(3) § 4 KP, który daje możliwość wprowadzenia w zakładzie innych niż uregulowane formy monitoringu, jeżeli jest to konieczne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Może tu chodzić o monitorowanie stron internetowych przeglądanych przez pracowników, śledzenie miejsca ich przebywania przy pomocy GPS czy też podsłuchiwanie rozmów z telefonów służbowych. Za słuszny należy uznać postulat, że w sytuacji, gdy pracownik korzysta ze sprzętu udostępnionego przez pracodawcę w celach prywatnych poza czasem pracy, np. telefon, samochód, pracodawca powinien umożliwić mu wyłączenie się spod monitoringu. **Technologie śledzenia sprzętu powinny być projektowane w taki sposób, aby nie służyły inwigilacji pracowników**[37].

Proces monitorowania zachowań pracowników pełni rolę „odstraszania" przed popełnianiem ewentualnych przestępstw. Wydaje się jednak, że pracodawcy powinni koncentrować się na nowych formach zarządzania,

[36] Ibid., s. 20.
[37] Ibid., s. 21.

których zadaniem nie są działania doraźne, ale raczej wyeliminowanie przesłanek mogących doprowadzić do niepożądanych zachowań. W literaturze przedmiotu podkreśla się, że pozytywne efekty w zarządzaniu przedsiębiorstwem może spowodować emocjonalny kontekst relacji pracownika i pracodawcy. Wysoka efektywność jest możliwa do osiągnięcia poprzez budowanie przywiązania i zaangażowania pracowników w sprawy całego przedsiębiorstwa[38]. Pracodawcy, którzy nie budują emocjonalnych więzi zarówno w relacjach wertykalnych (pracownik–pracodawca), jak również horyzontalnych (pracownik–pracownik), nie mogą w dłuższym horyzoncie czasowym oczekiwać osiągnięcia realnych sukcesów. Istotną rolę odgrywa również proces motywowania. **Brak identyfikacji pracowników z organizacją** może spowodować w efekcie zarówno brak wrażliwości na pojawiające się patologie, jak również odpływ wartościowych jednostek do innych podmiotów. Joanna Moczydłowska zwraca również uwagę na to, że niepożądane postawy mogą być wynikiem wewnętrznych konfliktów oraz patologicznych rywalizacji stymulowanych przez kulturę organizacji promującą agresję. Równie poważnym zaniedbaniem ze strony pracodawcy jest niezaznajomienie pracowników z celami strategicznymi organizacji[39]. Pracownik odpowiednio traktowany przez kierujących danym zakładem powinien utożsamiać się z firmą, czyli z jej misją, wizją, celem i wartościami[40]. Przy „tradycyjnym kierowaniu" podkreśla się szczególne znaczenie funkcji kontrolnej. Jednakże nowym paradygmatem w zarządzaniu współczesną organizacją staje się budowanie zaufania do pracownika[41]. Pozytywną rolę zaufania w procesie zarządzania przedsiębiorstwem dostrzeżono już w latach 50. i 60. XX w. Podkreśla się, że jest ono podstawą budowania kapitału społecznego organizacji, wpływa na transfer wiedzy i informacji oraz na efektywność i innowacyjność organizacji[42]. W związku z procesem budowania zaufania w relacjach

---

[38] J. M. Moczydłowska, *Błędy w zarządzaniu relacjami z pracownikami jako wewnętrzne źródło kryzysu w organizacji*, w: *Strategie działań w warunkach kryzysu*, red. S. Partycki, Wydawnictwo KUL, Lublin 2013, s. 347 (346–355).

[39] Ibid., s. 347–348.

[40] A. Kaj, *Wielka 7 – czyli kilka błędów w zarządzaniu zespołem*, https://inventage.pl/wielka-7-czyli-kilka-bledow-w-zarzadzaniu-zespolem/ (dostęp: 23.09.2019).

[41] A. Stankiewicz-Mróz, *Kontrola versus zaufanie. Nadzór nad pracownikami w erze koncepcji empowerment*, „ Zeszyty Naukowe Politechniki Łódzkiej", 2015, nr 60, s. 169 (169–184).

[42] Ibid., s. 170

pracownik-pracodawca, wytworzyła się nowa koncepcja w zarzadzaniu, określana mianem „empowerment". Jest to sposób zachowania i postępowania przełożonych zmierzających do obdarzenia swoich podwładnych władzą, to „delegowanie władzy i uprawnień w celu zwiększenia samoskuteczności pracowników". *Empowerment* jest procesem angażowania pracowników w procesy podejmowania decyzji oraz umożliwiania im brania odpowiedzialności za własne działania[43]. Pracodawcy nie powinni rezygnować z wprowadzania w swoich firmach tego typu rozwiązań, gdyż może to przyczynić się z jednej strony do budowania nowej jakości w relacjach ze swoimi pracownikami, z drugiej zaś spowodować zwiększenie efektywności przedsiębiorstwa.

Do katalogu dóbr osobistych zalicza się również szeroko pojęte dane osobowe, których zasady przetwarzania regulują m.in. przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. Z uwagi na obszerność zamieszczonych tam regulacji warto przytoczyć jedynie niektóre wyjaśnienia Urzędu Ochrony Danych Osobowych (UODO) dotyczących ich przetwarzania w związku z wykorzystywaniem nowoczesnych technologii[44]. Zagadnienia, które były przedmiotem analizy, dotyczyły m.in. problemu pozyskiwania danych kandydata na pracownika z portali społecznościowych. Jak wyjaśnia UODO, co do zasady niedopuszczalne jest gromadzenie i wykorzystywanie przez pracodawców i agencje reklamowe tego typu informacji.

Nieco odmiennie wygląda kwestia weryfikowania lub komunikowania się z kandydatem do pracy za pośrednictwem branżowych portali społecznościowych. W opinii UODO istnieje możliwość pozyskiwania, gromadzenia i udostępniania danych pod warunkiem wyrażenia zgody, podpisania umowy czy też na żądanie osoby, której dane dotyczą[45].

Problem, na który zwraca uwagę UODO, dotyczy ewidencjonowania czasu pracy za pomocą danych biometrycznych. Zdaniem urzędu nie można pobierać danych biometrycznych pracowników w celu rejestracji godzin przyjścia i wyjścia z zakładu nawet za ich zgodą. Zwrócił na to uwagę również Naczelny Sąd Administracyjny w jednym ze swoich orzeczeń, kiedy stwierdził,

---

[43] Ibid., s. 172.

[44] Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, Warszawa 2018.

[45] Ibid., s. 20.

że brak równowagi w relacjach pracodawca-pracownik stawia pod znakiem zapytania dobrowolność na pobieranie i przetwarzanie danych osobowych (biometrycznych). Naczelny Sąd Administracyjny powołał się przy tym na art. 22 KP, który określa, jakich danych pracodawca może żądać od pracownika i nie ma w tym katalogu danych biometrycznych. Zdaniem NSA uznanie faktu wyrażenia zgody jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22 KP stanowiłoby obejście tego przepisu[46]. Jedyna forma wykorzystywania tego typu informacji dotyczy ograniczenia w dostępie do miejsc, w stosunku do których pracodawca może wymagać specjalnych uprawnień. W grę wchodzi tajemnica przedsiębiorstwa bądź ograniczony zakres osób o fachowych umiejętnościach mogących przebywać w obszarach specjalnie chronionych[47].

Należy postulować, aby pracodawca, który decyduje się na ingerencję w sferę dóbr osobistych pracownika, czynił to z zachowaniem wskazań, jakie zawarł NSA w wyroku z 1 grudnia 2009 r. Zgodnie z wyrażonym wówczas stanowiskiem „ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy".

Ochrona godności i dóbr osobistych pracownika, jako podstawowa zasada prawa pracy, stanowi punkt odniesienia dla innych zasad obowiązujących w stosunkach pracownik-pracodawca. Niewątpliwie należy do nich zasada równości wyartykułowana w art. 11(2) KP. Zgodnie z treścią przywołanego przepisu: „pracownicy mają równe prawa z tytułu jednakowego wypełniania tych samych obowiązków, dotyczy to w szczególności równego traktowania mężczyzn i kobiet". Powyższa regulacja ma swoje odniesienie w przepisach obowiązującej konstytucji. Zgodnie z art. 32 wszyscy są wobec prawa równi. Z kolei art. 33 dotyczy równości praw kobiet i mężczyzn w życiu rodzinnym, politycznym społecznym i gospodarczym, Kobieta i mężczyzna mają w szczególności równe prawo m.in. do: zatrudnienia i awansów, do jednakowego wynagrodzenia za pracę jednakowej wartości, do zabezpieczenia społecznego oraz do zajmowania stanowisk (art. 33 ust. 2).

[46] Wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r (I OSK 249/09 – ONSAiWSA z 2011 r. nr 2, poz.39).

[47] Ibid., s. 35–36.

Problem równych płac i dostępu do najwyższych stanowisk w przypadku kobiet i mężczyzn występuje dość powszechnie, dlatego zarządzający przedsiębiorstwem powinni zwracać szczególną uwagę na te kwestie. Problem z całą pewnością nie tkwi w obowiązujących regulacjach, ale w stosowanych praktykach. Nie jest to także zjawisko typowe wyłącznie dla naszego kraju. Według danych Komisji Europejskiej za 2017 r. średnia różnica w wynagrodzeniach kobiet i mężczyzn w UE wynosi 16,3%. Polska nie wypada źle na tle statystyk unijnych, bo skalę zjawiska oszacowano na 8%, niemniej jednak stale należy na to zwracać uwagę[48].

Poszanowanie godności i równości pracowników wpływa pozytywnie na respektowanie przez pracodawców zasady dotyczącej zakazu dyskryminacji pracowników. Zgodnie z art. 11(3) zakazana jest jakakolwiek dyskryminacja w zatrudnieniu, bezpośrednia lub pośrednia, w szczególności ze względu na płeć, wiek, niepełnosprawność, rasę, religię, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientację seksualną, zatrudnienie na czas określony lub nieokreślony, zatrudnienie w pełnym lub w niepełnym wymiarze czasu pracy. Dyrektywa Rady 2000/78 WE definiuje pojęcie występujące w KP. Zgodnie z art. 2 ust. 1 lit. a **dyskryminacja bezpośrednia** występuje w przypadku, gdy osobę traktuje się mniej przychylnie niż traktuje się, traktowano by inną osobę w porównywalnej sytuacji z jakiejkolwiek przyczyny. Z kolei z **dyskryminacją pośrednią** ma się do czynienia w przypadku, gdy przepis, kryterium lub pozornie neutralna praktyka może doprowadzić do szczególnej niekorzystnej sytuacji dla osób danej religii lub przekonań, niepełnosprawności, wieku lub orientacji seksualnej w stosunku do innych osób (art. 2 ust. 1 lit. b.). Obowiązujący KP zawiera w swej treści również legalne definicje dyskryminacji bezpośredniej (art. 18 (3a) § 3 KP) i dyskryminacji pośredniej (art. 18 (3a) § 4 KP), które są zbieżne z określeniem zawartym w dyrektywie Rady 2000/78 WE.

Pracodawca lub inna osoba zarządzająca przedsiębiorstwem w jego imieniu może dopuszczać się różnych form dyskryminowania pracownika. Może tu chodzić zarówno o przesłanki dotyczące osobistych cech pracownika, np.

[48] Komisja Europejska, *Różnice w wynagrodzeniach kobiet i mężczyzn w UE*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/equal-pay/gender-pay-gap-situation-eu_en (dostęp: 29.09.2019).

wyznanie, rasę, narodowość (patrz art. 18 (3a) § 1 KP), jak również sposób zachowania polegający na zachęcaniu innej osoby do naruszenia zasady równego traktowania w zatrudnieniu lub wręcz nakazaniu naruszenia tejże zasady (art. 18 (3a) § 5 p. 1 KP). Może to mieć miejsce przy rozbudowanych strukturach zarządzania przedsiębiorstwem, kiedy to przełożeni, wykorzystując swoją silną pozycję, wywierają dominujący wpływ na niższe struktury organizacyjne.

W świetle przepisów KP dyskryminacją pracownika są rożne **formy molestowania**. Prawodawca w art. 18 (3a) § 5 p. 2 KP wyodrębnia molestowanie, nie uszczegóławiając jego rodzaju, polegające na niepożądanym zachowaniu, którego celem lub skutkiem jest naruszenie godności pracownika i stworzenie wobec niego wrogiej, poniżającej, upokarzającej lub uwłaczającej atmosfery. Zbliżoną formą jest mobbing, oznaczający działania lub zachowania dotyczące pracownika lub skierowane przeciwko pracownikowi, polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu pracownika, wywołujące u niego zaniżoną ocenę przydatności zawodowej, powodujące lub mające na celu poniżenie lub ośmieszenie pracownika, izolowanie go lub wyeliminowanie z zespołu współpracowników.

Stypizowaną formą dyskryminacji jest również molestowanie seksualne, które może dokonywać się ze względu na płeć pracownika. Cele molestowania są zbieżne z celami ogólnymi określonymi w art. 18 (3a) § 5 p. 2 KP. Może ono przybierać postać: fizycznego oddziaływania, werbalnych uwag oraz pozawerbalną (np. nacisk psychologiczny).

Pracownik poddany tym formom oddziaływania zarówno ze strony zarządzających przedsiębiorstwem, jak również swoich współpracowników, często osobiście nie podejmuje żadnych kroków, chociaż ustawodawca stwarza mu takie możliwości. **Dlatego też niezmiernie ważne jest, aby stworzyć system monitorowania patologicznych zachowań, polegający na zaangażowaniu całej społeczności. Z pewnością mogłoby to ułatwić usankcjonowanie w polskim systemie prawnym instytucji sygnalisty.** Pomimo tego, że w polskich realiach nie zdecydowano się ustawowo uregulować jego statusu, to podstawy normatywne istnieją już w standardach prawa międzynarodowego. Konwencja ONZ Przeciwko Korupcji z 31 października 2006 r. posługuje się terminem osoba zgłaszająca (art. 33). Stwierdza się tam m.in., że państwa rozważą włączenie do swego wewnętrznego systemu prawnego odpowiednich

środków w celu zapewnienia ochrony przed jakimkolwiek nieuzasadnionym działaniem każdej osobie, która zgłasza w dobrej wierze i na racjonalnych podstawach właściwemu organowi wszelkie zdarzenia związane z przestępstwami[49]. Ponadto zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/6 zwalnia się z odpowiedzialności za naruszenie tajemnicy przedsiębiorstwa osoby, które ujawniły poufne informacje, aby wykazać nieprawidłowości w miejscu pracy, jeżeli działały w celu ochrony ogólnego interesu publicznego (art. 5)[50]. Warto zauważyć, że w Polsce powołanie instytucji sygnalisty przewiduje m.in. projekt ustawy *o jawności życia publicznego*, gdzie pod tym określeniem rozumie się osobę fizyczną lub przedsiębiorcę, których współpraca z wymiarem sprawiedliwości, polegająca na zgłoszeniu informacji o możliwości popełnienia przestępstwa przez podmiot, z którym jest związana umową o pracę, stosunkiem służbowym lub innym stosunkiem umownym, może niekorzystnie wpłynąć na jej sytuację życiową, zawodową, materialną, i której prokurator przyznał status sygnalisty[51].

Przyczyną popełniania czynów niedozwolonych wobec pracowników jest niezachowanie przez pracodawców przepisów dotyczących bezpiecznych i higienicznych warunków pracy (art. 15 KP). Do obowiązków osoby odpowiedzialnej za BHP, kierującej pracownikami należy m.in. : 1) organizowanie stanowiska pracy zgodnie z przepisami i zasadami bezpieczeństwa i higieny pracy; 2) dbanie o sprawność środków ochrony indywidualnej oraz ich stosowanie zgodnie z przeznaczeniem; 3) organizowanie, przygotowywanie i prowadzenie prac, z uwzględnieniem zabezpieczenia pracowników przed wypadkami przy pracy, chorobami zawodowymi i innymi chorobami związanymi z warunkami środowiska pracy; 4) dbanie o bezpieczny i higieniczny stan pomieszczeń pracy i wyposażenia technicznego, a także o sprawność środków ochrony zbiorowej i ich stosowanie zgodnie z przeznaczeniem; 5) egzekwowanie przestrzegania przez pracowników przepisów

[49] *Konwencja Narodów Zjednoczonych Przeciwko Korupcji, przyjęta przez Zgromadzenie Ogólna Narodów Zjednoczonych z dnia 31 października 2003 r. (Dz.U. 2007 Nr 84 poz. 563).*

[50] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz. Urz. UE L. 157/1 15.6/2016).*

[51] *Projekt ustawy o jawności życia publicznego z dnia 8 stycznia 2018 r.*, https://www.rpo.gov.pl/sites/default/files/ustawa-o-jawnosci-zycia-publicznego (dostęp: 29.09.2019).

i zasad bezpieczeństwa i higieny pracy oraz 6) zapewnianie wykonania zaleceń lekarza sprawującego opiekę zdrowotną nad pracownikami[52]. **Zaniedbania w zakresie naruszenia przepisów przez osobę odpowiedzialną za bezpieczeństwo i higienę pracy mogą doprowadzić do popełnienia przestępstwa w sytuacji narażenia pracownika na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu** (art. 220 k.k.).

Przepisy KP nakładają na pracodawcę lub inną osobę kierującą pracownikami określone obowiązki w sytuacji zaistnienia wypadku przy pracy (art. 234 KP) oraz podejrzenia choroby zawodowej (art. 235 KP). Aby inny podmiot niż pracodawca podlegał odpowiedzialności karnej, powinien posiadać ogólne zwierzchnictwo w zakresie BHP nad pracownikiem, który uległ wypadkowi[53]. Przepisy k.k. penalizują te zachowania, które dotyczą niezawiadomienia właściwego organu o wypadku przy pracy lub chorobie zawodowej albo niesporządzenia lub nieprzedstawienia wymaganej dokumentacji. W myśl przepisu KP właściwym organem w sytuacji śmiertelnego, ciężkiego lub zbiorowego wypadku jest właściwy okręgowy inspektor pracy oraz prokurator (art. 234 § 2 KP). Z kolei w przypadku podejrzenia choroby zawodowej, niezwłocznie należy zgłosić ten fakt właściwemu państwowemu inspektorowi sanitarnemu oraz właściwemu okręgowemu inspektorowi pracy (art. 235 § 1).

W procesie zarządzania przedsiębiorstwem może dojść do złośliwego i uporczywego naruszania praw pracowniczych, wynikających z ubezpieczeń społecznych (art. 218 § 1, art. 219 k.k). Szczegółowy zakres obowiązków pracodawcy w tej materii regulowany jest przepisami ustawy[54]. Zaniedbania w tym zakresie mogą dotyczyć w szczególności następujących sytuacji: naliczania i odprowadzania składek ZUS, zgłoszenia pracowników do ubezpieczenia ZUS w ciągu 7 dni od daty powstania obowiązku zatrudnienia, wyrejestrowania ubezpieczonego w ciągu 7 dni od daty wygaśnięcia tytułu do ubezpieczeń społecznych, zawiadomienia ZUS o wszelkich zmianach, jakie

---

[52] *Niedopełnienie obowiązków BHP to przestępstwo*, https://kadry.infor.pl/bhp/bezpieczenstwo-pracy/266538,Niedopelnienie-obowiazkow-BHP-to-przestepstwo.html (dostęp: 29.09.2019).

[53] R. Widzisz, *Odpowiedzialność karna za niezawiadomienie o wypadku przy pracy*, „Prokuratura i Prawo", 2007, nr 5, s. 44 (41–64).

[54] *Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (tekst jedn.: Dz.U. 2019 poz. 300 ze zm.).*

nastąpiły w stosunku do danych osób ubezpieczonych zawartych w zgłoszeni, w terminie 7 dni od zaistnienia tych zmian. **Powyższy sposób postępowania może spowodować niekorzystną sytuację dla pracowników, ale także dla zakładu pracy, dlatego też niezbędne jest dokonywanie stałej kontroli w tym zakresie.** Ponadto dyspozycja art. 219 k.k. dotyczy również sytuacji, gdy zaniedbania w zakresie ubezpieczeń społecznych dokonują się za zgodą ubezpieczonego. Jest to dość powszechna praktyka, kiedy pracownicy kuszeni wyższym wynagrodzeniem godzą się na celowe zaniżanie odprowadzanych składek. Tworzy się w ten sposób zjawisko „szarej strefy", gdzie ZUS zostaje pozbawiony należnych wpływów, a Skarb Państwa podatków.

4. Podsumowanie

Powyższa analiza nie wyczerpuje problematyki przesłanek, które mogą doprowadzić do popełnienia czynów niedozwolonych w procesie zarządzania przedsiębiorstwem. Jednakże na kanwie poczynionych uwag można sformułować pewne postulaty *de lege ferenda* oraz praktyczne uwagi skierowane do podmiotów zarządzających.

Do postulatów *de lege ferenda* należy zaliczyć:

- Wprowadzenie procedury postępowania w sytuacjach, kiedy pracownik ma wątpliwości czy polecenie wydane przez pracodawcę jest zgodne z prawem. W takiej sytuacji należałoby zapewnić możliwość zgłoszenia swoich obaw pracodawcy i udokumentowanie tegoż zdarzenia na wypadek potencjalnych oskarżeń kierowanych przeciwko osobie pracownika.
- W celu łatwiejszego przeciwdziałania popełnianiu przestępstw oraz ich identyfikacji należy stworzyć system monitorowania patologicznych zachowań, polegający na zaangażowaniu całej społeczności przedsiębiorstwa. W związku z powyższym należy uregulować w sposób kompleksowy funkcjonowanie instytucji sygnalisty.
- Należy usankcjonować możliwości stosowania monitoringu poczty elektronicznej w przypadku podejrzenia naruszenia tajemnicy informacji przedsiębiorstwa.

Jeżeli chodzi o praktyczne wskazówki kierowane do zarządzających, należy postulować:

- W sytuacji wprowadzenia monitoringu wizyjnego na podstawie przesłanki bezpieczeństwa pracowników pracodawca powinien przeprowadzić konsultacje z samymi pracownikami bądź z reprezentującą ich organizacją związkową.
- W przypadku, gdy pracownik korzysta ze sprzętu udostępnionego przez pracodawcę w celach prywatnych poza czasem pracy, pracodawca powinien umożliwić mu wyłączenie się spod monitoringu.
- Wprowadzanie przez pracodawców nowych form zarządzania, których zadaniem nie są działania doraźne, ale wyeliminowanie przesłanek mogących doprowadzić do niepożądanych zachowań. W tym celu pracodawcy powinni stosować m.in. procedurę *empowerment*, polegającą na angażowaniu pracowników w procesy podejmowania decyzji oraz umożliwianiu im brania odpowiedzialności za własne działania.
- W sytuacji, kiedy zarządzający decyduje się na ingerencję w dobra osobiste pracowników, środki przez niego stosowane winny być proporcjonalne do celów, którym służą.

Bibliografia

I. Źródła

Akty normatywne

Konwencja Narodów Zjednoczonych Przeciwko Korupcji, przyjęta przez Zgromadzenie Ogólna Narodów Zjednoczonych z dnia 31 października 2003 r. (Dz.U. 2007 Nr 84 poz. 563).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (Dz. Urz UE L 119/L 4/5/2016).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz. Urz. UE L. 157/1 15.6/2016).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (tekst jedn.: Dz.U. 2018 poz. 1025 ze zm.).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn.: Dz.U. 2019 poz. 1040 ze zm.).

Ustawa z dnia 17 maja 1989 r., o gwarancjach wolności sumienia i wyznania (tekst jedn.: Dz.U. 2017 r. poz. 1153).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn.: Dz.U. 2018 poz. 1600 ze zm.).

Ustawa z 13 października 1998 r. o systemie ubezpieczeń społecznych (tekst jedn.: Dz.U. 2019 poz. 300 ze zm.).

Ustawa z dnia 28 października 2008 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (tekst jedn.: Dz.U. 2019 poz. 628 ze zm.).

Orzecznictwo

Wyrok Sądu Najwyższego z dnia 14 października 1977 r., (I PRN 136/77 – LEX nr 14431).

Wyrok Sądu Najwyższego z dnia 19 września 1997 r. (I PKN 244/87 – OSNP 12/98, poz. 358).

Wyrok Sądu Najwyższego z dnia 15 października 1999 r. (I PKN 309/99 – OSNP 5/2001, poz. 147).

Wyrok Sądu Najwyższego z dnia 2 lutego 2001 r. (I PKN 226/00 – OSNAPIUS z 2002/20, poz. 488).

Wyrok Sądu Najwyższego z dnia 25 listopada 2004 r. (I PK 42/04).

Wyrok Sądu Najwyższego z dnia 20 września 2005 r. II PK 412/04 – OSNP 2006/13-14/210.

Wyrok Sądu Najwyższego z dnia 3 kwietnia 2008 r. (II PK 288/07).

Wyrok Sądu Najwyższego z dnia 7 grudnia 2012 r. (II PK 121/12 LEX nr 1284747).
Wyrok Sądu Najwyższego z dnia 17 stycznia 2017 r. (WA 18/16 LEX nr 2203539).
Wyrok Naczelnego Sadu Administarcyjnego z dnia 1 grudnia 2009 r (I OSK 249/09 – ONSAiWSA z 2011 r. nr 2, poz.39).
Wyrok Sądu Okręgowego w Koszalinie z dnia 11 lutego 2010 r. (I C 639/09 – LEX nr 1713915).
Wyrok Sądu Okręgowego w Rzeszowie z dnia 24 października 2014 r. (II KA 434/14 – LEX nr 1860417).

Inne

Komisja Europejska, Różnice w wynagrodzeniach kobiet i mężczyzn w UE, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/equal-pay/gender-pay-gap-situation-eu_en (dostęp: 29.09.2019).
Ceremoniał Wojskowy Sił Zbrojnych Rzeczypospolitej Polskiej wprowadzony do użytku służbowego decyzją Ministra Obrony Narodowej nr 392/Mon z dnia 30 września 2014 r., Warszawa 2015.
Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, Warszawa 2018.
Projekt ustawy o jawności życia publicznego z dnia 8 stycznia 2018 r. https://www.rpo.gov.pl/sites/default/files/ustawa-o-jawnosci-zycia-publicznego (dostęp: 29.09.2019).

II. Literatura

Buczyńska T., *Mikroekonomia*, Warszawa–Łódź 2017.
Cur J., *Monitorowanie pracowników po 25.5.2018*, „Kwartalnik Edukacja Prawnicza", nr 2 (173), rok akademicki 2018/2019, s. 17–21.
Duraj T., *Granice uprawnień kierowniczych pracodawcy w stosunku pracy*, „Zeszyty Prawnicze", 2013, nr 13 (2), s. 101–130.
Florek L., Zieliński T., *Prawo pracy*, Warszawa 1997.
Gardocki L., *Pojęcie przestępstwa i podziały przestępstw w polskim prawie karnym*, Annales Universitatis Mariae Curie-Skłodowska", 2013, nr 2, s. 29–40.
Golnau W., Kalinowski M., Litwin J., *Zarządzanie zasobami ludzkimi*, Warszawa 2002.
Kaj A., *Wielka 7 – czyli kilka błędów w zarządzaniu zespołem*, https://inventage.pl/wielka-7-czyli-kilka-bledow-w-zarzadzaniu-zespolem/ (dostęp: 23.09.2019).
Leleń A., *Zarządzanie zasobami ludzkimi przedsiębiorstwa*, „Bezpieczeństwo i Technika Pożarnicza", 2011, nr 2, s. 31–42.
Mezglewski A., *Uzewnętrznienie przekonań religijnych*, w: A. Mezglewski, H. Misztal, P. Stanisz, *Prawo wyznaniowe*, Warszawa 2006, s. 86–90.

Moczydłowska J.M., *Błędy w zarządzaniu relacjami z pracownikami jako wewnętrzne źródło kryzysu w organizacji*, w: S*trategie działań w warunkach kryzysu*, red. S. Partycki, Wydawnictwo KUL, Lublin 2013, s. 346–355.

Niedopełnienie obowiązków BHP to przestępstwo, https://kadry.infor.pl/bhp/bezpieczenstwo-pracy/266538,Niedopelnienie-obowiazkow-BHP-to-przestepstwo.html (dostęp: 29.09.2019).

Stankiewicz-Mróz A., *Kontrola versus zaufanie. Nadzór nad pracownikami w erze koncepcji emprowerment*, „Zeszyty Naukowe Politechniki Łódzkiej", 2015, nr 60, s. 169–184.

Stelina J. (red.), *Stosunek pracy*, w: *Leksykon prawa pracy. 100 podstawowych pojęć*, Warszawa 2008.

Suknarowska-Drzewiecka E., *Godność pracownika pod ochroną prawną. Komentarz praktyczny*, ABC, https://sip.lex.pl/#/publication/469915847/suknarowska-drzewiecka-ewa-godnosc-pracownika-pod-ochrona-prawa?cm=URELATIONS (dostęp: 17.06.2019).

Widzisz R., *Odpowiedzialność karna za niezawiadomienie o wypadku przy pracy*, „Prokuratura i Prawo", 2007, nr 5, s. 41–64.

Wiszowata E., *Wykroczenia przeciwko prawom pracownika*, Warszawa 2012.