MOŻLIWE PRZYCZYNY I RODZAJE PRZESTĘPCZOŚCI W PRZYSZŁOŚCI ORAZ PRZYGOTOWANIA PREWENCYJNE

AUTORZY:

Paul HEALY, Harvard Business School
Bartosz JANASZEK, Executive Education Center
Marcin KIELISZCZYK, Executive Education Center
Radosław KOSZEWSKI, Executive Education Center
Mireia LAS HERAS, IESE Business School
Michael ROSENBERG, IESE Business School
Roland STEPHEN, SRI International
Antonino VACCARO, IESE Business School

KONSULTACJE NAUKOWE:

Joanna CYGLER, Szkoła Główna Handlowa
Agata KOSIERADZKA-FEDERCZYK,
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Gabriela JYŻ, Naczelny Sąd Administracyjny

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
Piotr KWIATKIEWICZ, Uniwersytet Zielonogórski
Grzegorz STRUPCZEWSKI, Uniwersytet Ekonomiczny w Krakowie
Joanna TACZKOWSKA-OLSZEWSKA, Akademia Sztuki Wojennej

MOŻLIWE PRZYCZYNY I RODZAJE PRZESTĘPCZOŚCI W PRZYSZŁOŚCI ORAZ PRZYGOTOWANIA PREWENCYJNE

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*

Copyright © by Instytut Wymiaru Sprawiedliwości, Warszawa 2021

WYDANIE 2

ISBN 978-83-66344-37-2

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

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

Spis treści

Słowo wstępne

Pierwsza część niniejszej publikacji (raport) stanowi podsumowanie prac badawczych przeprowadzonych w ramach czwartego, ostatniego modułu projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości". Jest to zatem także ostatnia praca z cyklu poświęconego przeciwdziałaniu przestępczości w kluczowych obszarach polskiej gospodarki. Podjęte badania wpisują się w nurt działań służących zwalczaniu przyczyn występowania przestępczości oraz ograniczaniu czynników ryzyka jej występowania. Celem badań podsumowanych w niniejszym raporcie było stworzenie narzędzi strategicznego zarządzania w warunkach niepewności, która jest nieodłącznie związana z niemożnością przewidzenia przyszłych zdarzeń na gruncie indeterministycznym. Uzyskane rezultaty mają przyczynić się do osiągnięcia długofalowych skutków, które pozwolą uzyskać lepszą efektywność i produktywność realizacji zadań operacyjnych określonych w misji każdej organizacji.

Przeprowadzone prace pozwoliły także uzupełnić szkielet metodologiczny (*B3*)[1] poprzez dodanie do niego elementów *polityki zgodności* oraz planowania scenariuszowego, które realizują odpowiednio elementy *Be a Team* oraz *Be Ready* wypracowanego modelu. W ramach prac dokonano przeglądu potencjalnych rodzajów przyszłych działań przestępczych, a także ich zakresu, charakteru, przyczyn oraz uwarunkowań, które mogą sprzyjać ich występowaniu. Na gruncie założeń metodyki planowania scenariuszowego skoncentrowano

[1] Szkielet metodologiczny *B3* stał się jednym z kluczowych przedmiotów rozważań już podczas drugiego etapu seminariów przeprowadzanych w ramach projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości".

się na tych problemach, na które nie umiemy jeszcze skutecznie reagować, choć ich symptomy są już obecnie zauważalne. Szczególną uwagę poświęcono przy tym zagrożeniom związanym z rozwojem technologii. Zaproszeni eksperci byli zgodni, że postępy w tym obszarze zachodzą w tempie bezprecedensowym, co tworzy liczne wyzwania natury operacyjnej, prawnej oraz etycznej. Ustalono, że konieczne jest podjęcie działań wyprzedzających, pozwalających na właściwe przygotowanie organizacji na zagrożenia, które mają istotnie wysoki potencjał urzeczywistnienia się w najbliższej przyszłości.

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 Heading into the Future. 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 możliwych przyczyn i rodzajów przestępczości w przyszłości oraz przygotowań prewencyjnych.

CZĘŚĆ PIERWSZA

RAPORT

AUTORZY:

Paul HEALY, Harvard Business School
Bartosz JANASZEK, Executive Education Center
Marcin KIELISZCZYK, Executive Education Center
Radosław KOSZEWSKI, Politechnika Warszawska
Mireia LAS HERAS, IESE Business School
Michael ROSENBERG, IESE Business School
Roland STEPHEN, SRI International
Antonino VACCARO, IESE Business School

KONSULTACJE NAUKOWE:

Joanna CYGLER, Szkoła Główna Handlowa
Agata KOSIERADZKA-FEDERCZYK,
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Gabriela JYŻ, Naczelny Sąd Administracyjny

1. Wprowadzenie

Seminaria przeprowadzone w ramach pierwszego etapu projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" oraz powiązane z nimi badania pozwoliły na identyfikację przyczyn oraz czynników sprzyjających popełnianiu przestępstw w Polsce i na świecie. Podczas kolejnego etapu uczestnicy zapoznali się z metodyką zarządzania operacyjnego oraz uznanymi i stosowanymi na świecie rozwiązaniami na rzecz przeciwdziałania przestępczości. Sformułowane przez nich wnioski, wpisujące się w ramy zaprezentowanej metodyki, pozwoliły na opracowanie nowatorskich koncepcji przeciwdziałania przestępczości poprzez zwiększenie efektywności organizacji w Polsce. Trzeci etap projektu został poświęcony problematyce *wdrażania zmiany*, czyli omówieniu metod i instrumentów dedykowanych przeciwdziałaniu przestępczości, które zostały oparte na fundamencie silnej kultury organizacji. Stwierdzono, że elementy te stanowią klucz do osiągnięcia sukcesu w dziedzinie zapobiegania przestępczości w organizacjach. Prace badawcze wykonane w ramach dotychczasowych seminariów zostały wpisane w ramy metodologii *B3* (*Be Lean – Be a Team – Be Ready*), która jest podstawą myśli przewodniej całego projektu (zob. rysunek 1).

Rysunek 1. Schemat metodologii B³

Źródło: opracowanie własne

Czwarty etap prac, który został podsumowany w niniejszym raporcie, skupiał się na nieomówionych wcześniej elementach metodologii *B*³. Seminaria dotyczyły więc problematyki planowania scenariuszowego, a dotychczasowy zestaw narzędzi zapobiegania przestępczości wzbogacono o istotny element *polityki zgodności*, której celem jest promowanie praworządności. Prace badawcze koncentrowały się na zagadnieniach związanych z przyczynami i rodzajami przestępczości, które mogą wystąpić w przyszłości, oraz działaniami prewencyjnymi.

1.1. Polityka zgodności

Omówienie problematyki dotyczącej polityki zgodności (ang. *compliance policy*) wiąże się z pojęciem tzw. miękkiego prawa (ang. *soft law*). Jest to element systemu prawnego, który nie posiada mocy wiążącej, a nieprzestrzeganie jego zapisów nie skutkuje nałożeniem sankcji formalnych[2]. Pomimo

[2] P. Skuczyński, *Soft law w perspektywie teorii prawa*, w: O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny,* Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2008, s. 334.

tych pozornych braków względem prawa twardego (ang. *hard law*), podmioty wyrażają chęć dobrowolnego związania się postanowieniami opartymi na mocy przepisów prawa miękkiego, w sposób niezależny od przymusu instytucjonalnego[3].

W 1999 roku Organizacja Narodów Zjednoczonych ustanowiła w ramach platformy *United Nations Global Compact* jedną z pierwszych inicjatyw, która ukształtowała wyjątkowy charakter zjawiska, które obecnie nazywa się kulturą zgodności (ang. *compliance culture*). W ramach tej inicjatywy określono zbiór zasad społecznych, obejmujący regulacje prawne, prawa człowieka, zasady ochrony środowiska oraz metody zapobiegania korupcji, które należy wdrożyć w organizacji, żeby mogła stać się jednym ze źródeł zdrowego, zrównoważonego rozwoju społecznego. W tym samym roku Organizacja Współpracy Gospodarczej i Rozwoju (ang. *Organisation for Economic Co-operation and Development*, OECD) opublikowała zbiór zasad zatytułowany *Principles of Corporate Governance*[4]. Zaktualizowana wersja tego dokumentu została najpierw zaprezentowana w kwietniu 2015 roku podczas *Global Corporate Governance Forum*, połączonego forum państw G20 oraz OECD, a następnie zatwierdzona jako oficjalna rekomendacja Rady OECD i zaprezentowana na szczycie państw G20, 8 lipca 2015 roku, pod nowym tytułem: *G20/OECD Principles of Corporate Governance*[5]. Zasady te określiły ramy dla relacji społeczno-biznesowych, których nadrzędnym celem jest dobro całego społeczeństwa. Stosowanie się do zawartych w dokumencie zaleceń oznacza przestrzeganie nie tylko zapisów prawa karnego *sensu largo* oraz prawa wykroczeń, ale także wszystkich innych norm, do których mogą mieć zastosowanie, w tym w kwestiach dotyczących administracji, prawa pracy i praw obywatelskich, dzięki czemu możliwe staje się wypracowanie efektywnego globalnego systemu zgodności.

Dążenie do spełnienia rygorów prawnych w sprawach związanych z zarządzaniem ludźmi staje się zatem równoznaczne z przestrzeganiem praw człowieka. Dlatego ryzyko naruszenia tych praw powinno być zawsze szacowane w celu określenia odpowiedniej polityki, a także mechanizmów ochronnych i zapobiegawczych. Polityka dotycząca praw człowieka stosowana przez

---

[3] Ibid.

[4] OECD, *OECD Principles of Corporate Governance*, OECD, Paryż 1999.

[5] OECD, *G20/OECD Principles of Corporate Governance*, OECD, Paryż 2015.

przedsiębiorstwa ujęta jest zwykle w kodeksie postępowania (ang. *code of conduct*) lub kodeksie etycznym organizacji.

Polityka zgodności zakłada, że „przykład idzie z góry" (ang. *tone at the top*[6]), co oznacza, że wszelkie zmiany dotyczące kultury organizacji muszą być inicjowane przez zarząd. Jego członkowie powinni angażować się w tworzenie kodeksów i stosować się zarówno do ich zapisów, jak i założeń kultury organizacji, stając się wzorem dla pozostałych pracowników.

1.2. Tworzenie map ryzyka

Jednym z kluczowych elementów implementacji polityki zgodności w organizacji jest tworzenie tzw. mapy ryzyka. Pierwszym etapem tworzenia mapy ryzyka jest identyfikacja i ocena ryzyka wystąpienia przestępstwa lub nieprawidłowości, wraz z estymacją prawdopodobieństwa tego wystąpienia oraz oszacowaniem poziomu związanego z nim zagrożenia. W celu przygotowania mapy ryzyka należy najpierw przeprowadzić analizę *due diligence* w zakresie treści regulacji. Pozwoli to określić poziom zgodności stosowanych praktyk z obowiązującym prawem i zaprojektować matrycę sytuacyjną[7] aktualnego stanu organizacji. Wykorzystując powstały w ten sposób wizualny i praktyczny schemat można postawić diagnozę i przygotować skuteczny plan działania. W celu opracowania planu implementacji polityki zgodności konieczne jest określenie kontekstu organizacji, tj. jej wielkości, lokalizacji, sektora operacyjnego, podmiotów zależnych oraz powiązań z innymi organizacjami. Kolejny etap analizy to badanie, którego celem jest rozpoznanie obszaru operacyjnego organizacji oraz potencjalnych zagrożeń. Szczególną uwagę należy zwrócić na czynniki ryzyka, które charakteryzuje nie tylko wysokie prawdopodobieństwo wystąpienia, ale też duża dotkliwość potencjalnych skutków. Poziom prawdopodobieństwa wystąpienia poszczególnych czynników określa się na podstawie liczby ich wystąpień w ciągu ostatnich pięciu lub dziesięciu lat. Nie

[6] J.S. Pickerd, S.L. Summers, D.A. Wood, *An Examination of How Entry-Level Staff Auditors Respond to Tone at the Top vis-à-vis Tone at the Bottom*, „Behavioral Research in Accounting", 2014, t.27, nr 1, s. 79–98.

[7] N. Sandford i in., *Compliance Risk Assessments. The Third Ingredient in a World-class Ethics and Compliance Program*, Deloitte 2015.

oznacza to jednak, że dany czynnik ryzyka jest wykluczany z analizy, jeśli określona sytuacja nie miała jeszcze miejsca. Natomiast dotkliwość ewentualnych skutków jest określana na podstawie kar finansowych i zakazów przewidzianych przez kodeks karny dla poszczególnych wykroczeń, a także tego, jak bardzo mogą one zaszkodzić reputacji organizacji.

Rysunek 2. Koncepcja wdrażania kultury zgodności w organizacjach

Źródło: opracowanie własne

Tego typu mapy mogą zawierać różne rodzaje ryzyka – nie tylko naruszenia przewidziane przez przepisy prawa karnego. Mogą również obejmować inne nieprawidłowości dotyczące zarządzania ludźmi, nieetyczne zachowania podczas prowadzenia działalności operacyjnej, przykłady łamania kodeksu postępowania, czy też inne naruszenia obowiązujących regulacji związanych z kierunkiem rozwoju organizacji oraz zarządzaniem personelem.

1.3. Planowanie scenariuszowe

Każdą organizację można opisać w ujęciu atrybutowym, rzeczowym, czynnościowym oraz podmiotowym jako pewną całość wyodrębnioną z otoczenia,

do którego przynależy[8]. Aktualny stan organizacji można opisać przy pomocy zestawu czynników, których indywidualna charakterystyka oraz wzajemne powiązania definiują jej niepowtarzalną tożsamość. Do wspomnianych czynników można zaliczyć m.in.:

- zestaw ogólnych praw ekonomicznych i społecznych, którym podlega organizacja,
- charakterystykę ekosystemu, w którym funkcjonuje (przynależność sektorowa, działalność konkurencyjna itd.),
- otoczenie regulacyjne (zestaw praw, którym podlega),
- zbiór procesów operacyjnych, stosowanych praktyk, kodeksów oraz wewnętrznych polityk postępowania.

Na gruncie determinizmu postuluje się, że znajomość bieżącego stanu danej rzeczy oraz praw, którym podlega, pozwala na przewidzenie jej przyszłego stanu. O ile jest to możliwe w przypadku pewnych prostych systemów fizycznych, o tyle organizacje są zbyt złożonymi bytami, żeby dało się tak prosto przewidzieć ich przyszłość. W przypadku organizacji postuluje się zatem, że próba przewidzenia ich przyszłego stanu może zostać przeprowadzona jedynie na gruncie indeterminizmu – koncepcji, w której przyszłe stany są definiowane jako potencjalnie możliwe z określonym prawdopodobieństwem[9].

Pomimo niemożności przewidzenia stanu, w którym organizacja znajdzie się w przyszłości, zarządzanie nią wymaga tworzenia scenariuszy uwzględniających prawdopodobne zdarzenia i traktujących organizację jako zamkniętą całość oraz element lokalnego i globalnego ekosystemu. Planowanie scenariuszowe jest jedną z metod, która uwzględnia powyższe założenia i gwarantuje pozbawione zakłóceń funkcjonowanie organizacji w kontekście ewentualnych przyszłych wyzwań. Metoda ta polega na tworzeniu zestawu scenariuszy przyszłości, przy czym każdy ze scenariuszy składa się z następujących dwóch elementów:

- przyszłego, hipotetycznego stanu organizacji oraz
- działań strategicznych, które zostaną podjęte w przypadku realizacji tego scenariusza.

---

[8] S. Marek, M. Białasiewicz, *Podstawy nauki o organizacji: przedsiębiorstwo jako organizacja gospodarcza*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2008.

[9] R. Janikowski, *Nieprzewidywalność w zarządzaniu przedsiębiorstwem*, „Modern Management Review", 2014, t.XIX, nr 21.

Zarówno uczestnicy, jak i zaproszeni eksperci postulowali, że należy tworzyć zarówno skrajnie optymistyczne, jak i pesymistyczne scenariusze. Takie podejście pozwala na wytworzenie warunków granicznych dla przeprowadzenia właściwej analizy scenariuszowej.

Owocem planowania scenariuszowego są strategie (plany), które można wdrożyć w przypadku zaistnienia zdarzeń, które były przesłanką dla opracowania danego scenariusza. Poszczególne plany reakcji mogą jednak zawierać elementy wspólne. Analiza identyfikująca tego typu zależności pozwala na wdrożenie rozwiązań, które pomagają zapobiegać skutkom zjawisk destabilizujących przed ich faktycznym wystąpieniem.

2. Seminarium jako narzędzie badawcze

Analogicznie do poprzednich etapów projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości", grudniowe seminaria także zostały przeprowadzone zgodnie z metodyką wykorzystującą studium przypadku jako podstawę dalszych prac badawczych. Ponieważ uczestnicy wykształcili już umiejętności pracy nad studium przypadku podczas poprzednich etapów projektu, prace badawcze w ramach niniejszego cyklu seminariów zostały znacznie zintensyfikowane poprzez zwiększenie liczby studiów przypadków, które poddano analizie. Całość wysiłków naukowych wykonanych w ramach seminariów zorganizowanych w grudniu 2018 roku ukierunkowana była na analizę zjawiska przestępczości przyszłości oraz opracowanie możliwych działań prewencyjnych, które należy podjąć bezzwłocznie, aby uchronić organizacje przez jej potencjalnymi skutkami.

Następna część niniejszego rozdziału przedstawia zakres zagadnień poruszonych w ramach każdego z paneli seminariów, a ostatnia prezentuje opis kompetencji zaproszonych ekspertów, a także ewaluację treści merytorycznej wystąpień oraz sposobu organizacji seminariów, którą przeprowadzono na podstawie ocen uczestników.

2.1. Faza wstępna

Niniejsza faza prac badawczych miała na celu nie tylko odpowiednie przygotowanie wszystkich uczestników seminariów do przeprowadzenia analiz, ale również odpowiedni dobór treści, aby dyskusje prowadzone podczas

seminariów w jak najwyższym stopniu wpisywały się w tematykę przeciwdziałania przestępczości przyszłości. W związku z powyższym zaproszeni eksperci zostali poproszeni o wybór adekwatnych dla rozważanych zagadnień studiów przypadków, a uczestnicy otrzymali stosowne zalecenia mające na celu ukierunkowanie procesu analizy indywidualnej.

2.1.1. Wybór studium przypadku

Motywem przewodnim grudniowych seminariów była analiza zagadnień związanych z przeciwdziałaniem potencjalnym rodzajom przestępstw, które mogą wystąpić w przyszłości. Aby właściwie ukierunkować dyskusje seminaryjne oraz przygotować uczestników do prowadzenia prac badawczych, zaproszeni eksperci dokonali wyboru studiów przypadków, których analiza przyczyniła się do lepszego poznania przyczyn i rodzajów przestępczości, które mogą wystąpić w przyszłości. Podczas procesu selekcji przypadków eksperci wzięli pod uwagę uwarunkowania właściwe dla każdego z rozważanych sektorów oraz ich cechy wspólne, aby zagwarantować, że wybrane opracowania zajmują się zarówno problemami przekrojowymi, jak i kwestiami charakterystycznymi dla poszczególnych sektorów. Zestawienie wybranych studiów przypadku wraz z podziałem na poszczególne grupy tematyczne zostało zawarte w poniższej tabeli (zob. tabela 1).

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

SEKTOR	STUDIUM PRZYPADKU
SEKTOR FINANSOWY	• *Jeffrey Skilling, Bernie Madoff the monster & the other smartest guys of the room* • *Mommy-track Backlash* • *Fast building (A)* • *Eurofirms: difficult decisions* • *Fighting corruption at Siemens*
SEKTOR UBEZPIECZEŃ	
SEKTOR ENERGETYKI	
ZARZĄDZANIE LUDŹMI W ORGANIZACJACH	• *Hausser Food Products Company* • *Jeffrey Smith* • *Eurofirms: difficult decisions* • *Fast building (A).* • *Fighting corruption at Siemens*

Odniesienia do wybranych studiów przypadków można znaleźć w rozdziale poświęconym tematyce seminariów (zob. rozdział 2.2.4).

2.1.2. Indywidualna analiza studiów przypadków

Przed rozpoczęciem wspólnych prac w ramach seminarium uczestnicy przeanalizowali we własnym zakresie materiały udostępnione im przez zaproszonych ekspertów. Szczególnej uwadze uczestników polecono artykuł autorstwa Pierre'a Wacka pod tytułem *Scenarios: Shooting the Rapids*[10] poświęcony zagadnieniu planowania scenariuszowego, które stanowi jeden z filarów grudniowych seminariów.

Aby odpowiednio przygotować się do dyskusji, uczestnicy poświęcili także czas na lekturę studiów przypadków, na których miały opierać się dalsze prace na seminariach, oraz przeprowadzenie indywidualnych analiz jakościowych dotyczących zagadnień z zakresu kultury zgodności. Uczestnicy kierowali się przy tym wytycznymi otrzymanymi od organizatorów seminariów.

2.2. Seminaria

Schemat seminariów przeprowadzonych w ramach cyklu grudniowego nie odbiegał znacząco pod względem aspektów organizacyjnych od pozostałych etapów projektu. Jednak doświadczenie w pracy nad studiami przypadków nabyte przez uczestników podczas wcześniejszych seminariów pozwoliło na zintensyfikowanie prac badawczych. Analizie poddano większą liczbę historii przypadków, co zaowocowało zwiększeniem różnorodności uzyskanych rezultatów.

Niniejszy rozdział został poświęcony założeniom organizacyjnym przyjętym na potrzeby seminariów oraz ich przebiegowi. Seminaria zostały wykorzystane jako narzędzia badawcze, pozwalające na sformułowanie wniosków oraz zaleceń w kontekście hipotetycznych przyczyn i rodzajów przestępczości,

[10] P. Wack, *Scenarios: Shooting the Rapids*, „Harvard Business Review", 1.11.1985, https://hbr.org/1985/11/scenarios-shooting-the-rapids

które mogą wystąpić w przyszłości, oraz przygotowania odpowiednich środków zaradczych. Niniejszy rozdział przedstawia przed wszystkim etapy oraz cele analizy przeprowadzonej przez uczestników (zob. rozdziały 2.2.1–2.2.3), zakres tematyczny seminariów z uwzględnieniem poszczególnych paneli (zob. rozdział 2.2.4), a także opis kompetencji zaproszonych ekspertów (zob. rozdział 2.2.4).

2.2.1. Praca w grupach

Prace grupowe przeprowadzone w ramach niniejszego etapu projektu zostały zorientowane na opracowanie planów możliwych działań przygotowawczych odpowiadających na nowe rodzaje przestępstw, które mogą zaistnieć w przyszłości. Analiza przeprowadzona przez uczestników poprzedzona była wprowadzeniem tematyki planowania scenariuszowego przez prof. Michaela Rosenberga, który przedstawił również założony schemat oraz cel badania. Uczestnicy seminariów przeznaczonych dla poszczególnych sektorów zostali podzieleni na grupy liczące do 10 osób. Ich zadaniem było zidentyfikowanie możliwych problemów o charakterze przestępczym, które mogą wystąpić w przyszłości, oraz opracowanie stosowanych działań zaradczych. W trakcie prac dyskusji poddano również celowość oraz zakres stosowalności planowania scenariuszowego jako narzędzia pozwalającego na przygotowanie organizacji do mierzenia się z wyzwaniami przyszłości. Efekty przeprowadzonych prac posłużyły jako punkt wyjścia do dalszej dyskusji w szerszym gronie uczestników i ekspertów oraz sformułowania wniosków oraz zaleceń zawartych w dalszych rozdziałach niniejszego raportu.

2.2.2. Praca nad studiami przypadków w grupach

Grupowa praca nad studiami przypadków stała się dla uczestników okazją do wymiany silnie kontrastujących poglądów na temat roli, którą pełnić powinna organizacja, jako pracodawca, w zakresie kształtowania relacji między pracownikami na gruncie założeń przyjętych w kodeksach oraz regulaminach organizacji. Studium przypadku *Eurofirms: Difficult Decisions* posłużyło także

za punkt wyjścia do dyskusji na temat tego, czy możliwe jest kształtowanie wizji strategicznej organizacji wyłącznie na podstawie wysokich standardów etycznych. Ważnym rezultatem tych prac było zakwestionowanie hipotezy, że instytucje publiczne, podobnie jak firmy prywatne, mogą i powinny kierować się zestawem wartości moralnych jako nadrzędnym wyznacznikiem dla podejmowanych działań. Aby zapewnić warunki sprzyjające dyskusji oraz swobodnej wymianie poglądów, uczestnicy zostali podzieleni na małe grupy liczące od 5 do 9 osób. Wykorzystanie różnorodnego doświadczenia i kompetencji każdego z uczestników zagwarantowało kompleksowy charakter przeprowadzonej analizy. Dyskusja przeprowadzona w ramach niniejszego etapu nie doprowadziła do sformułowania wspólnego stanowiska wszystkich uczestników, ale stanowiła wartościowy przyczynek do analizy przeprowadzonej w ramach dyskusji plenarnej.

2.2.3. Praca w grupach plenarnych

Rezultaty wypracowane wskutek prac przeprowadzonych podczas poprzednich części seminariów zostały poddane dalszej dyskusji w trakcie sesji plenarnej. Jednym z tematów przewodnich sesji moderowanej przez prof. Mireię Las Heras było wykorzystanie kultury zgodności do promowania w organizacjach postaw praworządności na rzecz przeciwdziałania przestępczości. Szczególną uwagę uczestników zwróciła koncepcja organizacji opartej na wartościach, którą przedstawił gość specjalny, Pan Miquel Jorda, absolwent IESE Business School oraz bohater studium przypadku *Eurofirms: Difficult Decisions*[11]. Całość prac przeprowadzonych w ramach dyskusji plenarnych stanowiła twórcze podsumowanie pozostałych części seminariów, co nie byłoby możliwe bez udziału zaproszonych ekspertów oraz pracy przygotowawczej wykonanej przez uczestników podczas poprzednich etapów pracy grupowej. Przeprowadzona na podstawie studiów przypadków analiza pozwoliła sformułować spostrzeżenia, wnioski oraz zalecenia końcowe dotyczące identyfikacji przyczyn występowania przestępczości

[11] J. Lagos Garcia de la Huerta, A. Miguel Angel, M. Las Heras, *Eurofirms: Difficult Decisions*, „IESE", 2018, nr DPO-430-E.

w Polsce, które zostaną podsumowane w kolejnych rozdziałach niniejszego raportu (zob. rozdziały 2.3.3 i 3).

2.2.4. Profile prelegentów

W niniejszym rozdziale zaprezentowane zostały sylwetki zaproszonych ekspertów, ze szczególnym uwzględnieniem ich kompetencji oraz doświadczenia, w tym udokumentowanego dorobku naukowego. Do udziału w wykładach zaproszeni zostali znani na całym świecie eksperci o ugruntowanej pozycji, zarówno w świecie naukowym, jak i biznesowym. Reprezentują różne dziedziny, ale ich dokonania cieszą się powszechnym uznaniem. Ich doświadczenie obejmuje pracę na rzecz rządów i międzynarodowych przedsiębiorstw. Eksperci zaproszeni do udziału w niniejszym etapie projektu wykładają na co dzień w Harvard Business School, IESE Business School oraz SRI International. Poniżej przedstawiono ich biogramy oraz skrócone opisy kompetencji. Bardziej szczegółowe opisy, wraz z listami wybranych publikacji, znaleźć można w załączniku do niniejszego raportu (zob. załącznik A).

Paul Healy

Profesor Healy dołączył do Harvard Business School w 1998 roku. Wcześniej przez 14 lat pełnił funkcję naukowo-dydaktyczną w Massachusetts Institute of Technology Sloan School of Management, gdzie w latach 1991, 1992 i 1997 był regularnie nagradzany za znakomitą pracę dydaktyczną. Jest autorem wielu publikacji w renomowanych czasopismach, a za swoją pracę naukową został uhonorowany licznymi nagrodami. Jest także współautorem książki dotyczącej analityki finansowej. Jego wykłady dotyczą przede wszystkim rachunkowości, analizy finansowej, rad nadzorczych i etycznego przywództwa. Prowadzi też kursy w ramach programów kształcenia Master of Business Administration (MBA).

Jego zainteresowania naukowe obejmują szeroki wachlarz tematów, w tym analizę finansową, etykę biznesu oraz badania zjawisk korupcyjnych. Profesor Healy ukończył studia z zakresu finansów i rachunkowości na Uniwersytecie Wiktorii w Nowej Zelandii. Stopień doktora uzyskał w roku 1981 w University of Rochester.

Mireia Las Heras

Biogram prof. Las Heras umieszczono w raporcie z wrześniowych seminariów 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".

Michael Rosenberg

Biogram prof. Rosenberga umieszczono w raporcie z wrześniowych seminariów 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".

Roland Stephen

Doktor Stephen ma ponad 20 lat doświadczenia w zarządzaniu projektami, tworzeniu planów strategicznych oraz ocenie skuteczności działania instytucji i programów badawczych w kontekście rozwoju i wspierania innowacyjności. Jego najważniejsze dokonania obejmują opracowanie nowego podejścia do oceny regionalnych systemów promowania innowacyjności oraz utworzenie nowatorskiego systemu oceny pracowników sektora energetycznego opartego na analizie umiejętności. Angażuje się też w szereg projektów dotyczących rozwoju gospodarczego opartego na technologii i innowacjach oraz różnicowania planów rozwojowych dużych miast przemysłowych.

Zanim dołączył do SRI International był profesorem na Uniwersytecie Karoliny Północnej, gdzie prowadził program badawczy dotyczący dopasowania programów uniwersyteckich do ekonomicznych celów rozwojowych poszczególnych regionów geograficznych, a także badania dotyczące wspierania rozwoju biznesów intensywnie wykorzystujących nowoczesne technologie poprzez odpowiednie polityki innowacyjności oraz wprowadzenie innowacyjnych praktyk do obszaru infrastruktury, zarządzania pracownikami oraz finansów publicznych. Roland Stephen uzyskał stopień doktora w dziedzinie międzynarodowej i porównawczej polityki ekonomicznej na Uniwersytecie Kalifornijskim w Los Angeles (USA), a licencjat (B.A.) z historii i ekonomii uzyskał na Uniwersytecie w Cambridge w Wielkiej Brytanii.

Antonino Vaccaro

Profesor Vaccaro pełni funkcję adiunkta na Wydziale Etyki Biznesu (*Department of Business Ethics*) oraz w Zespole ds. Nauki Negocjacji (*Negotiation Teaching Unit*) w IESE Business School. Jest dyrektorem ds. akademickich w centrum badań nad rolą biznesu w społeczeństwie (*Center for Business in Society*) oraz w ramach platformy badań nad społecznymi innowacjami i przedsiębiorczością (*Social Innovation and Social Entrepreneurship*). Ponadto pełni funkcję dyrektora ds. akademickich w licznych programach edukacyjnych dostosowanych do potrzeb międzynarodowych korporacji i instytucji edukacyjnych.

Jego badania były publikowane w wiodących recenzowanych czasopismach naukowych, takich jak *Academy of Management Journal*, *Research Policy*, *Technological Forecasting and Social Change*, *Journal of Management Studies*, *Ethics and Information Technology*, *Journal of Business Ethics*, czy *The Information Society*.

Profesor Vaccaro prowadził liczne projekty doradcze oraz badania stosowane dla różnych instytucji UE, ONZ oraz międzynarodowych korporacji, takich jak Southern Company (USA), Volkswagen Autoeuropa, CNIM (Francja), Artsana Group (Włochy), Alcoa (USA), Alcoa Defense (USA), REWE (Niemcy), Zaiput Technologies (USA), czy Tecnoreef (Włochy). Zasiada także w zarządach europejskich i amerykańskich start-upów i udziela porad w zakresie rozstrzygania sporów międzynarodowych.

Stopień doktora uzyskał w Instituto Superior Técnico w Lizbonie, w dziedzinie inżynierii przemysłowej i zarządzania, a karierę naukową kontynuował w ramach programów badawczych w Carnegie Mellon University oraz na Uniwersytecie w Oxfordzie (odpowiednio w obszarze polityki etyki i technologii oraz etyki w informatyce). Uzyskał także tytuł magistra inżyniera na Politechnice Mediolańskiej.

2.2.5. Zakres tematyczny seminariów

Going beyond compliance: caring for employees and their families

Uczestnicy panelu rozmawiali o tym, jak zagwarantować równe traktowanie pracowników, dbając jednocześnie o realizację strategii organizacji oraz

wartości determinujące jej kulturę organizacyjną. Jedną z takich wartości jest dbałość o dobro pracownika, czyli główny temat studium przypadku *Mommy-track Backlash*[12].

Kanwą dla omówionego przypadku był konflikt, który miał miejsce w zespole jednego z międzynarodowych dostawców oprogramowania. Dotyczył sytuacji, w której pracująca matka korzystała ze specjalnych przywilejów, które nie przysługiwały pracownikom, którzy nie posiadali dzieci (m.in. wolne piątki, ograniczona konieczność podróży służbowych, przydział do projektów wymagających mniejszego zaangażowania). Bezdzietni pracownicy twierdzili, że macierzyństwo nie różni się znacząco od innych przedsięwzięć (np. realizacji pasji czy hobby), którymi mogliby zajmować się w czasie wolnym, gdyby otrzymali podobne przywileje. Jednak zdaniem zarządu organizacji przyznanie takich samych przywilejów wszystkim pracownikom spowodowałoby, że organizacja straciłaby zdolność do realizacji celów operacyjnych w dotychczasowym zakresie.

Udział w tej dyskusji wzięli uczestnicy seminarium dedykowanego sektorowi energetycznemu oraz sektorowi ubezpieczeń. Traktując studium przypadku jako punkt wyjścia, dokonali identyfikacji oraz syntezy następujących problemów:

1. Organizacja dyskryminowała pracowników ze względu na rodzicielstwo poprzez przyznanie specjalnych przywilejów pracownikom będącym rodzicami i pozbawienie takich przywilejów pozostałych pracowników.
2. Ciężar odpowiedzialności za realizację części zadań zleconych pracownikom uprzywilejowanym został samoistnie przeniesiony na pozostałych pracowników bez ich wyraźnej zgody.
3. Element misji organizacji, którym stała się ochrona rodzicielstwa, nie był komunikowany pracownikom w chwili, gdy podejmowali oni zatrudnienie w organizacji.

Biorąc pod uwagę powyższe problemy, uczestnicy dyskusji zaproponowali następujące działania zaradcze:

1. Kodeks etyczny organizacji, regulamin pracy oraz regulamin wynagrodzeń powinny być tworzone z uwzględnieniem podstawowego

[12] A.M. Hayashi, *Mommy-track Backlash*, „Harvard Business Review", 2001, t.79, nr 3.

założenia, że wszystkich pracowników należy traktować sprawiedliwie. Nie oznacza to, że wszyscy pracownicy powinni być traktowani identycznie, ale wymaga takiego podejścia, które nie dopuszcza do powstawania asymetrii w zakresie wymagań lub wynagrodzenia na podstawie przynależności do uprzywilejowanej grupy społecznej.

2. Należy dopuścić elastyczne metody kształtowania regulaminu pracy i polityki płacowej, co umożliwi realizację celów operacyjnych organizacji przy zachowaniu dbałości o dobro wszystkich pracowników.

Wymienione powyżej kodeksy i regulaminy, jak również wszelkie elementy misji organizacji, które rzutują na zakres zaangażowania pracowników w sposób bezpośredni i niebezpośredni, muszą być wyraźnie komunikowane potencjalnym pracownikom w momencie, gdy podejmują decyzję o podjęciu pracy w organizacji.

Scenario planning: imagining the future

Celem tego panelu było przedstawienie roli planowania scenariuszowego w zarządzaniu strategicznym jako jednego z podstawowych narzędzi realizacji metodologii *Be Lean – Be a Team – Be Ready* wprowadzonej przez prof. Adriana Done'a. Podczas spotkania zwrócono uwagę na problem nieprzewidywalności przyszłości w kontekście konieczności tworzenia scenariuszy strategicznych w ramach przestrzeni wyznaczonej przez zdarzenia, których wystąpienie jest prawdopodobne w obrębie danej organizacji, ekosystemu, w którym funkcjonuje, a także w perspektywie globalnej. Opracowane scenariusze pozwalają na podjęcie zaplanowanych działań strategicznych w przypadku wystąpienia któregokolwiek z przewidzianych zdarzeń, a także natychmiastowe wdrożenie tych elementów, które były wspólne dla wszystkich scenariuszy. Za zasadne uznano rozważanie zarówno scenariuszy nadmiernie optymistycznych, jak i nadmiernie pesymistycznych, uznając je za warunki graniczne dla tworzenia właściwych scenariuszy.

Jeffrey Skilling, Bernie Madoff the monster & the other smartest guys of the room

Studium przypadku zatytułowane *Jeffrey Skilling, Bernie Madoff the Monster & the Other Smartest Guys of the Room*[13] zostało wykorzystane do omówienia czynników sprzyjających nadużyciom w organizacjach. Panel prowadził prof. Antonino Vacarro, a jego celem było przeprowadzenie analizy mechanizmów odpowiedzialnych za nieetyczne działania w organizacjach. W ramach wprowadzenia zaproszony ekspert przedstawił uczestnikom pojęcie neutralizacji odpowiedzialności (ang. *neutralization*) oraz koncepcję etycznej równi pochyłej (ang. *ethical slippery slope*) w kontekście nadużyć oraz przestępczości w organizacjach. Kolejnym zagadnieniem omówionym w ramach panelu był konflikt interesu jako nadrzędny czynnik ryzyka. Problem konfliktu interesu oraz związane z nim możliwości nadużyć oraz ich skutki zostały zilustrowane zaczerpniętymi ze studium przypadku przykładami nieetycznej działalności Bernard L. Madoff Investment Securities, a także Enron Corporation i firmy doradczo-audytorskiej Arthur Andersen LLP. Druga część panelu została poświęcona dyskusji nad czynnikami sprzyjającymi nieetycznym postawom oraz występowaniu nadużyć. W ramach analiz przeprowadzonych przez uczestników seminarium razem z zaproszonym ekspertem zidentyfikowano trzy rodzaje wzajemnie sprzężonych czynników sprzyjających działaniom o charakterze przestępczym:

- czynnik finansowy,
- czynnik etyczny,
- czynnik międzyludzki (związany z relacjami międzyludzkimi).

Według uczestników seminarium dla obszaru zarządzania ludźmi w organizacjach, aby skutecznie przeciwdziałać przestępczości, należy wprowadzić do organizacji promującą praworządność kulturę zgodności, wdrożyć transparentny oraz uczciwy system wynagrodzeń, a także zadbać o odpowiednie relacje międzyludzkie już na etapie rekrutacji pracowników, np. poprzez wdrożenie dodatkowych testów psychologicznych.

[13] A. Vaccaro, T. Ramus, *Jeffrey Skilling, Bernie Madoff the Monster & the Other Smartest Guys of the Room*, „Harvard Business Review Case Study", 2008, nr IES233-PDF-ENG.

Going beyond compliance: putting people first

Tematyka panelu dotyczyła kluczowej roli wartości w budowaniu organizacji. Prof. Mireia Las Heras z IESE Business School wykorzystała do przeprowadzenia panelu studium przypadku pod tytułem *Eurofirms: Difficult Decisions*[14]. Przykład Eurofirms Group, firmy, która zajmuje się pośredniczeniem w zatrudnianiu pracowników, został przedstawiony jako przeciwwaga dla tych organizacji, które opierają swoją kulturę korporacyjną wyłącznie na osiąganiu celów i współzawodnictwie. Właściwe kryteria doboru pracowników pozwoliły na zbudowanie dobrze prosperującej organizacji, której działalność została oparta za zaufaniu oraz założeniu dochowania wierności wyśrubowanym standardom etycznym. W dyskusji wziął udział założyciel Eurofirms Group, Pan Miquel Jorda, dzięki czemu uczestnicy panelu mogli lepiej zrozumieć, jakie trudności napotyka się, budując organizację opartą na wartościach.

Uczestnicy sformułowali w ramach panelu następujące wnioski:

- organizacja oparta na wartościach stanowi skuteczną metodę na promowanie praworządności, a tym samym przeciwdziałanie skłonnościom do popełnienia przestępstw,
- kluczowym elementem budowania organizacji opartej na wartościach jest właściwy proces rekrutacji, obejmujący przede wszystkim wyższą i średnią kadrę kierowniczą, ale również szeregowych pracowników,
- proces rekrutacji w organizacji opartej na wartościach powinien obejmować nie tylko kompetencje potencjalnego pracownika oraz jego gotowość do podejmowania inicjatyw, ale również wyznawane przez niego wartości,
- koszty procesów kontrolnych w organizacji mogą przewyższyć potencjalne straty wynikające z zaistnienia przestępstwa, dlatego bardziej efektywną metodą przeciwdziałania przestępczości jest budowanie postaw opartych na poczuciu praworządności,
- czynnik wartości może pełnić rolę jednego z elementów przewagi konkurencyjnej organizacji,
- organizacja oparta na wartościach ma znaczenie uniwersalne i może nią być zarówno administracja publiczna, jak i przedsiębiorstwo prywatne.

[14] J. Lagos Garcia de la Huerta, A. Miguel Angel, M. Las Heras, *Eurofirms: Difficult Decisions*, op.cit.

Going beyond compliance: when times change

Przypadek opisany w studium *Hausser Food Products Company*[15] pokazuje, jak istotna jest kwestia motywowania pracowników do podążania za zmianami zachodzącymi w organizacji, a także udoskonalanie procesów biznesowych, dostosowujących organizację do zmieniających się warunków rynkowych. Historia przedstawiona w studium zwraca uwagę na rolę czynników pozapłacowych, które zapewniają pracownikom poczucie przynależność, a tym samym świadomość współodpowiedzialności za realizację strategii organizacji.

Firma Hausser Food Products Company[16] jest wiodącym amerykańskim producentem i dystrybutorem żywności przeznaczonej dla dzieci w wieku przedszkolnym, w tym noworodków. Posiada ugruntowaną pozycję w branży (w ostatnich latach utrzymuje stabilny udział w rynku żywności dla dzieci na poziomie ok. 60%) i jest znana z dobrej jakości oferowanych produktów. Pomimo dobrze rozwiniętej sieci dystrybucji i rozpoznawalnej marki, firma musi mierzyć się z trudnościami spowodowanymi przez fundamentalne zmiany zachodzące na rynku. Niż demograficzny (nagły, niedający się przewidzieć spadek liczby narodzin) spowodował, że zarząd organizacji odnotował zauważalny spadek sprzedaży oraz powiązane z tym zmniejszenie zysków. Jednak w organizacji istnieje jedna grupa regionalna, która regularnie realizuje założone cele sprzedażowe, pomimo że funkcjonuje w podobnych realiach rynkowych jak inne zespoły. Zarząd firmy nie potrafi wskazać przyczyn takiego stanu rzeczy, a zespół odnoszący sukcesy nie jest skłonny do ujawnienia faktycznych powodów dla osiąganych wyników sprzedaży.

Uczestnicy seminarium określili, jakie przyczyny doprowadziły do zaistnienia opisanej powyżej sytuacji. Można je traktować jako zestaw uniwersalnych problemów, które dotykają organizacje o podobnej strukturze organizacyjnej:

1. Faktycznym źródłem innowacji w organizacji są pracownicy niższego szczebla (tutaj: sprzedawcy podlegający dyrektorom regionalnym).

---

[15] N. Capon, *Hausser Food Products Company*, 2008, Cases at Columbia Business School, nr ref.: CCW080503.

[16] Analizowane tu studium przypadku dotyczy autentycznego przedsiębiorstwa, a fikcyjna nazwa Hausser Food Products Company została zastosowana w celu ochrony tajemnicy przedsiębiorstwa.

2. Po przeprowadzeniu analizy struktury organizacji oraz regulaminu wynagradzania i premiowania uczestnicy uznali, że organizacja nie traktuje pracowników w sposób sprawiedliwy, ponieważ uzależnia od wyników sprzedaży jedynie premie osób pełniących stanowiska kierownicze.
3. W związku z tym wśród pracowników wytworzyło się uzasadnione przekonanie o tym, że warto być bardziej lojalnym wobec grupy swoich najbliższych współpracowników (tutaj: grupy regionalnej) niż organizacji jako całości.

W trakcie panelu omówiono także narzędzia pozwalające rozpowszechniać i promować kulturę organizacji wśród pracowników. Wykazano również, że odpowiedzialność organizacji jako pracodawcy nie jest ograniczona do zabezpieczenia potrzeb materialnych pracownika, ale wiąże się z koniecznością utworzenia takiego środowiska pracy, które zapewnia poczucie stabilności i bezpieczeństwa, stymulując pracownika do rozwoju osobistego i zawodowego.

Going beyond compliance: leadership and development of trust

Panel poprowadziła prof. Las Heras. Został poświęcony problemowi podejmowania decyzji w warunkach występowania wykluczających się kryteriów, gdy skutki podjętej decyzji rzutują w istotny sposób na sytuację materialną organizacji i mogą być źródłem tarć w zespole. Związane z takimi sytuacjami problemy zostały podczas panelu przedstawione i przeanalizowane na przykładzie studium przypadku *Jeffrey Smith*[17].

Opisany przypadek dotyczył sporu między członkami zarządu na temat strategii korporacji świadczącej usługi z zakresu doradztwa inwestycyjnego. Zaistniałe okoliczności zmusiły prezesa zarządu do zwolnienia z obowiązków wiceprezesa osoby odpowiedzialnej za zarządzanie portfelem aktywów inwestycyjnych. Decyzja ta wiązała się z ryzykiem pogorszenia relacji biznesowej z najważniejszym klientem organizacji, ryzykiem wycofania przez klientów znacznej części aktywów inwestycyjnych oraz utratą doświadczonego i efektywnego pracownika.

[17] H. Ibarra, J.M. Suesse, *Jeffrey Smith*, 1998, Harvard Business Publishing, nr ref.: 9-498-043.

Uczestnicy zgodzili się, że w zaistniałej sytuacji decyzja prezesa była prawidłowa. Działanie wiceprezesa uczestnicy jednogłośnie ocenili jako rażące naruszenie zaufania, którym obdarzył go zarząd oraz podlegli mu pracownicy. Zwrócono uwagę, że chociaż wszyscy pracownicy organizacji powinni być zaangażowani w proces kształtowania strategii organizacji, to jednak zarząd ponosi odpowiedzialność za wdrożenie wypracowanej strategii, a decyzje wykonawcze pracowników muszą ograniczyć się do jak najlepszej realizacji tej strategii. Wszelkie jednostkowe decyzje, które nie wpisują się w ramy całościowej strategii, stanowią zagrożenie dla stabilności organizacji oraz wprowadzają niekontrolowaną zmienność, która może otwierać przestrzeń do nadużyć.

Understanding technology, productivity, and progress: the next ten years

Panel dotyczył produktywności w kontekście prowadzenia badań naukowych oraz roli jaką odgrywa determinując postęp cywilizacyjny i zwiększając dobrobyt społeczeństw. Zwrócono uwagę na fakt, że pomimo ciągle rosnących nakładów na naukę i wysiłków publikacyjnych, poziom odkryć naukowych się obniża. Mamy obecnie do czynienia ze spadkiem produktywności rozumianej jako zdolność do pomysłowego i efektywnego przetwarzania środków produkcji – dóbr kapitałowych i inwestycyjnych – na dobra konsumpcyjne, co bezpośrednio rzutuje na zdolność społeczeństw do uzyskiwania powszechnego wysokiego standardu życia oraz ogólnej satysfakcji (dobrobytu). Zwiększanie produktywności jest zatem narzędziem służącym do eliminowania nierówności społecznych, które są czynnikiem sprzyjającym rozwojowi przestępczości. Podczas panelu zwrócono uwagę na konieczność rozwoju technologii przeznaczenia ogólnego, które pozwolą zwiększyć produktywność organizacji i ich zdolność do adaptacji w warunkach ciągłych zmian zachodzących w gospodarce i społeczeństwie.

Fighting corruption at Siemens

Ten panel został poświęcony zagrożeniom związanym z niewłaściwym zarządzaniem kulturą korporacyjną oraz odejściem od postaw opartych na praworządności. Do rozważań wykorzystano studium przypadku *Fighting*

Corruption at Siemens[18], autorstwa prof. Paula Healy'ego z Harvard Business School, który był również prelegentem oraz moderatorem podczas przeprowadzonych w trakcie panelu dyskusji. Wybrane studium przypadku dotyczy historii afery korupcyjnej związanej z niemieckim koncernem Siemens, która rozpoczęła się 15 listopada 2006 roku od aresztowania kilku pracowników spółki Siemens AG. Całe śledztwo w sprawie działalności korupcyjnej organizacji objęło przedsięwzięcia prowadzone na całym świecie, które stanowiły 60 proc. obrotów spółki. Ten przypadek został wybrany nie tylko z uwagi na skalę korupcji, ale również ze względu na sukces procesu naprawczego przeprowadzonego przez organizację w celu utrzymania zdolności operacyjnej. Śledztwa oraz postępowania karne wszczęte w Stanach Zjednoczonych oraz Niemczech zakończyły się zapłatą grzywien w wysokości 1,6 mld USD. Siemens AG poniósł również koszt śledztwa wewnętrznego (850 mln USD), w które zaangażowani byli zewnętrzni oraz wewnętrzni wykonawcy. Przeprowadzone działania doprowadziły też do zwolnienia pięciuset pracowników zamieszanych w działalność korupcyjną oraz złożenia pozwów przeciwko dziewięciu byłym członkom zarządu firmy. Jednym z kluczowych elementów dyskusji przeprowadzonej podczas seminarium była identyfikacja przyczyn eskalacji zjawiska korupcji w firmie Siemens oraz kwestia braku reakcji na symptomy. Uczestnicy seminarium oraz zaproszony ekspert zgodzili się, że jedną z głównych przyczyn wystąpienia tak dużej korupcji było wypaczenie wartości promowanych przez kulturę korporacyjną. Kolejny etap dyskusji dotyczył poszczególnych elementów procesu naprawczego, które zostały uznane za istotne w kontekście tworzenia planów naprawczych w organizacjach. Dyskusje przeprowadzone podczas panelu pozwoliły uczestnikom sformułować następujące wnioski:

- rola przywódcy jest kluczowa zarówno w procesie wprowadzania zmiany, jak i utrzymania ciągłości funkcjonowania wprowadzonego rozwiązania,
- dobór adekwatnych narzędzi kontroli kultury zgodności jest jednym z najistotniejszych elementów gwarantujących jej utrzymanie w organizacji,

[18] P. Healy, D. Petkoski, *Fighting Corruption at Siemens*, „Harvard Business School Multimedia/Video Case", 2012.

- konieczne jest prowadzenie nieustannego monitorowania oraz reagowanie w przypadku wystąpienia czynników świadczących o zwiększonej skłonności pracowników do popełniania przestępstw,
- zjawisko korupcji nie jest korzystne finansowo dla organizacji, zarówno pod względem osiąganych wyników, jak i potencjalnych kar związanych z tego typu działaniami,
- zachowanie wyższej kadry kierowniczej w odniesieniu do wdrożonych zmian jest jednym z ważniejszych elementów decydujących o tym, czy uda się utrzymać w organizacji kulturę zgodności oraz wdrożyć odpowiednie plany naprawcze,
- postawy oparte na praworządności kształtuje przekaz płynący od przedstawicieli wyższej kadry kierowniczej (ang. *tone at the top*),
- kreowanie postaw opartych na praworządności powinno współdziałać z systemem administracyjnym, który nie sprzyja postawom o charakterze korupcyjnym, włączając w to system premiowy oraz zasady współpracy z kontrahentami oraz klientami.

2.3. Faza podsumowania

Niniejszy rozdział stanowi podsumowanie prac badawczych przeprowadzonych w ramach seminariów naukowych. Podsumowanie wyników prac przeprowadzonych w ramach realizowanego etapu projektu objęło ocenę zaproszonych prelegentów (ekspertów) oraz ich wystąpień przez uczestników seminariów (zob. rozdział 2.3.1), analizę statystyczną odpowiedzi udzielonych podczas badania kwestionariuszowego (zob. rozdział 2.3.2), a także analizę wyników uzyskanych od grupy fokusowej złożonej z uczestników seminariów (zob. rozdział 2.3.3).

2.3.1. Ocena prelegentów, treści wystąpień oraz aspektów organizacyjnych seminariów

W niniejszym rozdziale uwzględniono także ocenę zakresu merytorycznego seminariów oraz ich aspektów organizacyjnych. Zaprezentowane poniżej

statystyki ocen prelegentów oraz seminariów zostały sporządzone na podstawie anonimowych kwestionariuszy ankietowych wypełnionych przez uczestników seminariów. Aby przeprowadzić kompleksową ocenę warsztatów pod względem merytorycznym oraz organizacyjnym, wyodrębniono odpowiednie kryteria, które zostały przedstawione 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

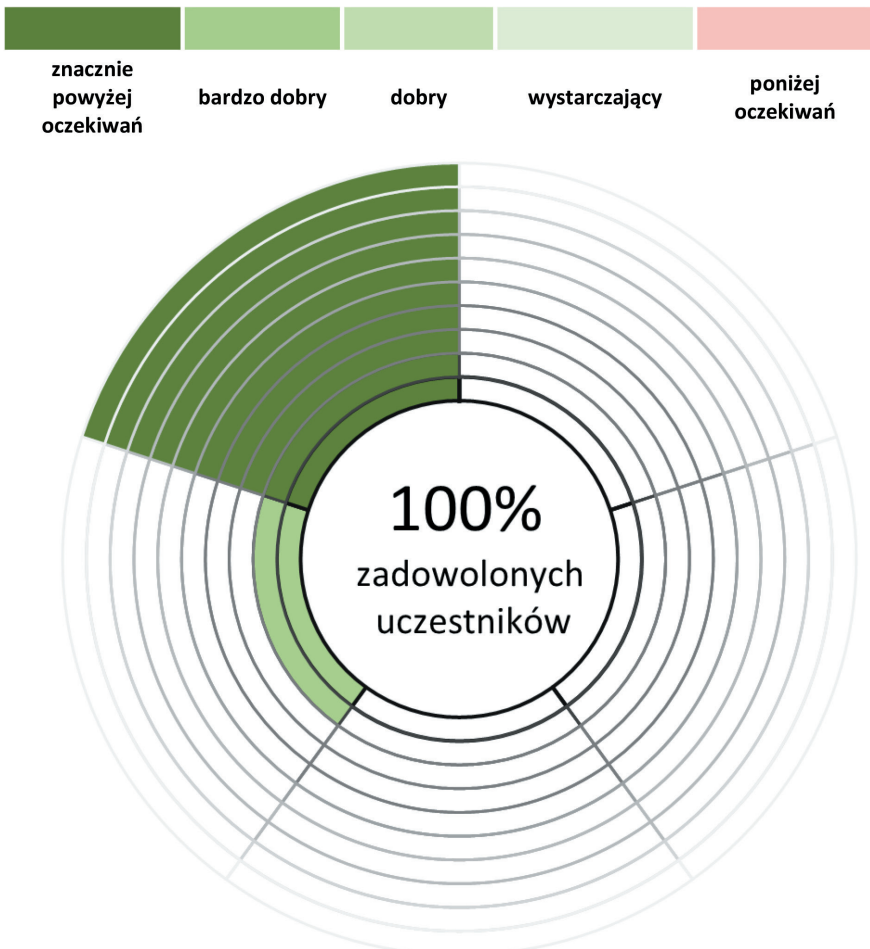
Kryterium nr 1	Standard obsługi warsztatów
Kryterium nr 2	Stan sali wykładowej oraz pomieszczeń do pracy grupowej
Kryterium nr 3	Możliwości nawiązania współpracy i nowych kontaktów
Kryterium nr 4	Jakość przerw na kawę
Kryterium nr 5	Jakość obiadów
Kryterium nr 6	Witryna internetowa projektu

Uczestnicy ocenili aspekty organizacyjne i merytoryczne seminariów według kryteriów zamieszczonych w powyższych tabelach w skali od 1 do 5. Zdobyte punkty zostały następnie podsumowane i przedstawione w formie diagramów satysfakcji uczestników[19] widocznych na poniższych ilustracjach (zob. rysunki 3–10).

[19] Diagramy opracowano na podstawie ankiet ewaluacyjnych. Oceny każdego sektora i aspektu (organizacyjnego lub merytorycznego) seminarium zsumowano według zadanej skali, tj. każdej ocenie (od 1 do 5) przyporządkowano liczbę ocen wystawionych. Dla większej przejrzystości przeskalowano liczbę wystąpień ocen do skali 10-stopniowej. Udział zadowolonych uczestników obliczono na podstawie procentowego udziału następujących ocen w całkowitej liczbie wystawionych ocen: wystarczający (2), dobry (3), bardzo dobry (4) i znacznie powyżej oczekiwań (5).

Sektor finansowy

Rysunek 3. Ocena aspektów merytorycznych seminarium dla sektora finansowego



Źródło: opracowanie własne

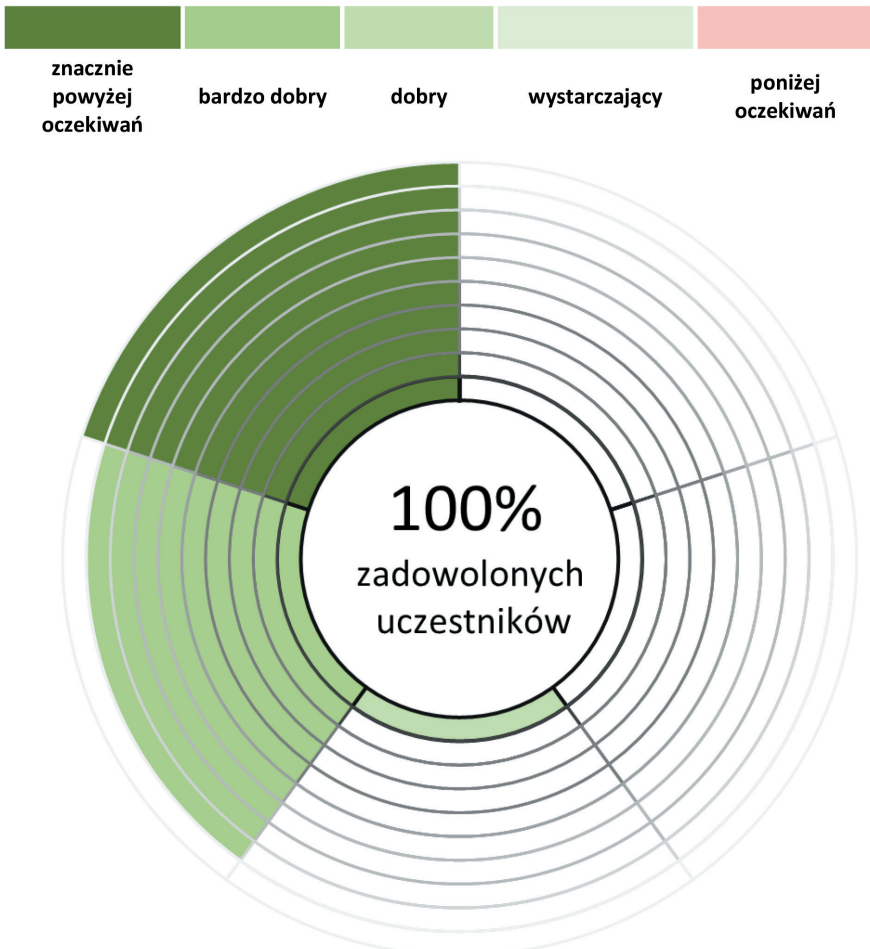
Rysunek 4. Ocena aspektów organizacyjnych seminarium dla sektora finansowego

Źródło: opracowanie własne

Uczestnicy modułu przeznaczonego dla reprezentantów polskiego sektora finansowego bardzo wysoko ocenili treści merytoryczne przeprowadzonych warsztatów. Wszyscy prelegenci otrzymali bardzo wysokie noty, tj. żadna z ocen średnich nie była niższa niż 93 procent. Szczególnie wysoko ocenione zostały prelekcje poświęcone strategii tworzenia organizacji opartej na wartościach oraz promowaniu postaw opartych na praworządności jako elemencie kultury organizacyjnej.

Sektor ubezpieczeń

Rysunek 5. Ocena aspektów merytorycznych seminarium dla sektora ubezpieczeń



Źródło: opracowanie własne

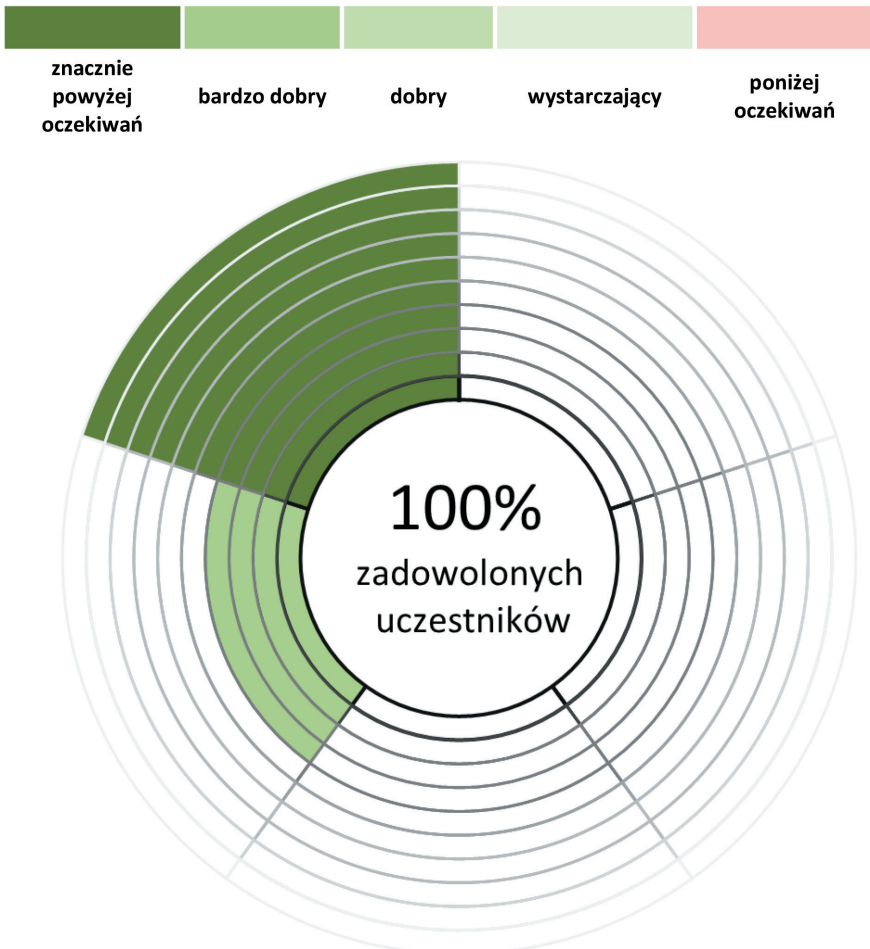
Rysunek 6. Ocena aspektów organizacyjnych seminarium dla sektora ubezpieczeń

Źródło: opracowanie własne

Przedstawiciele sektora ubezpieczeń najwyżej ocenili prelekcję profesora Michaela Rosenberga, która dotyczyła wykorzystywania planowania scenariuszowego w kontekście przeciwdziałania przestępczości w organizacjach oraz tworzenia i implementacji strategii zaradczych. Drugą najwyższą średnią ocen treści merytorycznych otrzymał profesor Paul Healy z Harvard Business School, który omawiał kwestię zmieniania podstaw kultury organizacyjnej w celu przeciwdziałania występowaniu przestępstw.

Sektor energetyki

Rysunek 7. Ocena aspektów merytorycznych seminarium dla sektora energetyki



Źródło: opracowanie własne

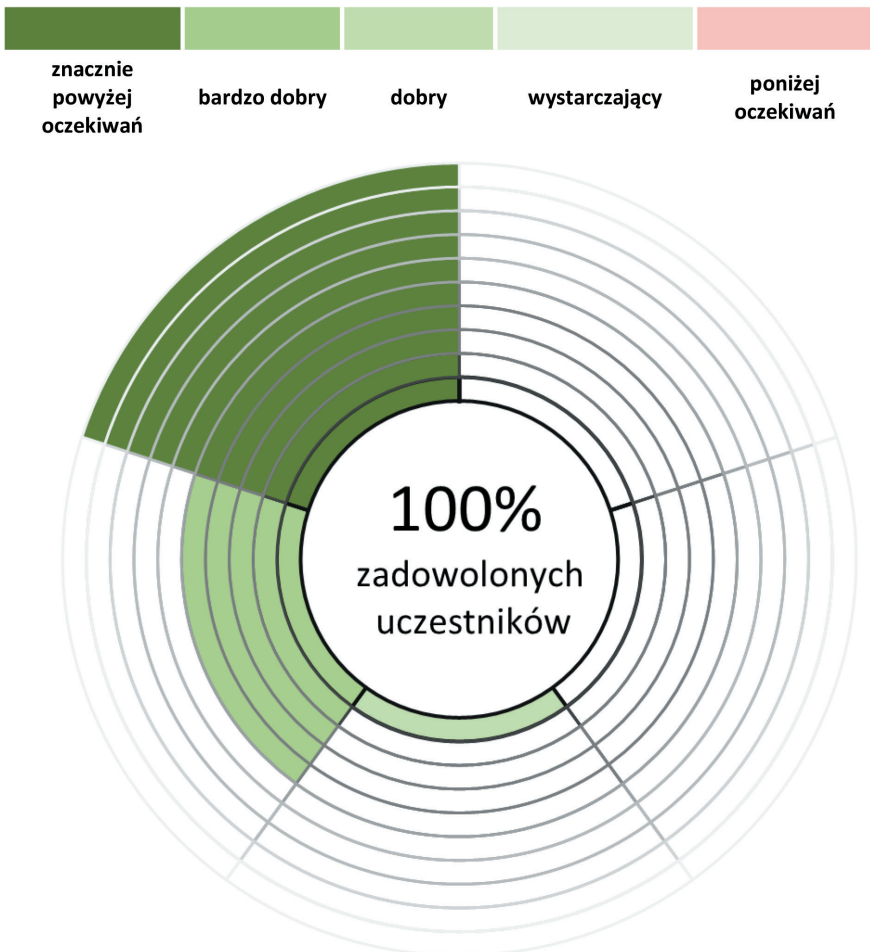
Rysunek 8. Ocena aspektów organizacyjnych seminarium dla sektora energetyki

Źródło: opracowanie własne

Reprezentanci sektora energetyki najwyżej ocenili tę część warsztatów, którą przedstawił profesor Rosenberg z IESE Business School, poświęconą roli planowania scenariuszowego w kontekście zapobiegania występowaniu przestępstw. Niemal równie wysoko oceniono wystąpienie Rolanda Stephena z SRI International, który opowiadał o roli badań naukowych w kontekście przeciwdziałania przestępczości na świecie.

Zarządzanie ludźmi w organizacjach

Rysunek 9. Ocena aspektów merytorycznych seminarium dla obszaru zarządzania ludźmi



Źródło: opracowanie własne

Rysunek 10. Ocena aspektów organizacyjnych seminarium dla obszaru zarządzania ludźmi

Źródło: opracowanie własne

Uczestnicy modułu dotyczącego obszaru zarządzania ludźmi w organizacjach najwyżej ocenili wystąpienie Paula Healy'ego, który przedstawił rolę kreowania kultury korporacyjnej w kontekście przeciwdziałania przestępczości na przykładzie procesów naprawczych wdrożonych w firmie Siemens. Drugą najwyższą notę otrzymał Michael Rosenberg, który zapoznał uczestników z metodyką planowania scenariuszowego oraz tworzenia planów prewencyjnych.

2.3.2. Analiza statystyczna w obszarze potencjalnych przyczyn występowania przestępczości oraz powstawania zagrożeń w przyszłości

Podsumowanie czwartego etapu projektu badawczego obejmowało wykorzystanie testów parametrycznych i nieparametrycznych do analizy statystycznej opinii uczestników dotyczących potencjalnych przyczyn oraz rodzajów przestępczości, które mogą wystąpić w przyszłości, a także wdrażanych przygotowań prewencyjnych. Celem pierwszego etapu analizy była weryfikacja parametrów wpływających na opinie uczestników. Druga część badania, bazująca na testach nieparametrycznych, była poświęcona identyfikacji korelacji między odpowiedziami udzielonymi na poszczególne pytania.

Istotność wpływu poszczególnych parametrów na odpowiedzi udzielone przez uczestników oszacowano na podstawie parametrycznego modelowania statystycznego bazującego na metodzie najmniejszych kwadratów, teście *t-Studenta* oraz teście *Shapiro-Wilka* weryfikującym normalność rozkładu parametrów. Analiza ta została przeprowadzona na podstawie następujących założeń:

- zmienna zależna jest funkcją liniową rozważanych parametrów,
- błąd istotności pierwszego rodzaju wynosi $\alpha = 0{,}05$,
- hipoteza zerowa zakłada brak istotności danego parametru w odniesieniu do udzielonych odpowiedzi.

Na podstawie uzyskanych danych można stwierdzić, że doświadczenie zawodowe oraz wielkość reprezentowanej przez uczestników organizacji były parametrami, które w istotny sposób wpływały na to, czy uczestnicy uważali, że organizacje, które reprezentują, mogą być w przyszłości poważnie zagrożone przez działalność przestępczą. Dla obu istotnych parametrów uzyskano współczynniki o zbliżonej wartości, co świadczy o podobnym poziomie istotności w ramach zakładanego modelu. W przypadku pozostałych zmiennych nie ma podstaw do odrzucenia hipotezy zerowej, zatem poziom ich istotności jest trudny do oszacowania, co jest również spowodowane wysoką wartością błędu standardowego dla rozważanych parametrów (zob. tabela 4).

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

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,636035	0,248232	2,562	0,0149
Typ organizacji	0,371257	0,459853	0,8073	0,4249
Wielkość organizacji	0,613636	0,234595	2,616	0,0131
Reprezentowany sektor	−0,0908415	0,215874	−0,4208	0,6765
Współczynnik korelacji R^2	0,902568			

Podobne zależności zaobserwowano dla pytania dotyczącego podatności instytucji na działalność przestępczą. Doświadczenie zawodowe oraz wielkość organizacji charakteryzują się wysoką istotnością dla udzielonych odpowiedzi. Jednak w tym przypadku wielkość organizacji ma silniejszy wpływ na odpowiedzi, co jest widoczne w wartości współczynnika (zob. tabela 5).

Tabela 5. Test istotności parametrów dla pytania nr 2 (liczba obserwacji n = 39)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,608723	0,271504	2,242	0,0314
Typ organizacji	0,000199448	0,502967	0,0003965	0,9997
Wielkość organizacji	0,809484	0,256589	3,155	0,0033
Reprezentowany sektor	−0,140586	0,236114	−0,5954	0,5554
Współczynnik korelacji R^2	0,871832			

Poprzednie pytanie dotyczyło konwencjonalnej działalności przestępczej, w tym wyłudzeń oszustw i kradzieży, a to pytanie skupia się wyłącznie na cyberatakach, co zmienia charakter uzyskanych wyników. Opinia uczestników na temat podatności instytucji na cyberataki jest zależna w istotnym stopniu jedynie od wielkości organizacji, zaś doświadczenie zawodowe, podobnie jak pozostałe parametry, nie wpływa w ramach zakładanego modelu na udzielone odpowiedzi (brak podstaw do odrzucenia hipotezy zerowej) (zob. tabela 6).

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

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,518016	0,273940	1,891	0,0669
Typ organizacji	−0,330863	0,507479	−0,6520	0,5187
Wielkość organizacji	0,617840	0,258891	2,386	0,0225
Reprezentowany sektor	0,341265	0,238232	1,432	0,1609
Współczynnik korelacji R^2	0,886088			

Na opinie uczestników w zakresie postrzegania cyberataków jako poważnego w skutkach zagrożenia dla reprezentowanej organizacji wpłynęło w sposób istotny zarówno indywidualne doświadczenie (najwyższy współczynnik), jak i wielkość reprezentowanej organizacji. W przypadku pozostałych parametrów, uzyskane dane nie pozwoliły na odrzucenie hipotezy zerowej (zob. tabela 7).

Tabela 7. Test istotności parametrów dla pytania nr 4 (liczba obserwacji n = 38)

	Współczynnik	**Błąd standardowy**	**Wynik testu**	**Wartość *pi***
Doświadczenie zawodowe	0,745753	0,253484	2,942	0,0058
Typ organizacji	0,0169128	0,467934	0,03614	0,9714
Wielkość organizacji	0,584156	0,243409	2,400	0,0220
Reprezentowany sektor	0,112866	0,219153	0,5150	0,6099
Współczynnik korelacji R^2	0,916188			

Odwrotną istotność parametrów można zaobserwować dla odpowiedzi na pytanie nr 5. Największą istotnością charakteryzuje się w tym przypadku wielkość organizacji, zaś doświadczenie uczestników stanowi parametr o porównywalnej sile (zob. tabela 8).

Tabela 8. Test istotności parametrów dla pytania nr 5 (liczba obserwacji n = 36)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,606321	0,268641	2,257	0,0310
Typ organizacji	0,654260	0,511468	1,279	0,2100
Wielkość organizacji	0,736970	0,273491	2,695	0,0111
Reprezentowany sektor	−0,449703	0,230535	−1,951	0,0599
Współczynnik korelacji R^2	0,868752			

Odpowiedzi na pytanie nr 6 były zależne w stopniu istotnym od doświadczenia zawodowego uczestników i wielkości organizacji. Wpływ reprezentowanego sektora oraz typu organizacji nie był możliwy do określenia na podstawie uzyskanych danych (zob. tabela 9).

Tabela 9. Test istotności parametrów dla pytania nr 6 (liczba obserwacji n = 36)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,700659	0,249045	2,813	0,0083
Typ organizacji	0,0128195	0,474385	0,02702	0,9786
Wielkość organizacji	0,460879	0,248849	1,852	0,0733
Reprezentowany sektor	0,135454	0,214948	0,6302	0,5331
Współczynnik korelacji R^2	0,905625			

Podobnie jak w przypadku poprzedniego pytania, na odpowiedzi udzielone na pytanie „Czy uważa Pan/Pani, że za 10 lat pojawią się nowe rodzaje przestępstw, na które będzie narażona organizacja, którą Pan/Pani reprezentuje?" dominujący wpływ miał czynnik doświadczenia zawodowego uczestników oraz wielkości reprezentowanych przez nich organizacji (zob. tabela 10).

Tabela 10. Test istotności parametrów dla pytania nr 7 (liczba obserwacji n = 38)

	Współczynnik	Błąd standardowy	Wynik testu	Wartość *pi*
Doświadczenie zawodowe	0,702642	0,203091	3,460	0,0015
Typ organizacji	0,332543	0,374909	0,8870	0,3813
Wielkość organizacji	0,616495	0,195020	3,161	0,0033
Reprezentowany sektor	0,175294	0,175586	0,9983	0,3252
Współczynnik korelacji R^2	0,958097			

Tabela 11. Wyniki analizy korelacji między udzielonymi odpowiedziami dla wybranych pytań

	nr 1	nr 2	nr 3	nr 4	nr 5	nr 6	nr 7
nr 1		**0,0000**	**0,0008**	**0,0002**	**0,0220**	0,1285	0,0503
nr 2	**0,0000**		**0,0019**	**0,0077**	**0,0001**	0,1741	0,0781
nr 3	**0,0008**	**0,0019**		**0,0000**	**0,0032**	0,0522	**0,0249**
nr 4	**0,0002**	**0,0077**	**0,0000**		**0,0206**	0,2170	**0,0061**
nr 5	**0,0220**	**0,0001**	**0,0032**	**0,0206**		**0,0193**	**0,0170**
nr 6	0,1285	0,1741	0,0522	0,2170	**0,0193**		0,8493
nr 7	0,0503	0,0781	**0,0249**	**0,0061**	**0,0170**	0,8493	

Drugim etapem przeprowadzonej analizy była identyfikacja korelacji występujących między odpowiedziami udzielonymi na pytania dotyczące potencjalnych przyczyn i zagrożeń przestępczością w przyszłości (zob. załącznik B – Kwestionariusz ankietowy). Badanie siły współzależności między odpowiedziami zostało przeprowadzone dla poszczególnych par pytań za pomocą testu nieparametrycznego z użyciem tzw. współczynnika *rho-Spearmana,* który charakteryzuje się dużą wiarygodnością i odpornością na brak rozkładu normalnego w zakresie badanego parametru. Założona hipoteza zerowa dotyczy braku korelacji między analizowanymi odpowiedziami. W powyższej tabeli umieszczono pełne wyniki, tj. uzyskane wartości *pi* dla analizowanych par pytań. Pogrubioną czcionką zaznaczono wyniki, dla których możliwe jest odrzucenie hipotezy zerowej (wartość *pi* > 0,05), co wskazuje na występowanie korelacji.

2.3.3. Analiza wyników wypracowanych z grupą fokusową w kontekście możliwych przyczyn i rodzajów przestępczości w przyszłości oraz przygotowań prewencyjnych

W ramach prac badawczych przeprowadzonych podczas seminariów naukowych, stanowiących ostatni etap projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości", przeprowadzono także zogniskowany wywiad grupowy oparty na opiniach zaproszonych ekspertów. Grupę fokusową stanowili zaproszeni uczestnicy, będący przedstawicielami kadry menadżerskiej wysokiego szczebla spółek państwowych, prywatnych przedsiębiorstw oraz administracji państwowej. Bogactwo kompetencji i doświadczeń uczestników, a także ich wnikliwe spostrzeżenia, umożliwiły właściwe ujęcie złożonych problemów rozważanych podczas seminariów.

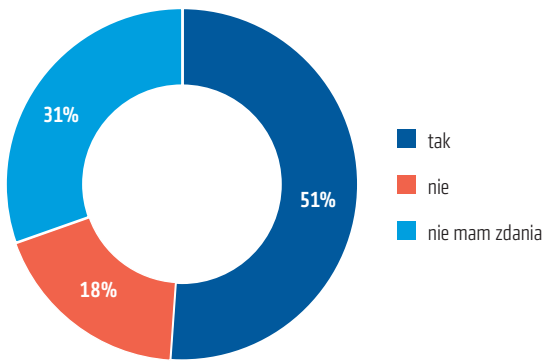
Rolę moderatorów dyskusji pełnili wybitni profesorowie międzynarodowych instytucji, w tym IESE Business School, SRI International i Harvard Business School, którzy również brali udział w dyskusjach na temat przeciwdziałania przestępczości, a ich eksperckie opinie stanowiły punkt wyjścia do omawiania poszczególnych zagadnień (zob. rozdział 2.2.4).

Celem niniejszego etapu projektu była identyfikacja potencjalnych przyczyn i rodzajów przestępczości, które mogą wystąpić w przyszłości, a także rozwój stosownego przygotowania prewencyjnego. W związku z tym przeprowadzone badanie koncentrowało się na poznaniu czynników sprzyjających wystąpieniu przestępstw, określeniu prawdopodobieństwa ich wystąpienia oraz oszacowaniu potencjalnych szkód, które mogą wywołać w przyszłości różne przestępstwa. Ponadto analiza objęła również obszary o szczególnie wysokim znaczeniu w kontekście przyszłych zagrożeń, które zostały wyróżnione na postawie opinii uczestników seminariów pełniących kluczowe role w największych polskich przedsiębiorstwach oraz agendach rządowych.

Pierwszy etap przeprowadzonej analizy poświęcony był roli planowania scenariuszowego w kontekście przeciwdziałania przestępczości, którą przybliżył uczestnikom prof. Michael Rosenberg. Zaproponowana przez eksperta metodyka została następnie poddana analizie grupowej przeprowadzonej w małych zespołach złożonych z zaproszonych uczestników, a kolejna część analizy została przeprowadzona w szerszym gronie, w czasie moderowanych dyskusji plenarnych. Końcowy etap analizy stanowiło badanie kwestionariuszowe pozwalające sformułować opis ilościowy badanych zjawisk.

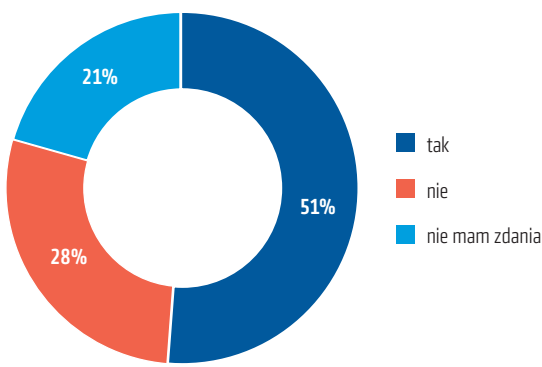
Pierwszy etap zogniskowanego wywiadu grupowego dotyczył identyfikacji skali zagrożeń wynikających z działalności przestępczej, w tym wyłudzeń, oszustw oraz kradzieży (dalej nazywanych konwencjonalną działalnością przestępczą) oraz aktualnego poziomu podatności polskich organizacji na tego typu przestępstwa.

Rysunek 11. Rozkład odpowiedzi na pytanie „Czy uważa Pan/Pani, że skutki działalności przestępczej, w tym wyłudzeń, oszustw oraz kradzieży, mogą w przyszłości poważnie zagrozić funkcjonowaniu organizacji, którą Pan/Pani reprezentuje?"



Źródło: opracowanie własne

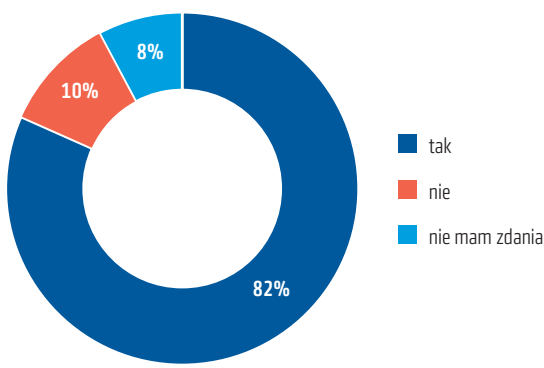
Rysunek 12. Rozkład odpowiedzi na pytanie „Czy uważa Pan/Pani, że organizacja, którą Pan/Pani reprezentuje, jest podatna na wpływ działalności przestępczej, w tym wyłudzeń, oszustw oraz kradzieży?"



Źródło: opracowanie własne

Uczestnicy sądzą, że przestępczość konwencjonalna będzie wciąż stanowić poważne zagrożenie dla funkcjonowania organizacji, które reprezentują. Warto podkreślić, że zagrożenia związane z tego typu działalnością przestępczą nie odnoszą się tylko do bezpośrednich strat finansowych, ale również niematerialnych, m.in. utraty reputacji. Uczestnicy seminariów podkreślali, że straty niematerialne stanowią często bardziej niepożądany skutek ze względu na swoje długofalowe konsekwencje, w tym utratę klientów. Na podstawie uzyskanych danych można stwierdzić, że ponad połowa uczestników uważa przestępstwa konwencjonalne za poważne zagrożenie dla funkcjonowania swoich organizacji w przyszłości (zob. rysunek 11), oraz, że reprezentowane przez nich instytucje są obecnie podatne na tego typu działalność przestępczą (zob. rysunek 12). Warto podkreślić, że oba pytania są silnie skorelowane pod względem udzielonych odpowiedzi (zob. 2.3.2), co może świadczyć, że ocena potencjalnych przyszłych zagrożeń jest silnie zależna od aktualnie panujących uwarunkowań. Analogiczna analiza została przeprowadzona dla obecnych oraz przyszłych zagrożeń wynikających z cyberprzestępczości. Następnie przeprowadzona analiza została zestawiona z danymi pochodzącymi z analogicznych badań przeprowadzonych przez uznane międzynarodowe ośrodki.

Rysunek 13. Rozkład odpowiedzi na pytanie „Czy uważa Pan/Pani, że skutki cyberataku mogą poważnie zagrozić funkcjonowaniu organizacji, którą Pan/Pani reprezentuje?"



Źródło: opracowanie własne

Na podstawie odpowiedzi uczestników oraz dyskusji przeprowadzonych w trakcie seminariów można stwierdzić, że cyberprzestępczość jest uznawana za działalność przestępczą wiążącą się z poważniejszymi reperkusjami dla funkcjonowania organizacji niż przestępczość konwencjonalna (zob. rysunek 11 i 13). Warto podkreślić, że uczestnicy stwierdzili, że reprezentowane przez nich organizacje są również bardziej podatne na cyberataki niż na konwencjonalną działalność przestępczą (por. rysunek 12 i 14).

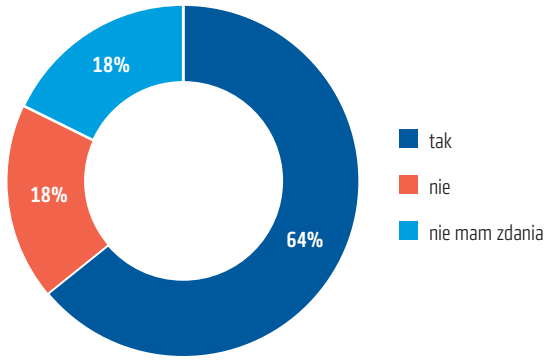
Postrzeganie cyberprzestępczości jako znacznego zagrożenia dla funkcjonowania gospodarki nie jest zjawiskiem typowym wyłącznie dla Polski. Według raportu Accenture[20] aż 74 proc. reprezentantów wyższego szczebla menadżerskiego[21] na całym świecie postrzega cyberataki jako działalność przestępczą mogącą poważnie zagrozić funkcjonowaniu organizacji oraz stanowiącą wciąż rosnące ryzyko. Opinie uczestników wskazują, że podobną tendencję można również zaobserwować w kontekście postrzegania zagrożeń związanych z potencjalnym wyciekiem danych wskutek cyberataku, szczególnie w kontekście udostępniania danych stronom trzecim za pośrednictwem infrastruktur opartych na technologii chmury[22].

[20] O. Abbosh i in., *Build Pervasive Cyber Resilience Now: Secure the Future Enterprise Today – 2018*, Accenture, 2018, https://www.accenture.com/t00010101T000000Z__w__/nz-en/_acnmedia/PDF-81/Accenture-Build-Pervasive-Cyber-Resilience-Now-Landscape.pdf

[21] W badaniu przeprowadzonym przez Accenture wzięło udział 1460 przedstawicieli kadry kierowniczej wyższego szczebla przedsiębiorstw z 16 krajów działających w 14 różnych sektorach.

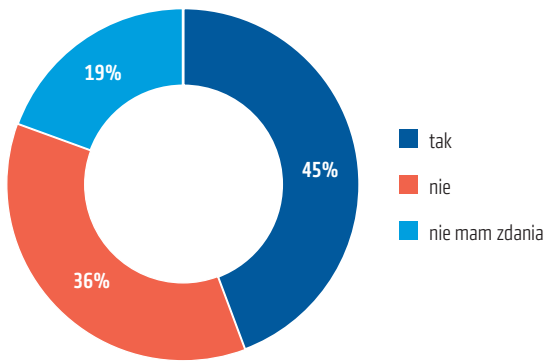
[22] O. Abbosh i in., *Build Pervasive Cyber Resilience Now: Secure the Future Enterprise Today – 2018*…, op. cit.

Rysunek 14. Rozkład odpowiedzi na pytanie „Czy uważa Pan/Pani, że organizacja, którą Pan/Pani reprezentuje, jest podatna na cyberatak?"



Źródło: opracowanie własne

Rysunek 15. Rozkład odpowiedzi na pytanie „Czy organizacja, którą Pan/Pani reprezentuje, była celem cyberataku w przeszłości?"

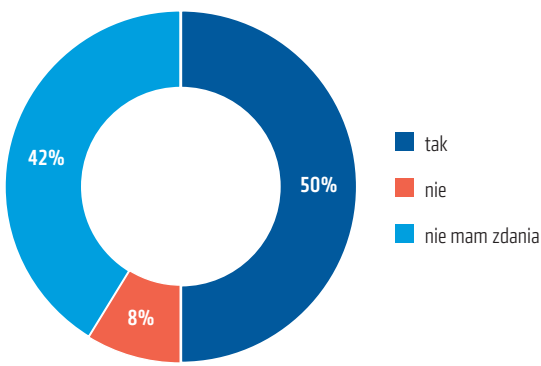


Źródło: opracowanie własne

Kolejnym zjawiskiem poddanym analizie była skala cyberataków, które mogą zostać w przyszłości przeprowadzone na polskich organizacjach. Według uzyskanych danych 36 proc. uczestników seminariów stwierdziło, że ich organizacja nigdy nie padła ofiarą cyberataku, a co piąta osoba nie miała zdania w zakresie rozważanego zjawiska (zob. rysunek 15). Biorąc pod uwagę fakt, że szacuje się, że co druga organizacja (51 proc.) na świecie padła ofiarą

cyberataku[23], poziom pewności wśród uczestników w obszarze zabezpieczenia przed cyberatakami wydaje się nie mieć odzwierciedlenia w faktycznym poziomie zabezpieczeń. Jednak ta tendencja do przeszacowywania poziomu cyberbezpieczeństwa także jest problemem obserwowanym na całym świecie. Według badań przeprowadzonych przez NTT security[24] aż 46 proc. respondentów ze Stanów Zjednoczonych twierdzi, że organizacja, którą reprezentują nigdy nie padła ofiarą cyberataku, co stanowi najwyższy odnotowany poziom pewności w stosunku do średniej światowej[25], plasującej się na poziomie 41 procent. W porównaniu z danymi światowymi Polska znajduje się nieco poniżej średniej światowej, co jest zjawiskiem korzystnym. Niepokojące jest jednak to, że stosunkowo duży procent uczestników badania nie ma zdania na temat rozważanego zjawiska, co może świadczyć o braku transparentnej polityki w zakresie cyberbezpieczeństwa. Kolejnym elementem przeprowadzonej analizy były plany dotyczące zwiększenia nakładów w obszarze przeciwdziałania przestępczości przez organizacje reprezentowane przez uczestników.

Rysunek 16. Rozkład odpowiedzi na pytanie „Czy organizacja, którą Pan/Pani reprezentuje planuje zwiększyć środki w zakresie zwalczania przestępczości?"



Źródło: opracowanie własne

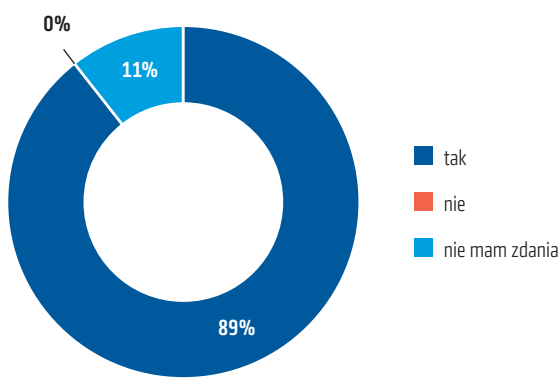
[23] *Cyber Attack Trends 2018 Mid-Year Report*, Check Point Research, 2018, https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf

[24] B. Vanson, *Prevention Is Better Than Cure: Business Security – The Journey Continues*, w: *2018 Risk: Value Report*, NTT security, 2018, https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_report_risk-value_2018_us_uea_v1.pdf

[25] W badaniu wzięło udział 1800 przedstawicieli wyższej kadry zarządzającej ze Stanów Zjednoczonych Wielkiej Brytanii, Niemiec, Austrii, Szwajcarii, Beneluksu, Szwecji, Norwegii, Hong Kongu, Singapuru oraz Australii.

Połowa ankietowanych uczestników zadeklarowała, że w reprezentowanych przez nich instytucjach planowane jest zwiększenie nakładów na działalność związaną z zapobieganiem przestępczości, ze szczególnym uwzględnieniem obszaru związanego z cyberbezpieczeństwem (zob. rysunek 16). Według badania przeprowadzonego przez Kaspersky Lab[26] aż 56 proc. organizacji na całym świecie[27] planuje zwiększenie środków wydawanych na rozwiązania dotyczące zwiększenia poziomu cyberbezpieczeństwa. Opierając się na dostępnych danych można zaobserwować, że trendy w zakresie zapewnienia cyberbezpieczeństwa w Polsce nie odbiegają znacząco od standardów światowych, co może świadczyć o globalnej skali zjawiska cyberprzestępczości. Uczestnicy seminariów stwierdzili, że rosnące zagrożenie cyberprzestępczością oraz globalny charakter tego typu działań sprawia, że konieczne staje się wykorzystanie efektów synergii uzyskiwanej w ramach szeroko zakrojonej współpracy międzynarodowej oraz adaptacji powszechnie uznanych dobrych praktyk mających na celu ograniczenie omawianego zjawiska.

Rysunek 17. Rozkład odpowiedzi na pytanie „Czy uważa Pan/Pani, że za 10 lat pojawią się nowe rodzaje przestępstw, na które będzie narażona organizacja, którą Pan/Pani reprezentuje?"



Źródło: opracowanie własne

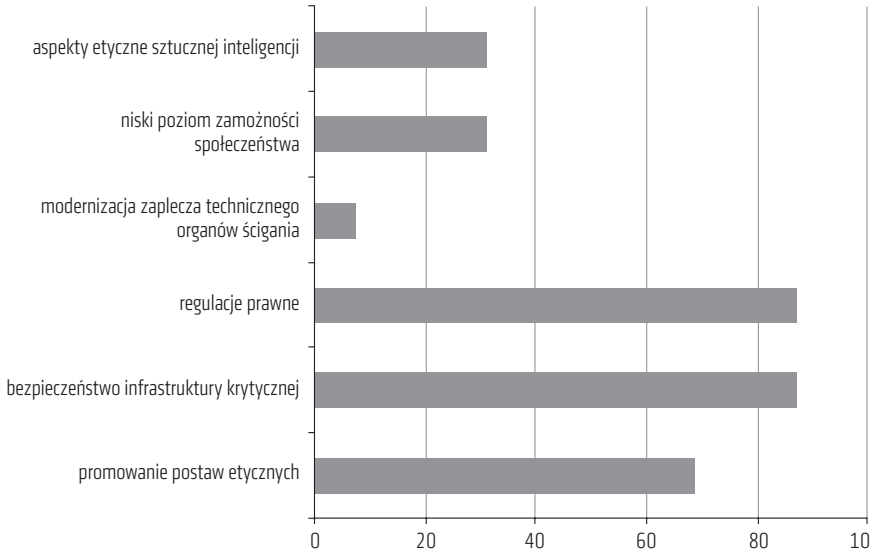
[26] W. Schwab, M. Poujol, *The State of Industrial Cybersecurity 2018*, Kaspersky Lab, CXP Group, 06.2018, https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

[27] Badanie zostało przeprowadzone wśród 320 respondentów należących do wyższej kadry zarządzającej w instytucjach z Europy, Ameryki Północnej, Ameryki Łacińskiej oraz Azji.

Dalszy etap dyskusji przeprowadzonej na seminariach dotyczył potencjalnych zagrożeń dla polskiej gospodarki związanych z nowymi rodzajami przestępstw oraz ewolucją już istniejących przejawów przestępczości. Pierwszy element przeprowadzonej analizy dotyczył prawdopodobieństwa powstania nowych przestępstw w sektorach gospodarki reprezentowanych przez uczestników Aż 89 proc. uczestników seminariów jest przekonanych, że w ciągu 10 lat pojawią się nowe rodzaje działalności przestępczej, które będą stanowiły zagrożenie dla reprezentowanych przez nich organizacji (zob. rysunek 17). Można zaobserwować, że poziom świadomości w zakresie potencjalnych przyszłych zagrożeń jest wysoki i można się spodziewać, że zaprezentowana podczas seminariów metodyka planowania scenariuszowego zostanie wykorzystana do usprawnienia działalności przedsiębiorstw w obszarze przeciwdziałania przestępczości.

Kolejnym zagadnieniem poruszonym przez uczestników były przygotowania prewencyjne mające służyć zapobieganiu wystąpienia przestępstw w przyszłości. W ramach dyskusji uczestnicy wyróżnili obszary, które wymagają szczególnej uwagi w rozważanym kontekście (zob. rysunek 18). Przeprowadzone badanie ilościowe pozwoliło zidentyfikować trzy obszary o kluczowym znaczeniu dla prawidłowego funkcjonowania polskiej gospodarki – zapewnienie bezpieczeństwa krytycznej infrastruktury, promowanie postaw etycznych oraz modernizacja zaplecza technicznego organów ścigania.

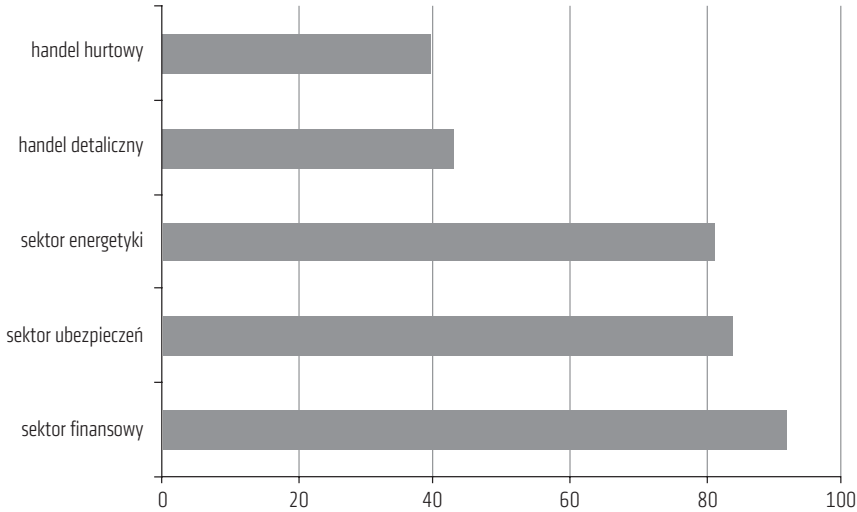
Rysunek 18. Opinia uczestników w zakresie obszarów wymagających szczególnej uwagi w kontekście zagrożeń przyszłości



Źródło: opracowanie własne

Kolejnym etapem przeprowadzonej analizy była identyfikacja sektorów polskiej gospodarki, które w przyszłości mogą być szczególnie narażone na nowo powstałe zagrożenia. Zadanie to przeprowadzono za pomocą badania kwestionariuszowego, które zobrazowało rozważane zagadnienia w sposób ilościowy. Na podstawie uzyskanych danych można stwierdzić, że najbardziej zagrożonym przez przyszłe przestępstwa sektorem będzie sektor finansowy, ze szczególnym uwzględnieniem obszaru zdalnych usług płatniczych i bankowych.

Rysunek 19. Rozkład odpowiedzi uczestników na pytanie dotyczące sektorów najbardziej narażonych na działalność przestępczą w przyszłości



Źródło: opracowanie własne

3. Wnioski seminaryjne i zalecenia w zakresie możliwych przyczyn i rodzajów przestępczości w przyszłości oraz przygotowania prewencyjne

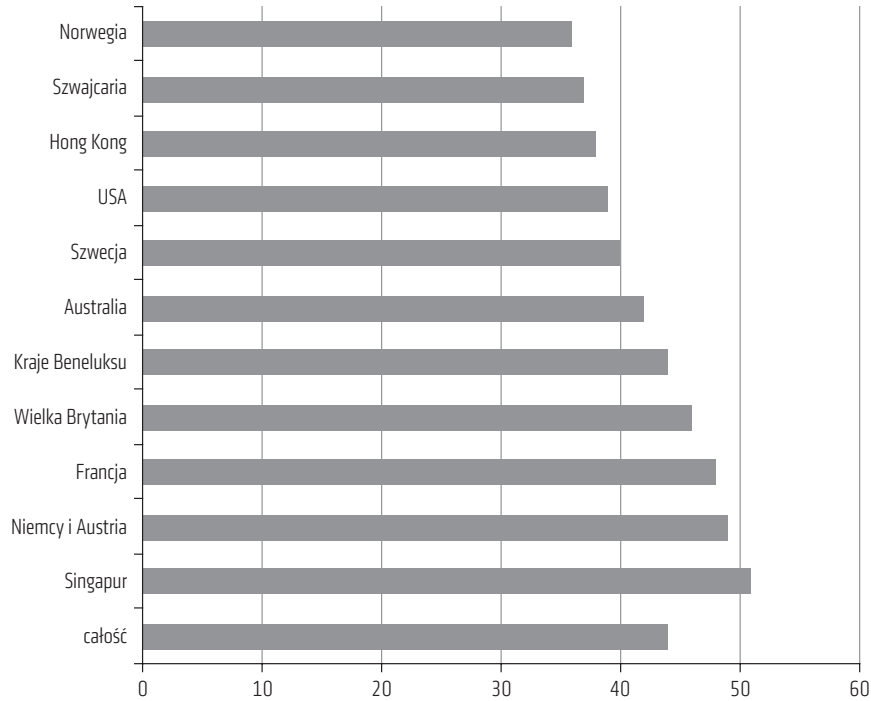
3.1. Identyfikacja przyszłych rodzajów przestępczości

W niniejszym rozdziale zawarto opracowanie wniosków sformułowanych przez uczestników seminariów na podstawie wiedzy zaproszonych ekspertów oraz aktualnego poziomu cyberbezpieczeństwa na świecie. Opracowania dokonano w zakresie fundamentalnych zagrożeń dla bezpieczeństwa cybernetycznego, które mogą się pojawić w przyszłości.

Pierwszym elementem przeprowadzonej analizy była diagnoza obecnego stanu przygotowania na zagrożenia przyszłości. Podczas dyskusji uczestnicy zauważyli, że obecny poziom cyberbezpieczeństwa w Polsce jest zdecydowanie niewystarczający (zob. rozdział 2.3.2) i większość organizacji jest w dużym stopniu narażona na potencjalne cyberataki. Obserwacje wskazują, że podobny trend jest obserwowany na całym świecie. Według Rolanda Stephena niemal co druga organizacja na świecie nie dysponuje wystarczającymi środkami do przeciwdziałania cyberatakom. Powyższą tezę potwierdza analiza przeprowadzona przez NTT Security[28], według której 44 proc. organizacji na całym świecie nie posiada wystarczających środków, aby zapobiec cyberatakom, zaś w Singapurze ponad połowa respondentów potwierdziła, że ich organizacje miały kłopoty z cyberatakami (zob. rysunek 20).

[28] B. Vanson, *Prevention Is Better Than Cure: Business Security – The Journey Continues…*, op. cit.

Rysunek 20. Udział organizacji, które nie posiadają wystarczających środków, aby zapobiec cyberatakom, z podziałem na kraje



Źródło: opracowanie własne na podstawie danych NTT Security[29]

Analizując dostępne dane, uczestnicy seminariów stwierdzili, że obecna sytuacja jest spowodowana istotną różnicą między poziomem wiedzy niezbędnym do zapobiegania cyberatakom oraz potrzebnym do przeprowadzenia samego cyberataku. Z uwagi na fakt, że do przeciwdziałania cyberprzestępczości potrzebne są dużo większe nakłady, istnieje duża dysproporcja pomiędzy przestępcami oraz istniejącymi zabezpieczeniami. Należy wdrożyć odpowiednie działania prewencyjne, których pierwszym etapem jest identyfikacja potencjalnych zagrożeń, które mogą wystąpić w przyszłości.

[29] Ibid.

Cyberataki wykorzystujące sztuczną inteligencję

Według Rolanda Stephena wykorzystanie sztucznej inteligencji (ang. *artificial intelligence*, AI). było do tej pory ograniczone ze względu na trudną dostępność infrastruktury posiadającej wystarczającą moc obliczeniową. Jednak rosnąca popularność komercyjnych produktów pozwalających na uzyskanie nieosiągalnych dotąd mocy obliczeniowych[30] zaczyna pozwalać na wykorzystanie pełnego potencjału sztucznej inteligencji. W czasie prowadzonych dyskusji uczestnicy zwrócili uwagę na ryzyko związane z potencjalną eksploatacją skonsolidowanej mocy obliczeniowej na potrzeby przeprowadzenia cyberataku wykorzystującego sztuczną inteligencję. Zaproszeni eksperci potwierdzili, że w najbliższych latach prawdopodobieństwo wystąpienia tego typu ataków będzie bardzo duże. Co więcej, z uwagi na wykorzystanie sztucznej inteligencji, tego typu ataki będą opierać się na innych niż aktualnie istniejące mechanizmach operacyjnych, co może uniemożliwić ich wykrycie dotychczas stosowanymi metodami. W związku z powyższym uczestnicy ustalili, że w celu przeciwdziałania tego typu atakom konieczne jest wdrożenie środków, które są współmierne do potencjalnych zagrożeń, tj. metod wykorzystujących AI.

Ataki za pośrednictwem Internetu rzeczy

Uczestnicy zgodnie stwierdzili, że Internet rzeczy[31] (z ang. *Internet of Things*, IoT), tj. sieć urządzeń codziennego użytku, które gromadzą, przetwarzają oraz wymieniają między sobą dane, stanowi istotne wyzwanie w obszarze bezpieczeństwa organizacji, z uwagi na swoją dynamicznie rozwijającą się architekturę. Z prognoz SRI International wynika, że w roku 2025 liczba urządzeń należących do IoT przekroczy 70 miliardów, co wpłynie nie tylko

[30] Moc obliczeniowa wyrażana jest w liczbie operacji zmiennoprzecinkowych na sekundę (ang. *floating point operations per second*, Flop/s). Szczytowe moce obliczeniowe dzisiejszych superkomputerów opartych na architekturze hybrydowej (łączącej rdzenie ogólnego przeznaczenia – CPU – z wielordzeniowymi akceleratorami przeznaczonymi do obliczeń równoległych – GPU lub rzadziej FPGA) sięgają przeciętnie dziesiątek tysięcy TFlop/s (w przypadku najszybszego superkomputera jest to ok. 200 000 TFlop/s). Akceleratory GPU, znajdujące się w powszechnej ofercie komercyjnej, pozwalają zgromadzić nieosiągalną dotąd moc obliczeniową nawet w standardowym zestawie komputerowym. Źródło: *TOP500 List – November 2018 | TOP500 Supercomputer Sites*, b.d., https://www.top500.org/list/2018/11/ (dostęp: 2.02.2019).

[31] J. Gubbi i in., *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions*, „Future Generation Computer Systems", 2013, t.29, nr 7.

na złożoność całej architektury sieci, ale również na jej zasięg. Uczestnicy seminariów podkreślali, że ułatwienia wynikające z centralizacji kontroli wielu urządzeń, która jest możliwa dzięki IoT, mogą również stanowić znaczne zagrożenie w kontekście potencjalnych kanałów ataku oraz wykorzystania rozproszonej infrastruktury do ich przeprowadzenia. Według ekspertów Internet rzeczy może być narażony na wykorzystanie przez przestępców, nie tylko jako źródło potencjalnych informacji, ale również jako narzędzie do przeprowadzenia ataków typu DDoS[32, 33]. W związku z powyższym uczestnicy zaproponowali wdrożenie odpowiedniej polityki dotyczącej używania oraz izolacji inteligentnych urządzeń, co pozwoliłoby ograniczyć możliwości zaistnienia tego typu ataków. Dodatkowo zalecenia uczestników objęły również stworzenie inicjatyw mających na celu dalsze badanie zjawiska IoT w kontekście przeciwdziałania przestępczości poprzez wykorzystanie technik podstępu, które obejmują m.in. generowanie fałszywych danych oraz wirtualnych sieci.

Cyberataki na fizyczną infrastrukturę

Roland Stephen przewiduje, że w najbliższych latach dojdzie do znacznego zwiększenia liczby cyberataków mających na celu przejęcie bądź uszkodzenie fizycznej infrastruktury, takiej jak sieci energetyczne lub telekomunikacyjne. Ten typ zagrożenia charakteryzuje się nadzwyczaj wysokim poziomem ryzyka związanego z uszkodzeniem krytycznych elementów infrastruktury, które mogłoby uniemożliwić organizacji prowadzenie dalszej działalności operacyjnej. Podczas rozważania scenariuszy przyszłości warto wziąć pod uwagę nowe kanały potencjalnego ataku, takie jak Internet rzeczy.

Fałszywe oprogramowanie antywirusowe

Uczestnicy dyskusji przeprowadzanej podczas seminariów ustalili, że potencjalne cyberzagrożenia mogą w przyszłości wykorzystywać również nowe formy znanych już technik wykorzystywanych przez złośliwe oprogramowanie. Według Rolanda Stephena z SRI International potencjalne wektory

[32] DDoS (Distributed Denial of Service) – atak, którego celem jest uniemożliwienie normalnego działania usługi sieciowej lub systemu komputerowego poprzez zajęcie dostępnych zasobów przez sieć kontrolowanych przez atakującego terminali.

[33] J. Mirkovic, P. Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, „ACM SIGCOMM Computer Communication Review", 2004, t.34, nr 2, s. 39.

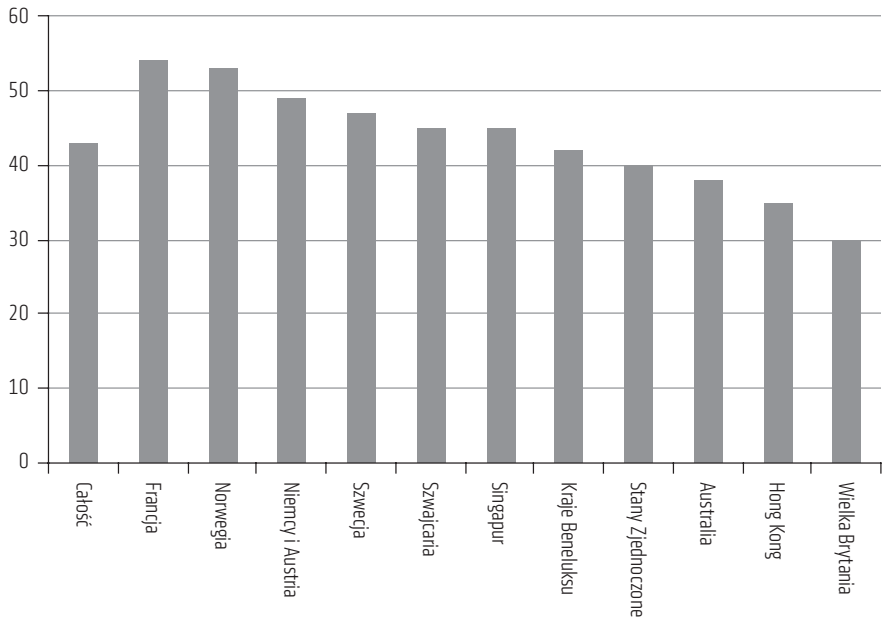
ataku mogą obejmować nieodpłatne udostępnianie fałszywych wersji popularnego oprogramowania, co pozwoli atakującemu na przejęcie kontroli nad systemem użytkownika lub dokonać kradzieży danych. Uczestnicy uzgodnili, że darmowe oprogramowanie antywirusowe stanowi najbardziej prawdopodobny wektor ataku, z uwagi na powszechność oraz różnorodność dostępnego oprogramowania, a także wysoko zindywidualizowane preferencje użytkowników końcowych. Rekomendacją zaradczą uczestników jest tworzenie w ramach organizacji wspólnej polityki dotyczącej oprogramowania użytkowego i objęcie nią prywatnych terminali użytkowników poprzez program zniżek na rekomendowane oprogramowanie.

Brak kompetencji w zakresie cyberbezpieczeństwa

Uczestnicy zgodnie twierdzą, że brak odpowiednich umiejętności w zakresie cyberbezpieczeństwa jest powszechnym problemem wśród pracowników w organizacjach na całym świecie. Często wynika on nie tylko z niedostatku fachowych kompetencji, ale również z braku świadomości, że zapewnienie bezpieczeństwa wymaga zaangażowania wszystkich pracowników.

Według danych NTT Security problem braku świadomości występowania zagrożeń jest często spotkany na całym świecie, a rekordowo wysoki poziom braku świadomości odnotowano we Francji (54 proc.) oraz Norwegii (53 proc.) (zob. rysunek 21). Roland Stephen podkreślił, że charakter tego zjawiska był szczególnie niepokojący w kontekście nieustannego udoskonalania narzędzi oraz metod używanych do przeprowadzania cyberataków, które wykorzystują braki w kompetencjach pracowników. Ten niewystarczający poziom umiejętności personelu może prowadzić w przyszłości do utraty zdolności obrony przed cyberprzestępcami. Dlatego też, zgodnie z postulatami uczestników, kluczowe jest wprowadzenie polityki promującej świadome poruszanie się w cyberprzestrzeni w celu zagwarantowania cyberbezpieczeństwa w organizacji, niezależnie od sektora i regionu świata.

Rysunek 21. Udział odpowiedzi „tak" na pytanie „Czy uważasz, że zapewnienie cyberbezpieczeństwa w organizacji jest wyłącznie odpowiedzialnością działu IT?"



Źródło: opracowanie własne na podstawie danych NTT Security[34]

Cyberataki kwantowe

Dyskusja przeprowadzona na seminariach objęła również nowe zagrożenia związane z działalnością przestępczą oraz szeroko rozumianym postępem technologicznym. Uczestnicy seminarium dla sektora finansowego poświęcili wiele uwagi potencjalnym zagrożeniom związanym z wykorzystaniem przez cyberprzestępców komputerów kwantowych. Roland Stephen przewiduje, że moc obliczeniowa komputerów kwantowych stanie się w rękach cyberprzestępców dużym zagrożeniem, ponieważ pozwala na łamanie obecnie istniejących algorytmów zabezpieczających. Powyższą tezę potwierdza również opinia prof. Michaela Biercuka[35], uznanego na świecie specjalisty z zakresu technologii i zabezpieczeń kwantowych, który prowadzi aktualnie badania

[34] B. Vanson, *Prevention Is Better Than Cure: Business Security – The Journey Continues*…, op. cit.

[35] J.P. Power, *Quantum Leap: What Will Quantum Computing Mean for Encryption?*, „Symatec Security Blog", 2017.

na Uniwersytecie w Sydney. W odpowiedzi na realne zagrożenie ze strony cyberataków kwantowych, uczestnicy zalecili zainicjowanie badań w obszarze kwantowego przetwarzania danych mających na celu stworzenie koncepcji oraz bazujących na nich implementacji algorytmów odpornych na ataki z użyciem komputerów kwantowych.

3.2. Polityka zgodności jako element tworzenia przyszłościowej wizji strategicznej

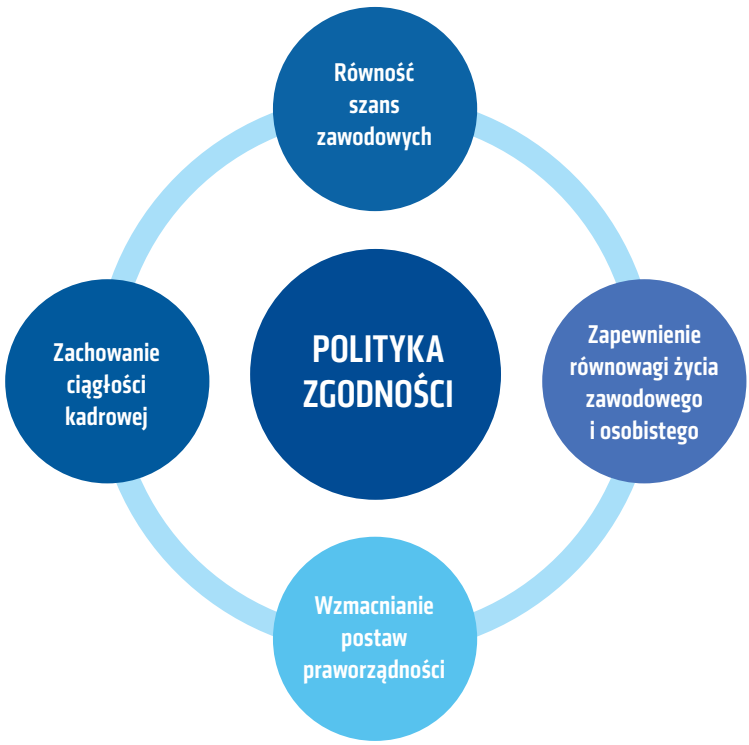
Niniejszy rozdział zawiera podsumowanie prac badawczych dotyczących zastosowania polityki zgodności jako elementu kreowania strategicznej wizji funkcjonowania firmy w warunkach zagrożenia, które przeprowadziła profesor Mireia Las Heras. Badania opierały się nie tylko na analizie przeprowadzonej przez zespół profesor Las Heras, ale również na wiedzy eksperckiej oraz opiniach zaproszonych uczestników. Prace dotyczyły przede wszystkim określenia dobrych praktyk w zakresie stosowania wybranych elementów polityki zgodności (zob. rysunek 22) do przeciwdziałania przestępstwom, nadużyciom i nieprawidłowościom.

3.2.1. Zalecenia dotyczące kształtu polityki publicznej, która ułatwia wdrażanie polityki zgodności w organizacjach

Dyskusje przeprowadzone podczas seminariów pozwoliły uczestnikom zidentyfikować czynniki sprzyjające wdrażaniu kultury zgodności w organizacjach. Jednym z najbardziej istotnych elementów kształtujących oraz asymilujących kodeks postępowania w organizacji jest sprzyjająca polityka publiczna ukierunkowana na zachowanie równowagi pomiędzy życiem rodzinnym a zawodowym. Według uczestników instrumenty polityki publicznej, zarówno normy prawne, jak i zalecenia, pomagają zapobiegać nadużyciom oraz ograniczają nierówności w kontekście zarządzania różnorodnością. Niniejszy rozdział zawiera omówienie elementów polityki zgodności, które według uczestników wymagają szczególnej uwagi. Podczas seminariów zaproponowano szereg zaleceń dotyczących implementacji poszczególnych elementów polityki zgodności

w skali kraju, a rozważania zostały osadzone w kontekście międzynarodowych trendów, obrazującym przykładowe wdrożenia rozważanych zaleceń.

Rysunek 22. Podstawowe elementy polityki zgodności



Źródło: opracowanie własne

Usługi pomocnicze stanowiące wsparcie dla rodzin

Regulacje promujące zachowanie równowagi między życiem rodzinnym a zawodowym stwarzają równe szanse dla rozwoju zawodowego obojga rodziców[36] i pozwalają każdemu pracownikowi dokonać indywidualnego wyboru najlepszego sposobu integracji życia zawodowego z rodzinnym. Uczestnicy seminariów uważają, że wysokim priorytetem należy objąć regulacje

[36] *Childcare Vouchers in the UK*, Accor Services 2008, https://www.edenred.com/sites/default/files/pdf/documentations/presentation-idayfocuschildcarevouchers-oct2008-en.pdf

rynku usług[37] przeznaczonych dla gospodarstw domowych lub powiązanych z życiem rodzinnym, np. dotyczących opieki nad osobami starszymi lub dziećmi, czy pomocy w obowiązkach domowych. Założenia proponowanej regulacji obejmowałyby legalizację tego typu usług, co sprzyjałoby uczciwej wymianie rynkowej i wspierałoby rodziny planujące skorzystać z takich usług poprzez zwiększenie ich dostępności i wiarygodności.

Wdrożenie polityki zgodności w organizacji nie powinno mieć na celu wyłącznie uniknięcia sankcji wynikających z niewypełnienia norm bezwzględnie obowiązujących. Celem powinno być także wypracowanie programów pomocowych promujących łączenie życia rodzinnego z pracą[38]. Według zaproszonej ekspertki asymilacja właściwych postaw prowadzi do redukcji znaczenia formalnych programów, które zyskują charakter zaleceń. Na poparcie tej tezy przytoczono przykład Francji, gdzie w 1990 roku rząd dał rodzinom z dziećmi możliwość odliczenia od podatku dochodowego nawet 50 proc. kosztów usług domowych opartych na umowach cywilnoprawnych lub uzyskania rekompensaty za te usługi w formie czeków[39].

Po przeprowadzeniu dyskusji uczestnicy zarekomendowali stosowanie czeków socjalnych w ramach polityki wspierania rodzin przez organy publiczne oraz prywatne. Profesor Mireia Las Heras potwierdziła, że stosowanie czeków zapomogowych jako formy świadczeń socjalnych jest uznanym na całym świecie rozwiązaniem i stanowi element wspólnej polityki prowadzonej przez wiele europejskich państw. Tego typu działania wpisują się w nurt polityki pomocy rodzinie, której głównym celem jest wspieranie obywateli w uzyskiwaniu równowagi pomiędzy życiem zawodowym a dbaniem o rodzinę. Jednym z przykładów polityki pomocy rodzinie są działania brytyjskiego rządu,

---

[37] *Formalizing Domestic Work Through the Use of Service Vouchers*, International Labour Organization, 2012, http://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@actrav/documents/publication/wcms_220717.pdf

[38] *Universal Service Employment Cheque*, Eurofond b.d., https://www.eurofound.europa.eu/es/data/tackling-undeclared-work-in-europe/database/universal-service-employment-cheque-france

[39] *Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law*, 2018, t. 2018/0106 (COD), https://eur-lex.europa.eu/resource.html?uri=cellar:a4e61a49-46d2-11e8-be1d-01aa75ed71a1.0001.02/DOC_1&format=PDF

który zwiększył zakres darmowej opieki nad dziećmi w wieku od 3 do 4 lat z 15 do 30 godzin, co ma na celu ułatwienie rodzicom powrotu do pracy[40].

Polityka wspierająca godzenie życia rodzinnego z zawodowym

Profesor Mireia Las Heras twierdzi, że promowanie prawidłowych postaw w zakresie ojcostwa i macierzyństwa stanowi podstawowy instrument polityki państwa w zakresie ochrony rodziny. Postawy te mają bezpośredni wpływ na zachowanie równowagi pomiędzy życiem osobistym, rodzinnym oraz społecznym jednostki. Kluczowym elementem polityki dotyczącej roli ojcostwa oraz macierzyństwa w życiu pracownika są następujące tematy:

- długość oraz znaczenie urlopu macierzyńskiego i ojcowskiego,
- ochrona stanowiska pracy,
- ramy elastyczności w zakresie wymienności urlopu dla ojca i matki.

Warto podkreślić, że w obowiązującym prawie międzynarodowym nie istnieje żadna regulacja nakładająca na pracodawcę obowiązek zapewnienia pracownikowi urlopu ojcowskiego, ale istnieją analogiczne regulacje dotyczące udzielania urlopu macierzyńskiego[41].

Regulacje wspierające godzenie życia rodzinnego i zawodowego mają na celu ochronę dobra kobiety i jej zdrowia. Urlop macierzyński ma za zadanie zapewnić matce wystarczającą ilość czasu do powrotu do zdrowia po ciąży i porodzie, chroniąc w ten sposób zdrowie zarówno dziecka, jak i jej samej. Uczestnicy seminariów uważają jednak, że promowanie równowagi między urlopem macierzyńskim i ojcowskim powinno przyczynić się do stymulowania i rozwoju poczucia współodpowiedzialności obojga rodziców za opiekę nad dzieckiem, co z kolei miałoby pozytywny wpływ na zdrowie i życie zawodowe zarówno kobiet, jak i mężczyzn.

Obecnie obowiązujące normy i prawa regulujące urlop macierzyński pozwalają na to, aby kobieta mogła dostosować swój dzień pracy do opieki nad dzieckiem, co stanowi element ochrony życia nowonarodzonych dzieci. Warto zwrócić uwagę na zmianę paradygmatu w zakresie regulacji w rozważanym obszarze. W przeszłości głównym założeniem było zapewnienie dobra dziecka

[40] *Help Paying for Childcare*, b.d., https://www.gov.uk/help-with-childcare-costs/free-childcare-and-education-for-2-to-4-year-olds (dostęp: 2.02.2019).

[41] *Council Directive 92/85 /EEC*, „Official Journal of the European Communities", 28.11.1992, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31992L0085&from=PL

poprzez utrzymanie ciągłości opieki, natomiast rola elastycznych godzin pracy matki była drugorzędna. Obecnie nacisk stawiany jest na uelastycznienie funkcjonowania pracownika w organizacji. Według zaproszonej ekspertki takie podejście pozwala pracownikom zachować równowagę między życiem zawodowym i osobistym, a także pozytywnie wpływa się na ich motywację i rozwój zawodowy. Jest też elementem promującym równe traktowanie pracowników i zmniejsza ryzyko dopuszczenia się przez pracownika nadużyć.

W najogólniejszym ujęciu urlop macierzyński oraz ojcowski to prawo do bycia nieobecnym w pracy przez określony czas, ale otrzymywania jednak za ten czas wynagrodzenia, oraz prawo do powrotu do tego samego miejsca pracy na takich samych warunkach. W Europie jedynie urlop macierzyński został uregulowany prawnie przez Dyrektywę Rady 92/85/EEC przyjętą 19 października 1992 roku. Jednak w niektórych krajach Europy występują bardziej zintegrowane rozwiązania, które zakładają, że rodzice dzielą wspólne obowiązki.

Jednym z przykładów zintegrowanej polityki pomocy rodzinom jest obecna polityka rządu Islandii[42], według której zarówno ojciec, jak i matka mają zapewnione trzy miesiące płatnego urlopu, którego nie mogą przekazać innym osobom. Dodatkowo, jeśli ojciec zdecyduje się na wykorzystanie przysługującego mu urlopu, rodzinie przysługują dodatkowe trzy miesiące urlopu, które może wykorzystać zarówno matka, jak i ojciec, w zależności od sytuacji rodzinnej. Zgodnie z dalszymi zapisami wspomnianej regulacji jedno z rodziców może także otrzymać dodatkowy bezpłatny trzymiesięczny urlop, który może zostać wykorzystany w całości lub podzielony na okresy, zależnie od potrzeb rodziców. Regulacja przewiduje też możliwość wykorzystania urlopu na poczet wizyt lekarskich, choroby dziecka lub każdej innej sytuacji, która wymaga rodzicielskiego poświęcenia. Prowadzenie takiej polityki ma na celu zwiększenie przyrostu naturalnego, promowanie postaw opartych na praworządności, a także wspieranie godzenia życia zawodowego z rodzinnym. Pełni również funkcję wyrównująca w zakresie praw przysługujących obu rodzicom i daje rodzinie niezbędny czas na dbanie o siebie i swój rozwój.

[42] *Maternity/Paternity Leave and Parental Leave*, Registers Island, b.d., https://www.island.is/en/family/having_a_baby/maternity_paternity_leave_and_parental_leave/

W niektórych krajach stosowana jest alternatywna opcja, umożliwiająca przeniesienie części urlopu macierzyńskiego na ojca. Tego typu podejście jest coraz częściej krytykowane, z uwagi na pomijanie znaczenia początkowego urlopu macierzyńskiego, którego głównym założeniem jest ochrona zdrowia fizycznego oraz psychicznego matki i dziecka. Jednak aktualne trendy dotyczące instrumentów światowej polityki publicznej zawierają element wspólny w postaci wsparcia w zakresie urlopu ojcowskiego i dążenia do ochrony oraz rozwoju relacji ojca i dziecka[43].

Uczestnicy seminariów podkreślali, że istotną częścią urlopu rodzicielskiego jest powszechny system edukacji dostępnej od wczesnego etapu rozwoju dziecka. Ważne, aby polityka płatnych urlopów macierzyńskich i ojcowskich była wspierana przez szeroko zakrojony system dotowanych przedszkoli i żłobków, które ułatwią rodzicom powrót do pracy. W szczególności istotne przy tym jest nie tylko zaangażowanie podmiotów publicznych, ale również organizacji prywatnych, które mogłyby zapewnić pracownikom wsparcie w zakresie dotowanej opieki oraz edukacji ich dzieci[44]. Równie istotne jest istnienie systemu publicznych oraz prywatnych domów seniora, a także dostępność pomocy socjalnej dla rodzin. Warto podkreślić, że polityka pomocy rodzinie nie może ograniczać się wyłącznie do urlopów rodzicielskich. Konieczne jest rozwijanie publicznego systemu świadczeń socjalnych dla całej rodziny, wraz z subsydiowanymi usługami oferowanymi wszystkim jej członkom[45].

Przy omawianiu korzyści płynących z polityki wspierającej opiekę nad dziećmi należy nawiązać do tzw. „międzynarodowego konsensusu"[46], według którego tego typu regulacje pozwalają na utrzymanie równowagi między

---

[43] S. Blum, A. Koslowski, P. Moss, *13th International Review of Leave Policies and Related Research 2017*, International Network on Leave Policies and Related Research, 06.2017, https://www.researchgate.net/profile/Peter_Moss2/publication/318324882_International_Review_of_Leave_Policies_and_Related_Research_2017/links/5964a2b2aca2720a5ccda9ce/International-Review-of-Leave-Policies-and-Related-Research-2017.pdf

[44] A. Thoursie, *El modelo de familia de dos sustentadores con un permiso parental prolongado: lecciones de suecia*, Instito de Studios Fiscales, b.d., http://www.ief.es/docs/investigacion/genero/LG_Thoursie.pdf

[45] Ibid.

[46] I.K. Naumann, *'Universal Childcare' and Maternal Employment: the British and the Swedish Story*, Social Policy Association 2015, http://www.social-policy.org.uk/wordpress/wp-content/uploads/2015/04/22_naumann.pdf

czasem pracy rodziców a opieką nad dzieckiem, zapewniając jednocześnie lepszy rozwój dziecka. Z przeprowadzonych badań wynika, że ustandaryzowana opieka nad dzieckiem lepiej przygotowuje dzieci do edukacji wczesnoszkolnej w pierwszym i kolejnych latach[47]. Warto podkreślić, że koniecznym elementem polityki wspierania rodziny jest zapewnienie dobrej opieki oraz skuteczne przedstawienie korzyści płynących z otrzymywanej pomocy, dla której nadrzędnym celem jest dobro dziecka. Szczególnie istotne w tym kontekście jest podkreślanie korzyści, które dziecko czerpie ze standardowej opieki dziennej otrzymywanej od najmłodszych lat życia. Badania dotyczące polityki godzinowego dostępu do darmowej opieki dziennej wykazują również, że tego typu działania znacznie ułatwiają kobietom powrót do pracy, co z kolei niweluje nierówności płciowe w zakresie możliwości rozwoju osobistego[48]. Na podstawie przeprowadzonej analizy uczestnicy uznali, że konieczne jest włączenie kompleksowej opieki rodzinnej do polityki realizowanej w organizacjach na poziomie krajowym i lokalnym w celu zagwarantowania równych szans zawodowych wszystkim pracownikom. W szerszym ujęciu pozwoli to na redukcję skłonności do popełniania nadużyć i przestępstw wśród pracowników.

Równość szans w rozwoju zawodowym kobiet i mężczyzn

Polityka publiczna, pomagająca zachować równowagę między życiem rodzinnym i zawodowym, gwarantuje równość szans w rozwoju zawodowym kobiet i mężczyzn. Celem takiej polityki jest stworzenie ogólnie dostępnych środków pozwalających na pogodzenie życia zawodowego z rodzinnym, tak aby środowisko pracy umożliwiało kobietom i mężczyznom równy dostęp do wszystkich możliwości rozwoju zawodowego, w tym awansu lub zmiany profilu działalności.

Nowatorskie badanie przeprowadzone przez zespół z IESE Business School pod kierownictwem profesor Las Heras dowodzi, że zaangażowanie pracowników obu płci w realizację misji firmy jest znacznie większe, gdy pracują w globalnym środowisku, zapewniającym im równe szanse rozwoju. Badanie

[47] T. Cornelissen i in., *Universal Childcare: The Potential to Level the Playing Field Between the Rich and Poor*, CEPR Policy Portal, 07.06.2018, https://voxeu.org/article/universal-child-care-family-background-and-school-readiness

[48] Ibid.

dotyczyło również stanu zdrowia pracowników. Z uzyskanych danych wynika, że osoby pracujące w otoczeniu sprzyjającym utrzymaniu równowagi między życiem zawodowym i osobistym mają więcej energii, a tego typu środowisko pracy redukuje prawdopodobieństwo wystąpienia u pracowników takich problemów jak załamania nerwowe. Przeprowadzone badanie wykazało również brak korelacji między niektórymi rozważanymi parametrami.

Przeprowadzona analiza wykazała, że równość szans w rozwoju zawodowym kobiet i mężczyzn ma wiele pozytywnych następstw, np. większe zaangażowanie pracowników w realizację misji firmy, większą satysfakcję z wykonywanej pracy, a także redukcję liczby konfliktów między pracą a życiem rodzinnym. Równość na polu rozwoju pomaga pracownikom osiągnąć większe spełnienie w różnych dziedzinach życia i zmniejsza szansę na wystąpienie u nich syndromu wypalenia zawodowego. Te ostatnie czynniki mają szczególne znaczenie w przypadku pracowników, którzy z uwagi na trudną sytuację osobistą borykają się z większą odpowiedzialnością za opiekę nad domem oraz zależnymi od nich osobami.

3.2.2. Przeciwskazania dotyczące instrumentów polityki zgodności w kontekście planowania scenariuszowego

Implementacja kultury zgodności w organizacji pozwala na poprawę i optymalizację działalności operacyjnej, a także zwiększa poziom bezpieczeństwa, zapewnia spójność funkcjonowania organizacji oraz zmniejsza prawdopodobieństwo popełnienia przestępstwa poprzez eliminację postaw sprzyjających angażowaniu się w działalność przestępczą. Jednak według uczestników niektóre instrumenty lub ich niewłaściwa implementacja mogą okazać się bezproduktywne, a nawet stwarzać przestrzeń do potencjalnych nadużyć. W związku z powyższym, w ramach dyskusji seminaryjnych z udziałem profesor Las Heras, uczestnicy określili krytyczne obszary wdrażania oraz utrzymywania kultury zgodności w organizacjach.

Według uczestników niektóre z wykorzystywanych dotychczas dozwolonych przez prawo środków służących zapewnieniu przestrzegania norm i zasad organizacji wywołują nieufność, zmniejszają zaangażowanie pracownika i tworzą wrażenie bycia w nadmiernym stopniu kontrolowanym przez

organizację, co zwiększa skłonność do popełniania nadużyć. W związku z powyższym należy zachować szczególną ostrożność przy tworzeniu koncepcji audytu wewnętrznego, tak aby nie wiązał się on z naruszaniem podstawowych praw pracowniczych, takich jak prawo do prywatności i poufności komunikacji. Protokoły operacyjne, nawet jeśli są zgodne z obowiązującymi normami, nie powinny obejmować aktów przemocy, zarówno fizycznej, jak i psychicznej, być niekomfortowe, lub sugerować, że organizacja nie ufa własnym pracownikom[49]. Na tej podstawie można stwierdzić, że dbałość o zaufanie, oddanie i zaangażowanie pracowników jest wyznacznikiem rzetelności oraz rygoru w zarządzaniu kulturą zgodności.

Analogiczne problemy pojawiają się w odniesieniu do instrumentów polityki publicznej dedykowanych wspieraniu rodzin i integracji życia zawodowego, osobistego i rodzinnego, które także mogą okazać się bezproduktywne dla pracowników. Niektóre z form wsparcia socjalnego, które nie zostały dobrze skonstruowane i które nie są połączone z niezbędnymi usługami uzupełniającymi, dotacjami lub pomocą, przynoszą negatywny efekt dla beneficjentów. Przykładowo w polityce dotyczącej urlopów macierzyńskich należy uwzględnić rolę państwowych oraz dotowanych instytucji oferujących dzienną opiekę nad dzieckiem. W przypadku braku odpowiedniej liczby tego typu instytucji, kobiety mogą mieć trudności z powrotem do życia zawodowego z powodu braku adekwatnej pomocy. Może to także spowolnić rozwój samego dziecka oraz proces powrotu matki do zdrowia[50].

Uczestnicy zauważyli również, że negatywne skutki uboczne pojawiają się też w kontekście regulacji związanych z ochroną praw kobiet oraz zapewnieniem warunków niezbędnych dla zachowania przez matki równowagi między życiem zawodowym i rodzinnym. Szczególnie negatywne efekty może przynieść polityka pozytywnej dyskryminacji, która często zniechęca organizacje do zatrudniania większej liczby kobiet[51].

---

[49] F. Javier Lluch Corell, *Derecho a la intimidad del trabajador versus control empresarial: una jurisprudencia inestable*, elderecho.com, 01.12.2004, https://elderecho.com/derecho-a-la-intimidad-del-trabajador-versus-control-empresarial-una-jurisprudencia-inestable

[50] International Labour Organization, United Nations Development Programme, *Work and Family: Towards New Forms of Reconciliation with Social Co-responsibility*, ILO/UNDP, Santiago 2009, http://www.undp.org/publications/pdf/undp_ilo.pdf

[51] C. Cifuentes Hurtado, *Derecho a Sala Cuna: Situación Actual y Propuesta de Política*, libertad desarrollo 2012, http://www.sociedadpoliticaspublicas.cl/archivos/CBLOQUET/

Według uczestników niektóre organizacje starają się unikać osiągania limitów wynikających z obowiązujących regulacji, z uwagi na to, że powodowałoby to zwiększoną złożoność zarządzania strategicznego ze względu na konieczność zastosowania obligatoryjnych środków i modyfikacji związanych z pozytywną dyskryminacją. Zagwarantowanie kobietom i mężczyznom równości w aspektach zawodowych robi się przez to kwestią problematyczną, przyczyniając się do zwiększania poczucia dyskryminacji wśród pracowników. Warto zauważyć, że analogiczne problemy występują również w przypadku wprowadzania w organizacji parytetów. W takiej sytuacji rzeczywiste umiejętności i kompetencje potencjalnego pracownika stanowią drugorzędną kategorię w stosunku do jego płci, wieku, pochodzenia, rasy lub innej cechy, decydującej o zastosowaniu pozytywnej dyskryminacji służącej spełnieniu wymogów narzucanych przez system parytetów[52].

Zagrożenia związane z systemem parytetów – problematyka pozytywnej dyskryminacji

Zagwarantowanie równouprawnienia wszystkich pracowników, bez względu na ich wiek, pochodzenie etniczne, płeć, czy jakąkolwiek inną cechę, jest jednym z głównych obowiązków organizacji kierującej się zasadami polityki zgodności i aspirującej do miana odpowiedzialnej społecznie instytucji.

Jedną z głównych zasad zapewniających równouprawnienie kobiet i mężczyzn w sferze zawodowej, przy jednoczesnym zachowaniu różnorodności płciowej, jest zadbanie o to, aby określony odsetek decyzyjnych lub politycznie strategicznych stanowisk był w organizacji obsadzony przez kobiety. Zakładając, że stanem wyjściowym jest brak równowagi płciowej na tych stanowiskach, tego typu działalność ma na celu ułatwienie kobietom uzyskania dostępu do stanowisk decyzyjnych. Zazwyczaj regulacje mające na celu ułatwienie dostępu do określonych stanowisk poprzez dyskryminację pozytywną są ustanawiane przez państwa na poziomie konstytucyjnym, ustawodawczym lub za pośrednictwem indywidualnych zaleceń. Nie istnieje żadna zatwierdzona europejska norma, która obligowałaby kraje członkowskie do ustanowienia praw promujących równouprawnienie w tym zakresie.

Panel_Trabajo_y_Maternidad/Derecho%20a%20Sala%20Cuna%20Una%20propuesta%20de%20politica.pdf

[52] *Affirmative Action* | *Overview*, National Conference of State Legislature, 02.07.2014, http://www.ncsl.org/research/education/affirmative-action-overview.aspx

Niemniej jednak dyskusje dotyczące tego tematu są bardzo intensywne. Wiele państw broni swojej suwerenności w kwestiach związanych z zarządzaniem różnorodnością w organizacjach, odwołując się do charakterystycznych cech kultury swoich krajów[53].

Przykładem takiego kraju może być Szwecja, gdzie każda organizacja przyjmuje właściwe dla siebie działania, środki lub regulacje wewnętrzne, odnosząc się do równości na różnych stanowiskach zawodowych. Natomiast w Norwegii[54] w 2003 roku wprowadzono regulację ustanawiającą obowiązek zagwarantowania zrównoważonej reprezentacji kobiet i mężczyzn na stanowiskach zarządczych. W obu krajach wzrosła liczba kobiet zajmujących najwyższe stanowiskach w organizacjach. W Szwecji, w 2017 roku, reprezentacja kobiet na stanowiskach zarządczych plasowała się na poziomie 32 proc., podczas gdy w Norwegii już w 2010[55] roku osiągnięto poziom 44 procent. Mimo, że wprowadzenie parytetu dało pozytywny rezultat w krótkim czasie, należy także wziąć pod uwagę konsekwencje długoterminowe. Gdy liczba kobiet, przedstawicieli mniejszości, czy osób w określonym wieku, zajmujących wysokie stanowiska jest narzucona za pomocą ustawy, powstaje wrażenie, że różnorodność została wymuszona. Oznacza to odejście od koncepcji naturalnej integracji oraz promowania różnorodności poprzez podkreślanie jej zalet i tworzonej przez nią wartości dodanej, co może skutkować powstaniem nowych nierówności i łamać zasady merytokracji panujące w organizacji.

Kolejnym wartym rozważenia przykładem jest Hiszpania, gdzie Ustawa nr 32/2014 z dnia 3 grudnia wprowadziła zmiany obowiązujących przepisów w celu zagwarantowania większej przejrzystości w zarządzaniu przedsiębiorstwem. Jedno z postanowień nowej ustawy dotyczyło konieczności zapewnienia równej reprezentacji płci na stanowiskach, a także składania

---

[53] R. Kallqwist, R. Aremann, *Gender Diversity on Swedish Companies' Board of Directors: A Study on Gender Diversity in 60 Swedish Listed Small, Medium and Large Cap Companies Between 2009–2015*, Jönköping International Business School, b.d., http://hj.diva-portal.org/smash/record.jsf?pid=diva2%3A1109219&dswid=-513

[54] A. Storvik, M. Teigen, *Women on Board the Norwegian Experience*, Friedrich Ebert Stiftung, International Policy Analysis, Berlin 06.2010, https://library.fes.de/pdf-files/id/ipa/07309.pdf

[55] *Ten Years on from Norway's Quota for Women on Corporate Boards*, „The Economist", 17.02.2018, https://www.economist.com/business/2018/02/17/ten-years-on-from-norways-quota-for-women-on-corporate-boards

odpowiedniej sprawozdawczości dotyczącej zastosowanych przez organizację środków, mających zagwarantować osiągnięcie minimalnej wymaganej ustawowo liczby kobiet na stanowiskach kierowniczych. Regulacja zaleca także, aby firmy brały pod uwagę zarządzanie różnorodnością, a także zapewniały wgląd w sposób wdrażania tego procesu oraz stosowne wyjaśnienia dotyczące osiągania zakładanych minimów kadrowych, w tym w odniesieniu do specjalistów potrzebnych na wypełnienie strategicznych pozycji w organizacji. Za obowiązek przedstawienia w rocznych sprawozdaniach organizacji wyjaśnień dotyczących środków podjętych w procesie nominowania kandydatów i kandydatek na poszczególne stanowiska odpowiada specjalny komitet ds. nominacji[56].

Parytety, których celem jest zapewnienie różnorodnej reprezentacji, również mogą mieć skutek demotywujący, tj. ich beneficjenci mogą uważać się za dłużników systemu zgodności i nie czuć, że uzyskaną pozycję zawdzięczają własnym umiejętnościom. Powyższe zjawisko będzie się wiązało na dłuższą metę ze zmniejszeniem produktywności, a także prowadziło do zwiększania nierówności i postaw sprzyjających popełnianiu przestępstw i naruszeń. Tego typu polityka może w szczególności skutkować umniejszeniem rzeczywistych kompetencji grup, które ma wspierać, czyli grup zróżnicowanych z uwagi na płeć, rasę, pochodzenie etniczne, czy wiek, co może doprowadzić do obniżenia poziomu uczciwości wewnątrz organizacji, a także sprzyjać pogłębianiu istniejących nierówności.

Według uczestników seminariów kluczem do sukcesu systemu parytetów jest prawidłowy proces nominacji na stanowiska oparty na zgodności wyboru ze strategią biznesową firmy, a także określeniu wartości dodanej wnoszonej przez danego kandydata. Udane wprowadzenie do organizacji kultury zgodności wymaga umiejętność zidentyfikowania prawdziwego „bogactwa" firmy, a także określenia i wzmocnienia tych wartości, które przyświecają zarówno organizacji, jak i pracownikom, i które można wykorzystać, aby uplasować organizację na strategicznie uprzywilejowanej pozycji. Natomiast błędem jest formułowanie strategii kadrowej jedynie w celu spełnienia wymogów

[56] *Good Governance Code of Listed Companies*, Comision nacional del mercado de valores, 02.2015, https://www.cnmv.es/docportal/publicaciones/codigogov/good_governanceen.pdf

przepisów dotyczących parytetów[57]. Jako precedensową decyzję w zakresie rozstrzygnięcia kwestii parytetów można przytoczyć rezygnację przez szwedzki rząd z planu zwiększenia wymaganego udziału kobiet na stanowiskach członków rad nadzorczych spółek notowanych na giełdzie do 40 proc. w roku 2019, co było spowodowane zmianą podejścia do polityki parytetowej[58].

Środki kontroli wewnętrznej zagrażające zaangażowaniu i oddaniu pracowników

Realizacja założeń wynikających z polityki zgodności wymaga przedsięwzięcia pewnych środków służących do kontroli oraz monitorowania tego, na ile personel stosuje się do jej postanowień. W wielu organizacjach pojawia się problem z określeniem zakresu stosowania narzędzi kontrolnych w kontekście potencjalnego naruszania prywatności pracowników.

Możliwości kontroli nie mogą przekraczać granic poszanowania godności osobistej pracowników i ich podstawowych praw takich jak ochrona intymności oraz poufności komunikacji[59]. Prawa te są zabezpieczone przez szereg regulacji, które obowiązują zarówno pracodawcę, jak i pracowników, i określają wytyczne dotyczące granic kontrolowania pracowników. W związku z powyższym, aby środki kontroli działalności biznesowej były uzasadnione, należy spełnić wymogi dotyczące ich proporcjonalności, stosowności i wystarczalności[60]. Europejski Trybunał Praw Człowieka sformułował analogiczne orzeczenie, stwierdzając, że trybunały krajowe powinny zagwarantować, żeby wdrażaniu środków kontroli korespondencji oraz innej komunikacji pracowników towarzyszyły zawsze odpowiednie i wystarczające gwarancje zapobiegające naruszania podstawowych praw pracowników.

---

[57] Ibid.

[58] D. Milliken, *Swedish Government Drops Plans for Gender Quota Bill for Company Boards*, „Reuters", 12.01.2017, https://www.reuters.com/article/us-sweden-board-equality/swedish-government-drops-plans-for-gender-quota-bill-for-company-boards-idUSKBN14W2AM

[59] *Best Practice Guide Workplace Privacy*, Australian Government Fair Work Ombudsman, 2014, https://www.fairwork.gov.au/ArticleDocuments/711/Workplace-privacy-best-practice-guide.pdf.aspx

[60] *Employee Rights 101: What Every Business Owner Needs to Know*, Square, Inc., b.d., https://squareup.com/townsquare/employee-rights-101-what-every-business-owner-needs-to-know

Wdrażając powyższe rekomendacje w organizacji, należy opracować adekwatne zasady eksploatacji narzędzi informatycznych wykorzystywanych w ramach kontroli wewnętrznych. Wcześniejsze zdefiniowanie protokołów określających okoliczności i warunki, na podstawie których pracodawca może uzyskać dostęp do informacji i sprzętu informacyjno-komunikacyjnego, np. gdy przeprowadzony zostanie atak na system bezpieczeństwa, pozwala zachować zaufanie w ramach organizacji oraz wdrożyć jasną i przejrzystą politykę zgodności. Transparentne procedury informują pracowników o możliwości nadzorowania jego komunikacji przez osoby zarządzające. Taki nadzór stanowi więc jedynie zgodny z prawem sposób przestrzegania protokołów zgodności, a informacje, do których organizacja ma dostęp, mogą stanowić dowody, w przypadku wystąpienia nadużycia bądź naruszenia, do którego dopuści się pracownik.

Zagrożenia związane z nieprawidłowym wdrażaniem polityki dotyczącej urlopów rodzicielskich

Polityka opracowana w celu promowania i ochrony urlopu macierzyńskiego wpływa często negatywnie na wynagrodzenie kobiet i stabilność ich zatrudnienia. Jest to tzw. „efekt urlopu macierzyńskiego”[61]. Kobiety są uważane za aktywa, które ze względu na urlop macierzyński, wykorzystywanie urlopu na opiekę nad dziećmi lub pracę w niepełnym wymiarze godzin, nie wykazują ciągłości eksploatacyjnej, co często odzwierciedla się negatywnie w wysokości ich wynagrodzenia.

W ramach debat nad rozwojem polityki dotyczącej urlopów macierzyńskich pojawiają się dyskusje na temat odnoszonych przez kobiety porażek zawodowych, u których źródła leżą niewystarczające lub źle skonstruowane środki pomocowe. Nawet jeśli polityka posiada poprawnie zdefiniowane cele, tj. jej celem będzie ochrona zdrowia matki i jej więzi z dzieckiem, a także poprawienie wskaźnika urodzeń, pozostaje źle skonstruowaną regulacją, jeśli nie obejmuje dodatkowo przepisów gwarantujących młodym matkom równe szanse na rynku pracy. Według uczestników prawidłowo skonstruowana

[61] *Labour Market Effects of Parental Leave Policies in OECD Countries*, OECD Social, Employment and Migration Working Papers, 10.01.2013, https://www.oecd-ilibrary.org/social-issues-migration-health/labour-market-effects-of-parental-leave-policies-in-oecd-countries_5k8xb6hw1wjf-en

polityka powinna obejmować środki ułatwiające kobietom powrót do pracy, a także oferować publiczny system opieki nad dzieckiem lub pomoc w zakresie pokrycia kosztów usług w tym zakresie. Kolejnym elementem niepoprawnie skonstruowanej polityki dotyczącej urlopów macierzyńskich jest też ich zbytnia długość, która stanowi główną przyczynę rosnącej nierówności płac między płciami, ponieważ powoduje spadek wysokości zarobków kobiet w ujęciu bezwzględnym, klasyfikując zawodowe możliwości matek w zakresie niższej jakości[62].

Profesor Las Heras oraz uczestnicy seminariów ustalili wspólnie, że fakt istnienia dużych różnic między politykami dotyczącymi urlopów rodzicielskich nawet w krajach wysokorozwiniętych sugeruje, że nie istnieje jednoznaczny konsensus dotyczący prawidłowego zarządzania polityką rodzinną, szczególnie w odniesieniu do samych narodzin dziecka oraz okresu wczesnego dzieciństwa. Opierając się na przeprowadzonej analizie, uczestnicy stwierdzili również, że źle skonstruowane zasady mogą w ujęciu długoterminowym wyostrzać różnice między płciami, zarówno w gospodarstwach domowych, jak i na rynku pracy, co może przekładać się na dalsze pogłębianie nierówności i stwarzać przestrzeń do potencjalnych nadużyć.

Zachęcanie do pracy – równowaga między życiem zawodowym a prywatnym

Według profesor Las Heras badania wskazują, że wprowadzenie elastycznego czasu pracy, które miało na celu ułatwienie godzenia życia zawodowego i rodzinnego, doprowadziło do spadku liczby zatrudnianych kobiet. U źródeł tego fenomenu leżą obawy zatrudniających kobiety organizacji, dla których elastyczny grafik pracy matek oznacza zaburzenia w zarządzaniu zasobami ludzkimi lub potencjalne konflikty wśród współpracowników wynikające z nierównego traktowania. W rzeczywistości niektóre zasady mające motywować do lepszego łączenia życia osobistego i zawodowego, np. skrócenie godzin pracy w celu umożliwienia pracownicy opieki nad dzieckiem[63], stanowią

[62] D. Richardson, *Key Findings on Families, Family Policy and the Sustainable Development Goals*, United Nations Children's Fund (UNICEF), Florencja 05.2018, https://www.unicef-irc.org/publications/pdf/Families_and_SDGs_Synthesis_Report.pdf

[63] I. Naumann i in., *Early Childhood Education and Care Provision: International Review of Policy Delivery and Funding: Final Report*, 2013, http://www.nls.uk/scotgov/2013/9781782564164.pdf

dla organizacji strategiczny problem, ponieważ wprowadzają komplikacje związane z tworzeniem zróżnicowanych harmonogramów pracy bez jakiejkolwiek kompensacji w postaci ulg podatkowych czy innych środków pomocy socjalnej, która jest niezbędna, żeby móc zatrudnić dodatkowy personel w celu realizacji strategicznych potrzeb firmy[64].

Świadczenia oferowane w ramach instrumentów polityki publicznej promujących godzenie życia zawodowego z rodzinnym w większości przypadków okazują się niewystarczające lub zbyt złożone[65]. Szczególnie takie świadczenia jak bony przedszkolne lub dofinansowanie opieki nad dziećmi powinny być zrównoważone poprzez ocenę wszystkich zmiennych, takich jak kwestia czasu, kosztu dodatkowych godzin, jeśli są obowiązkowe, a także analiza jakości i ilości usług oferowanych najbliższej rodzinie w celu wsparcia życia rodzinnego. Gdy tego typu pomoc jest niewystarczająca, rodziny muszą zatrudnić dodatkową pomoc domową, co może okazać się obciążeniem dla budżetu domowego. Należy zadbać o to, aby charakter usług opieki nad osobami starszymi, zasady dostępności domów opieki, lub cechy innych usług specjalistycznych, były dostosowane do faktycznych potrzeb rodzin, co sprawi, że ich funkcjonowanie będzie przebiegało w harmonii[66].

3.3. Podstawowe zasady inicjatywy Global Compact ONZ w kontekście kultywowania odpowiedzialnych praktyk dotyczących zarządzania organizacją

Platforma *Global Compact* Organizacji Narodów Zjednoczonych jest inicjatywą wspierającą wspólne działania wszystkich interesariuszy na rzecz zrównoważonego rozwoju. Na jej gruncie wytworzyła się globalna sieć lokalnych inicjatyw dążących do przyjęcia trwałych i odpowiedzialnych zasad ładu korporacyjnego oraz monitorowania postępów w ich wdrażaniu. Organizacje

[64] OECD, OCDE, *Society at a Glance 2016: OECD Social Indicators*, OECD Publishing; Éditions OCDE, 2016.

[65] *Universal Service Employment Cheque*…, op. cit.

[66] B. Mcpartland, *Are You Missing out on the Billions of Unclaimed Family Benefits in France?*, „The Local", 10.07.2018, https://www.thelocal.fr/20180710/are-you-missing-out-on-the-billions-of-benefits-that-go-unclaimed-in-france

zrzeszone wokół tej inicjatywy kierują się zbiorem dziesięciu podstawowych zasad, służących realizacji powyższych celów.

Uczestnicy seminariów doszli do wniosku, że przedstawiony poniżej zbiór zasad powinien zostać ujęty w kodeksach postępowania wszystkich organizacji.

A. PRAWA CZŁOWIEKA

1. Organizacje powinny: przestrzegać i wspierać ochronę uznanych na arenie międzynarodowej praw człowieka, a także
2. eliminować wszelkie przypadki łamania praw człowieka przez firmę.

B. STANDARDY PRACY

3. Organizacje powinny: popierać wolność zrzeszania się i w praktyce uznawać prawo do prowadzenia zbiorowych negocjacji
4. wspierać eliminację wszelkich form niewolnictwa i pracy przymusowej
5. przyczyniać się do faktycznego zniesienia pracy dzieci oraz
6. przeciwdziałać dyskryminacji w sferze zatrudnienia.

C. OCHRONA ŚRODOWISKA

7. Organizacje powinny: wspierać zapobiegawcze podejście do problemów środowiska naturalnego
8. podejmować inicjatywy propagujące większą odpowiedzialność środowiskową oraz
9. wspierać rozwój i upowszechnianie technologii przyjaznych środowisku.

D. PRZECIWDZIAŁANIE KORUPCJI

10. Organizacje powinny przeciwdziałać korupcji we wszystkich jej formach, w tym łapówkarstwu i wymuszeniom.

Uwagi końcowe – podsumowanie cyklu

Między wrześniem a grudniem 2018 roku zorganizowano w Warszawie cykl spotkań w ramach projektu badawczego Instytutu Wymiaru Sprawiedliwości zatytułowanego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości". Nadrzędnym celem projektu było podjęcie szeroko zakrojonych rozważań na temat przyczyn występowania przestępczości w Polsce oraz metod ograniczania czynników ryzyka jej występowania. Uczestnikami projektu byli wysokiej rangi przedstawiciele organów administracji rządowej oraz podległych im instytucji, a także członkowie zarządów i reprezentanci spółek Skarbu Państwa działających w strategicznych sektorach polskiej gospodarki, takich jak energetyka, bankowość, czy ubezpieczenia. Wśród uczestników znaleźli się w szczególności praktycy aktywni w sferze zarządzania ludźmi w organizacji.

Dokumentacja wyników badań została sporządzona w formie cyklu czterech raportów podsumowujących dokonania uczestników projektu w ramach każdego z comiesięcznych spotkań. Cykl ten należy traktować jako niepodzielną całość z uwagi na fakt, że prace wykonane w kolejnych etapach bazują silnie na osiągnięciach wypracowanych w etapach wcześniejszych, a całość prac wpisuje się w ramy metodologii *Six Step Process* wprowadzonej w pierwszej części cyklu („Raport z przeprowadzenia badań wraz z organizacją seminariów w zakresie zapobiegania przestępczości: identyfikacja przyczyn przestępczości w wybranych obszarach gospodarki w Polsce i na świecie").

Przeprowadzone prace badawcze przyczyniły się do pełniejszego zrozumienia przez uczestników seminariów zagadnień dotyczących zarządzania strategicznego. Nie można też pominąć tego, że udział w projekcie „Prawo,

gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" stanowi dla uczestników źródło twórczej inspiracji do wprowadzania koniecznych zmian zarówno w organizacjach, które obecnie reprezentują, jak i tych, które będą reprezentowali w przyszłości. To proaktywne nastawienie ma szczególne znaczenie w warunkach ciągłych wyzwań związanych z nieustanną obecnością zjawisk przestępczych zagrażających stabilnemu funkcjonowaniu publicznych i prywatnych organizacji, a co za tym idzie, także całemu społeczeństwu, rozumianemu jako zbiorowość determinowana przez wspólnotę wartości i celów.

Podziękowania

Badania podsumowane w niniejszym raporcie, a także cały 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. Powstanie tego raportu nie byłoby możliwe bez ich wnikliwych uwag i spostrzeżeń.

Załącznik A. Dodatkowe informacje dotyczące prelegentów

Paul Healy, Ph.D.

PROWADZONE PANELE	• Fighting corruption at Siemens
AKTUALNIE PEŁNIONE FUNKCJE	• Profesor w Harvard Business School (James R. Williston Professor) • Prodziekan ds. rozwoju kadry w Harvard Business School
NAJWAŻNIEJSZE PUBLIKACJE[67]	1. Healy P.M, Wahlen J.M., *A Review of the Earnings Management Literature and Its Implications for Standard Setting*, „Accounting Horizons", 1999, t. 13, nr 4. 2. Healy P.M, Palepu K.G., Ruback R. S., *Does Corporate Performance Improve after Mergers?*, „Journal of Financial Economics", 1992, t. 31, nr 2. 3. Healy P.M, Palepu K.G., *Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature*, „Journal of Accounting and Economics", 2001, t. 31, nr 1–3. 4. Healy P.M., Hutton A.P., Palepu K.G., *Stock Performance and Intermediation Changes Surrounding Sustained Increases in Disclosure*, „Contemporary Accounting Research", 1999, t. 16, nr 3. 5. Healy P.M., *The Effect of Bonus Schemes on Accounting Decisions*, „Journal of Accounting and Economics", 1985, t. 7, nr 1–3.

[67] Pięć najczęściej cytowanych prac spośród całego dorobku naukowego. Selekcja na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 21.12.2018).

Mireia Las Heras, Ph.D.

PROWADZONE PANELE	• Going beyond compliance: putting people first • Going beyond compliance: caring for employees and their families • Going beyond compliance: leadership and development of trust • Going beyond compliance: when times change
AKTUALNIE PEŁNIONE FUNKCJE	• Dyrektor naukowy w międzynarodowym centrum International Center for Work and Family (ICWF) • Profesor w IESE Business School • Konsultantka w NCH & Partners
NAJWAŻNIEJSZE PUBLIKACJE[68]	1. Hall D.T., Heras M.L., *Reintegrating Job Design and Career Theory: Creating not Just Good Jobs but Smart Jobs*, „Journal of Organizational Behavior", 2010, nr 31. 2. Chudzikowski K., Demel B., Mayrhofer W., Briscoe J.P., Unite J., Bogićević Milikić B., Hall D.T., Heras M.L., Shen Y., Zikic J., *Career Transitions and Their Causes: A Country-comparative Perspective*, „Journal of Occupational and Organizational Psychology", 2009, nr 82. 3. Hall D.T., Lee M.D., Kossek E.E., Heras M.L., *Pursuing Career Success while Sustaining Personal and Family Well-Being: A Study of Reduced-Load. Professionals over Time*, „Journal of Social Issues", 2012, nr 68. 4. Hall D.T., Heras M.L., *Long Live the Organisational Career,* w: Collin A, Patton W. (red.) *Vocational Psychological and Organisational Perspectives on Career: Towards a Multidisciplinary Dialogue*, 2009. 5. Rofcanin Y., Heras M.L., Bakker A.B., *Family Supportive Supervisor Behaviors and Organizational Culture: Effects on Work Engagement and Performance*, „Journal of Occupational Health Psychology", 2017, nr 22.

Michael Rosenberg, Ph.D.

PROWADZONE PANELE	• Scenario planning: imagining the future
AKTUALNIE PEŁNIONE FUNKCJE	• Profesor w katedrze Zarządzania Strategicznego IESE Business School • Dyrektor naukowy programów Advanced Management Program w IESE Business School • Dyrektor naukowy projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości"
NAJWAŻNIEJSZE PUBLIKACJE	1. Rosenberg M., *Strategy and Geopolitics: Understanding Global Complexity in a Turbulent World*, Emerald Group Publishing Limited, 2017. 2. Rosenberg M., Seager P. (red.), *Managing Media Businesses: A Game Plan to Navigate Disruption and Uncertainty*, Palgrave Macmillan, Switzerland 2017. 3. Rosenberg M., *Strategy and Sustainability: A Hard-Nosed and Clear-Eyed Approach to Environmental Sustainability for Business*, Palgrave Macmillan, 2015.

[68] Dla każdego prelegenta przedstawiono pięć najczęściej cytowanych prac spośród całego dorobku naukowego. Selekcja na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 28.09.2018).

Roland Stephen, Ph.D.

PROWADZONE PANELE	• Understanding technology, productivity, and progress: the next ten years
AKTUALNIE PEŁNIONE FUNKCJE	• Dyrektor Center for Innovation Strategy and Policy w SRI International
UDZIAŁ W PROJEKTACH	1. Researching the Teacher Wallets Program – program badawczy analizujący to, w jaki sposób nauczyciele nauczania podstawowego w Stanach Zjednoczonych (K-12) wybierają i oceniają materiały cyfrowe oraz wdrażają je do programów nauczania. 2. States' Methods of Funding Higher Education – badanie porównujące różne sposoby finansowania edukacji wyższej w poszczególnych stanach USA w kontekście metod stosowanych w stanie Nevada.

Antonino Vaccaro, Ph.D.

PROWADZONE PANELE	• Jeffrey Skilling, Bernie Madoff the monster & the other smartest guys of the Room
AKTUALNIE PEŁNIONE FUNKCJE	• Adiunkt na Wydziale Etyki Biznesu oraz w Zespole Negocjacyjnym IESE Business School • Dyrektor akademicki Center for Business in Society (CBS) oraz platform Social Innovation i Social Entrepreneurship IESE Business School
NAJWAŻNIEJSZE PUBLIKACJE[69]	1. Vaccaro A., Veloso F., Brusoni S., *The Impact of Virtual Technologies on Knowledge-based Processes: An Empirical Study*, „Research Policy", 2009, t. 38, nr 8. 2. Vaccaro A., Parente R., Veloso F.M., *Knowledge Management Tools, Inter-organizational Relationships, Innovation and Firm Performance*, „Technological Forecasting and Social Change", 2010, t. 77, nr 7. 3. Vaccaro A., Palazzo G., *Values against Violence: Institutional Change in Societies Dominated by Organized Crime*, „Academy of Management Journal", 2015, t. 58, nr 4. 4. Vaccaro A, Madsen P., *Corporate Dynamic Transparency: The New ICT-driven Ethics?*, „Ethics and Information Technology", 2009, t. 11, nr 2. 5. Vaccaro A., Echeverri D.P., *Corporate Transparency and Green Management*, „Journal of Business Ethics", 2010, t. 95, nr 3.

[69] Dla każdego prelegenta przedstawiono pięć najczęściej cytowanych prac spośród całego dorobku naukowego. Selekcja na podstawie systemu Google Scholar®, https://scholar.google.pl/ (dostęp: 28.09.2018).

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

Heading into the future

1. Czy uważa Pan/Pani, że skutki działalności przestępczej, w tym wyłudzeń, oszustw oraz kradzieży, mogą w przyszłości poważnie zagrozić funkcjonowaniu organizacji, którą Pan/Pani reprezentuje?	1	2	3	4	5
2. Czy uważa Pan/Pani, że organizacja, którą Pan/Pani reprezentuje, jest podatna na wpływ działalności przestępczej, w tym wyłudzenia, oszustwa oraz kradzieże?	1	2	3	4	5

3. Czy uważa Pan/Pani, że organizacja, którą Pan/Pani reprezentuje, jest podatna na cyberataki?	1	2	3	4	5
4. Czy uważa Pan/Pani, że skutki cyberataku mogą poważnie zagrozić funkcjonowaniu organizacji, którą Pan/Pani reprezentuje?	1	2	3	4	5
5. Czy organizacja, którą Pan/Pani reprezentuje, była w przeszłości celem cyberataku?	1	2	3	4	5
6. Czy organizacja, którą Pan/Pani reprezentuje planuje zwiększyć środki w zakresie zwalczania przestępczości?	1	2	3	4	5
7. Czy uważa Pan/Pani, że za 10 lat pojawią się nowe rodzaje przestępstw, na które będzie narażona organizacja, którą Pan/Pani reprezentuje?	1	2	3	4	5
8. Obszary wymagające szczególnej uwagi w kontekście zagrożeń przyszłości:					
a. promowanie postaw etycznych	1	2	3	4	5
b. bezpieczeństwo krytycznej infrastruktury	1	2	3	4	5
c. regulacje prawne	1	2	3	4	5
d. modernizacja zaplecza technicznego organów ścigania	1	2	3	4	5
e. niski poziom zamożności społeczeństwa	1	2	3	4	5
f. aspekty etyczne sztucznej inteligencji	1	2	3	4	5
g. inny:	1	2	3	4	5
9. Sektory najbardziej podatne na działalność przestępczą w przyszłości to:					
a. sektor finansowy	1	2	3	4	5
b. sektor ubezpieczeń	1	2	3	4	5
c. sektor energetyki	1	2	3	4	5
d. handel detaliczny	1	2	3	4	5
e. handel hurtowy					
f. transport	1	2	3	4	5
g. inny:	1	2	3	4	5

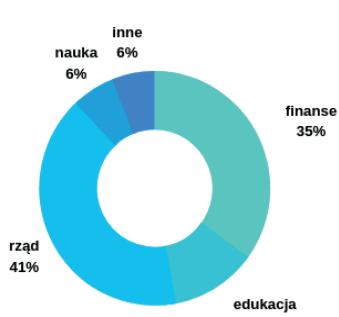
10. Czy Państwa firma planuje utworzenie jednostki, stanowiska bądź zespołu odpowiedzialnego za przeciwdziałanie przestępczości?	☐ tak	☐ nie	☐ nie wiem	☐ nie dotyczy
11. Na jakie rodzaje przestępstw organizacja, którą Pan/Pani reprezentuje będzie narażona w największym stopniu za 10 lat?				

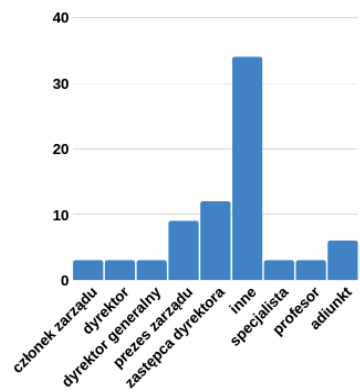
Załącznik C. Profile statystyczne uczestników w podziale na sektory

Profil statystyczny uczestników

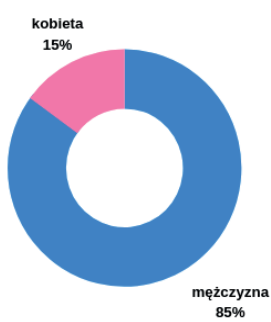
Sektor finansowy

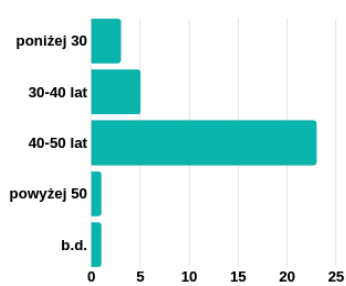
OBSZAR DZIAŁALNOŚCI I PEŁNIONE STANOWISKA





PODZIAŁ POD WZGLĘDEM CECH DEMOGRAFICZNYCH

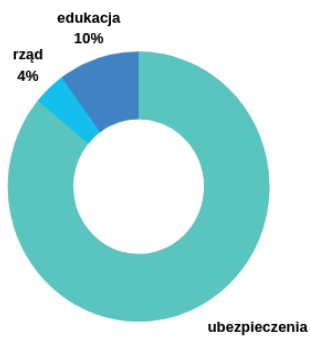


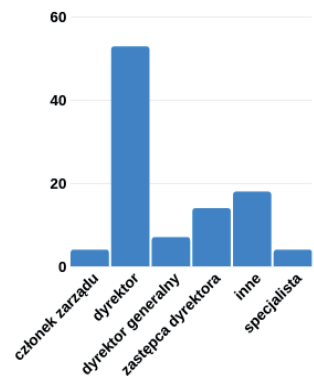


Profil statystyczny uczestników

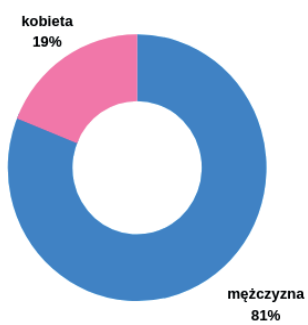
Sektor ubezpieczeń

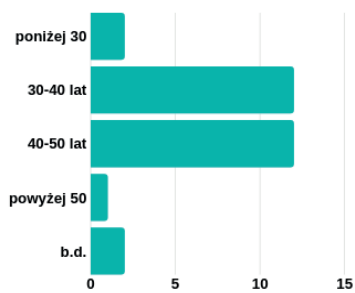
OBSZAR DZIAŁALNOŚCI I PEŁNIONE STANOWISKA





PODZIAŁ POD WZGLĘDEM CECH DEMOGRAFICZNYCH

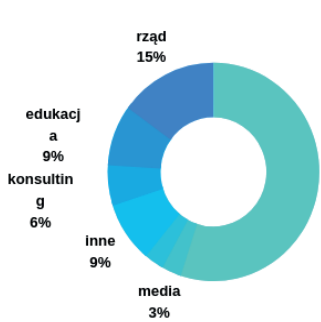


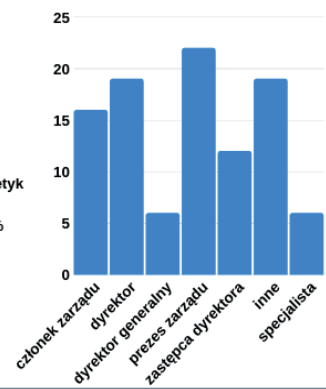


Profil statystyczny uczestników

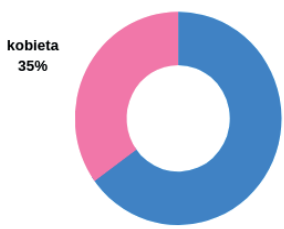
Sektor energetyki

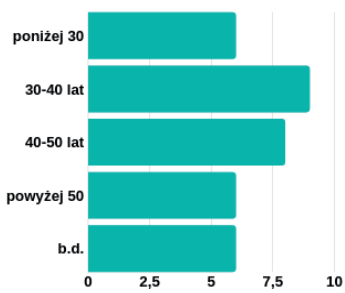
OBSZAR DZIAŁALNOŚCI I PEŁNIONE STANOWISKA





PODZIAŁ POD WZGLĘDEM CECH DEMOGRAFICZNYCH

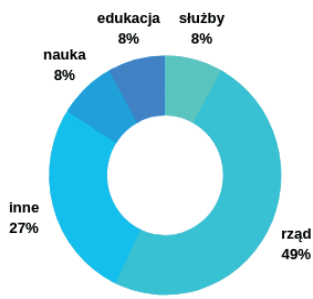


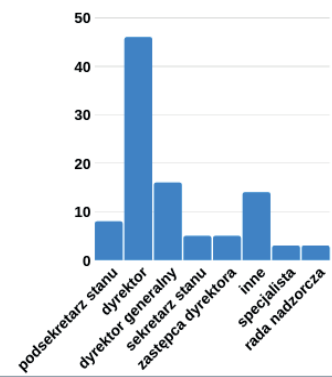


Profil statystyczny uczestników

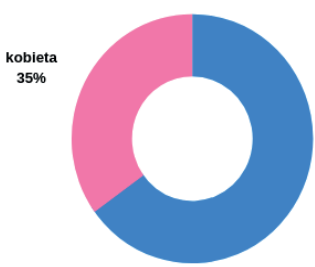
Obszar zarządzania ludźmi w organizacjach

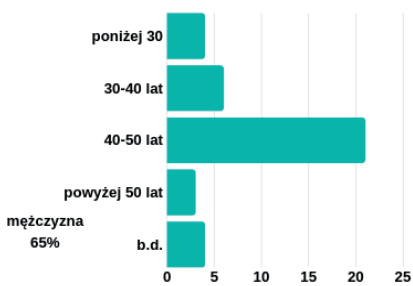
OBSZAR DZIAŁALNOŚCI I PEŁNIONE STANOWISKA





PODZIAŁ POD WZGLĘDEM CECH DEMOGRAFICZNYCH





Załącznik D. Lista organizacji reprezentowanych przez uczestników

(w kolejności alfabetycznej)

Agencja Bezpieczeństwa Wewnętrznego
Alior Bank SA
Bank Gospodarstwa Krajowego
Bank Pocztowy SA
BBS Banner Sp. z o. o.
Bartosiak i Partnerzy Kancelaria Adwokacka Sp. p.
Centralny Szpital Kliniczny MSWiA w Warszawie
Centralny Zarząd Służby Więziennej
Centrum Badań nad Rodziną, Uniwersytet Mikołaja Kopernika w Toruniu
DEEP BI INC SA, Oddział w Polsce
Departament Wojskowych Spraw Zagranicznych MON
Executive Education Center Sp. z o. o.
Gas and Energy Trading Sp. z o. o.
Generalna Dyrekcja Dróg Krajowych i Autostrad
Generalna Dyrekcja Ochrony Środowiska
Główny Inspektorat Jakości Handlowej Artykułów Rolno-Spożywczych
Grupa Azoty SA
Grupa LOTOS SA
Instytut Chemicznej Przeróbki Węgla
Instytut Profilaktyki i Resocjalizacji, Uniwersytet Warszawski
Instytut Wymiaru Sprawiedliwości
Izba Rozliczeniowa Giełd Towarowych SA
JSW KOKS SA
Kancelaria Prezesa Rady Ministrów
Krajowy Depozyt Papierów Wartościowych SA

Kossecki Tax Planning Sp. z o. o.
Krajowa Szkoła Administracji Publicznej
im. Prezydenta RP Lecha Kaczyńskiego
Lubelski Urząd Wojewódzki w Lublinie
Ministerstwo Cyfryzacji
Ministerstwo Edukacji Narodowej
Ministerstwo Energii
Ministerstwo Finansów
Ministerstwo Infrastruktury
Ministerstwo Infrastruktury, Biuro Pełnomocnika Rządu
ds. Centralnego Portu Komunikacyjnego dla RP
Ministerstwo Nauki i Szkolnictwa Wyższego
Ministerstwo Obrony Narodowej
Ministerstwo Przedsiębiorczości i Technologii
Ministerstwo Sprawiedliwości
Ministerstwo Sprawiedliwości,
Departament Informatyzacji i Rejestrów Sądowych
Ministerstwo Zdrowia
Narodowe Centrum Badań i Rozwoju
Narodowy Bank Polski
Oddział Warszawski Stowarzyszenia Elektryków Polskich
Operator Gazociągów Przesyłowych Gaz-System SA
Państwowa Agencja Atomistyki
PGE Polska Grupa Energetyczna SA
PGNiG Serwis Sp. z o. o.
Polski Koncern Naftowy Orlen SA
PKO Bank Hipoteczny SA
PKO Bank Polski SA
PKO Życie Towarzystwo Ubezpieczeń SA
Polska Agencja Prasowa SA
Polska Grupa Górnicza SA
Polskie Górnictwo Naftowe i Gazownictwo SA
Polskie Sieci Elektroenergetyczne SA
PORT Polski Ośrodek Rozwoju Technologii Sp. z o. o.
Powszechny Zakład Ubezpieczeń SA

Prokuratoria Generalna Rzeczypospolitej Polskiej
Prokuratura Krajowa Rzeczypospolitej Polskiej
Prokuratura Okręgowa w Warszawie
Polskie Sieci Elektroenergetyczne SA
SGB-Bank SA
Stowarzyszenie Edukacji Menedżerskiej FORUM
Śląski Urząd Wojewódzki w Katowicach
Tauron Polska Energia SA
Teatr Muzyczny w Poznaniu
Towarowa Giełda Energii SA
Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie
Węglokoks SA
Uniwersytet im. Adama Mickiewicza w Poznaniu,
Wydział Prawa i Administracji
Uniwersytet Warszawski, Wydział Prawa i Administracji

Spis rysunków

Spis tabel

Bibliografia

Abbosh O., Bissel K., LaSalle R., Vazirani M., *Build Pervasive Cyber Resilience Now: Secure the Future Enterprise Today – 2018*, Accenture 2018, https://www.accenture.com/t00010101T000000Z__w__/nz-en/_acnmedia/PDF-81/Accenture-Build-Pervasive-Cyber-Resilience-Now-Landscape.pdf

Blum S., Koslowski A., Moss P., *13th International Review of Leave Policies and Related Research 2017*, International Network on Leave Policies and Related Research, czerwiec 2017, https://www.researchgate.net/profile/Peter_Moss2/publication/318324882_International_Review_of_Leave_Policies_and_Related_Research_2017/links/5964a2b2aca2720a5ccda9ce/International-Review-of-Leave-Policies-and-Related-Research-2017.pdf

Capon N., *Hausser Food Products Company*, Cases at Columbia Business School, 2008, nr ref.: CCW080503.

Cifuentes Hurtado C., *Derecho a Sala Cuna: Situación Actual y Propuesta de Política*, libertad desarrollo, 2012, http://www.sociedadpoliticaspublicas.cl/archivos/CBLOQUET/Panel_Trabajo_y_Maternidad/Derecho%20a%20Sala%20Cuna%20Una%20propuesta%20de%20politica.pdf

Cornelissen T., Dustmann C., Raute A., Schoenberg U., *Universal Childcare: The Potential to Level the Playing Field Between the Rich and Poor*, CEPR Policy Portal, 7.06.2018, https://voxeu.org/article/universal-childcare-family-background-and-school-readiness

Gubbi J., Buyya R., Marusic S., Palaniswami M., *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions*, „Future Generation Computer Systems", 2013, t. 29, nr 7.

Hayashi A.M., *Mommy-track Backlash*, „Harvard Business Review", 2001, t.79, nr 3.

Healy P., Petkoski D., *Fighting Corruption at Siemens*, „Harvard Business School Multimedia/Video Case", 2012, nr 112–702.

Ibarra H., Suesse J.M., *Jeffrey Smith*, 1998, Harvard Business Publishing, nr. ref.: 9-498-043.

International Labour Organization, United Nations Development Programme, *Work and Family: Towards New Forms of Reconciliation with Social Co-responsibility*,

ILO/UNDP, Santiago 2009, http://www.undp.org/publications/pdf/undp_ilo.pdf

Janikowski R., *Nieprzewidywalność w zarządzaniu przedsiębiorstwem*, „Modern Management Review", 2014, t.XIX, nr 21.

Javier Lluch Corell F., *Derecho a la intimidad del trabajador versus control empresarial: una jurisprudencia inestable*, elderecho.com, 01.12.2004, https://elderecho.com/derecho-a-la-intimidad-del-trabajador-versus-control-empresarial-una-jurisprudencia-inestable

Kallqwist R., Aremann R., *Gender Diversity on Swedish Companies' Board of Directors: A study on Gender Diversity in 60 Swedish Listed Small, Medium and Large Cap Companies Between 2009–2015*, Jönköping International Business School, 2017, http://hj.diva-portal.org/smash/record.jsf?pid=diva2%3A1109219&dswid=-513

Lagos Garcia de la Huerta J., Miguel Angel A., Las Heras M., *Eurofirms: Difficult Decisions*, „IESE", 2018, nr DPO-430-E.

Marek S., Białasiewicz M., *Podstawy nauki o organizacji: przedsiębiorstwo jako organizacja gospodarcza*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2008.

Mcpartland B., *Are You Missing out on the Billions of Unclaimed Family Benefits in France?*, „The local", 10.07.2018, https://www.thelocal.fr/20180710/are-you-missing-out-on-the-billions-of-benefits-that-go-unclaimed-in-france

Milliken D., *Swedish Government Drops Plans for Gender Quota Bill for Company Boards*, „Reuters", 12.01.2017, https://www.reuters.com/article/us-sweden-board-equality/swedish-government-drops-plans-for-gender-quota-bill-for-company-boards-idUSKBN14W2AM

Mirkovic J., Reiher P., *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, „ACM SIGCOMM Computer Communication Review", 2004, t.34, nr 2.

Naumann I., McLean C., Koslowski A.S., Tisdall E.K.M., Lloyd E., *Early Childhood Education and. Care Provision: International. Review of Policy, Delivery and Funding. Final Report*, University of Edinburgh, Centre for Research on Families and Relationships, Social Research, Scotland 2013, http://www.nls.uk/scotgov/2013/9781782564164.pdf

Naumann I.K., *'Universal Childcare' and Maternal Employment: the British and the Swedish story*, Social Policy Association, 2015, http://www.social-policy.org.uk/wordpress/wp-content/uploads/2015/04/22_naumann.pdf

OECD, *G20/OECD Principles of Corporate Governance*, OECD, Paryż 2015.

OECD, *Society at a Glance 2016: OECD Social Indicators*, OECD Publishing; Éditions OCDE 2016.

Organisation for Economic Co-operation and Development, *OECD Principles of Corporate Governance*, Paryż 1999.

Pickerd J.S., Summers S.L., Wood D.A., *An Examination of How Entry-Level Staff Auditors Respond to Tone at the Top vis-à-vis Tone at the Bottom*, „Behavioral Research in Accounting", 2014, t.27, nr 1.

Power J.-P., *Quantum Leap: What Will Quantum Computing Mean for Encryption?*, „Symatec Security Blog", 2017.

Richardson D., *Key Findings on Families, Family Policy and the Sustainable Development Goals*, United Nations Children's Fund (UNICEF), Florencja maj 2018, https://www.unicef-irc.org/publications/pdf/Families_and_SDGs_Synthesis_Report.pdf

Sandford N., Darcy K., Mohlenkamp M., Clark B., Eissler L., Haskovec N., Lane K., Nicolosi T., Tucker H., *Compliance Risk Assessments The Third Ingredient in a World-class Ethics and Compliance Program*, Deloitte 2015.

Schwab W., Poujol M., *The State of Industrial Cybersecurity 2018*, Kaspersky Lab, CXP Group, czerwiec 2018, https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

Skuczyński P., *Soft law w perspektywie teorii prawa*, w: Bogucki O., Czepita s. (red.), *System prawny a porządek prawny,* Wydawn. Naukowe Uniw. Szczecińskiego, Szczecin 2008.

Storvik A., Teigen M., *Women on Board The Norwegian Experience*, Friedrich Ebert Stiftung, International Policy Analysis, Berlin czerwiec 2010, https://library.fes.de/pdf-files/id/ipa/07309.pdf

Thoursie A., *El modelo de familia de dos sustentadores con un permiso parental prolongado: lecciones de suecia*, Instito de Studios Fiscales, b.d., http://www.ief.es/docs/investigacion/genero/LG_Thoursie.pdf

Vaccaro A., Ramus T., *Jeffrey Skilling, Bernie Madoff the Monster & the Other Smartest Guys of the Room*, „Harvard Business Review Case Study", 2008, nr IES233-PDF-ENG.

Vanson B., *Prevention Is Better Than Cure: Business Security – The Journey Continues*, w: *2018 Risk: Value Report*, NTT security, 2018, https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_report_risk-value_2018_us_uea_v1.pdf

Council Directive 92/85 /EEC, „Official Journal of the European Communities", 28.11.1992, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31992L0085&from=PL

Childcare Vouchers in the UK, Accor services, 2008, https://www.edenred.com/sites/default/files/pdf/documentations/presentation-idayfocuschildcarevouchers-oct2008-en.pdf

Formalizing Domestic Work Through the Use of Service Vouchers, Internationa Labour Organization, 2012, http://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@actrav/documents/publication/wcms_220717.pdf

Labour Market Effects of Parental Leave Policies in OECD Countries, OECD Social, Employment and Migration Working Papers, 10.01.2013, https://www.oecd-ilibrary.org/social-issues-migration-health/labour-market-effects-of-parental-leave-policies-in-oecd-countries_5k8xb6hw1wjf-en

Best Practice Guide Workplace Privacy, Australian Government Fair Work Ombudsman 2014, https://www.fairwork.gov.au/ArticleDocuments/711/Workplace-privacy-best-practice-guide.pdf.aspx

Affirmative Action | Overview, National conference of state legislature, 02.07.2014, http://www.ncsl.org/research/education/affirmative-action-overview.aspx

Good Governance Code of Listed Companies, Comision nacional del mercado de valores, luty 2015, https://www.cnmv.es/docportal/publicaciones/codigogov/good_governanceen.pdf

Cyber Attack Trends 2018 Mid-year Report, Check Point Research, 2018, https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf

Ten Years on from Norway's Quota for Women on Corporate Boards, „The Economist", 17.02.2018, https://www.economist.com/business/2018/02/17/ten-years-on-from-norways-quota-for-women-on-corporate-boards

Directive of The European Parliament and of The Council on The Protection of Persons Reporting on Breaches of Union Law, t. 2018/0106 (COD), https://eur-lex.europa.eu/resource.html?uri=cellar:a4e61a49-46d2-11e8-be1d-01aa75ed71a1.0001.02/DOC_1&format=PDF

TOP500 List – November 2018 | TOP500 Supercomputer Sites, https://www.top500.org/list/2018/11/.

Universal Service Employment Cheque, Eurofound, b.d., https://www.eurofound.europa.eu/es/data/tackling-undeclared-work-in-europe/database/universal-service-employment-cheque-france

Help Paying for Childcare, https://www.gov.uk/help-with-childcare-costs/free-childcare-and-education-for-2-to-4-year-olds

Maternity/Paternity Leave and Parental Leave, Registers Island, b.d., https://www.island.is/en/family/having_a_baby/maternity_paternity_leave_and_parental_leave/

Employee Rights 101: What Every Business Owner Needs to Know, Square, Inc., b.d., https://squareup.com/townsquare/employee-rights-101-what-every-business-owner-needs-to-know

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
Piotr KWIATKIEWICZ, Uniwersytet Zielonogórski
Grzegorz STRUPCZEWSKI, Uniwersytet Ekonomiczny w Krakowie
Joanna TACZKOWSKA-OLSZEWSKA, Akademia Sztuki Wojennej

ROZDZIAŁ I

Heading Into the Future. Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w konteście przyszłości i przyszłych zmian

BARTŁOMIEJ ORĘZIAK[1], MARCIN WIELEC[2]

1. Heading Into ihe Future: Wprowadzenie

Ostatnim modułem międzynarodowego projektu badawczego „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości"[3] był Heading into the Future, który dokonywał podejścia analitycznego dotyczącego przyszłości i przyszłych zmian, w szczególności na podstawie wcześniejszych modułów: Assessing Foundations, Improving Performance, Transforming People and Organizations. Zasadniczym celem było określenie możliwych przyczyn i rodzajów przestępczości w przyszłości oraz przygotowania prewencyjnego (komparatystyczne ujęcie polskich problemów) na tle starannie wyselekcjonowanych zagadnień drugiego rzędu. Prowadzone badania miały zamiar dokonać podejścia analitycznego dotyczącego rynku

[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/

finansowego, rynku ubezpieczeniowego, rynku energetycznego oraz zarządzania ludźmi w organizacji z wykorzystaniem technologii utrudniających dokonywanie przestępstw w tych zakresach nie tylko w wymiarze Heading into the Future[4], ale także w świetle modułów Assessing Foundations[5] Improving Performance[6] oraz Transforming People and Organizations[7]. Podejmowane działania uwzględniały fakt, że analiza przyczyn powstawania sytuacji, w których dochodzi do przestępstw w obszarze rynku finansowego, ubezpieczeniowego, energetycznego oraz zarządzania ludźmi w organizacji została zakwalifikowana jako główny obszar badawczy oraz analityczny pryzmat Projektu[8]. W tym aspekcie skoncentrowano się na wskazanych kwestiach oraz ocenie poziomu zaawansowania i zakresu wykorzystania przyszłej technologii zapobiegającej przyczynom przestępczości, w szczególności w kontekście zagrożeń dla podstawowych zasad polskiego porządku prawnego.

2. Heading Into the Future: Przedmiot prac

Moduł Heading into the Future polegał w przeważającej mierze na zwróceniu uwagi na przedstawienie perspektywy najnowocześniejszych metod kwantyfikujących rozwiązania prawne, gospodarcze, technologiczne oraz

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

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

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

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

[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.

organizacyjne z zakresu przeciwdziałania przestępczości. Moduł Heading Into the Future został poświęcony problematyce przygotowania planów na przyszłość w poszczególnych obszarach, gdzie zakres tematyczny obejmował budowanie kultury organizacyjnej wspierającej postawy praworządności, tworzenie strategicznych scenariuszy na przyszłość oraz innowacyjnych strategii rozwoju dla poszczególnych obszarów. Relewantne dla przedmiotu prowadzonych badań okazały się także zagadnienia dotyczące przygotowania na nowe rodzaje przestępstw w przyszłości. Interdyscyplinarne ujęcie problematyki przeciwdziałania przestępczości pozwoliło na szeroką analizę przedstawionych segmentów badawczych oraz aktualnie stanowi podstawy do dalszych prac i ukazuje konieczność podjęcia daleko idącej współpracy, w szczególności w kontekście aktualnie dostrzegalnego postępu technicznego, technologicznego oraz cywilizacyjnego.

3. Heading Into the Future: Metodologia

Metodologia zastosowana w module Heading into the Future nie różniła się w założeniach od tej wykorzystywanej w całym projekcie. W związku z powyższym, przy zwróceniu uwagi na kryteria ewaluacyjne[9], zastosowano klasyczną dla nauk prawnych metodę dogmatyczno-formalną, która zwierała w sobie elementy egzegezy treści aktu prawnego oraz hermeneutykę językową. Dodatkowo za uzasadnione specyfiką desygnatów tytułowego zagadnienia uznano wykorzystanie metody prawnoporównawczej, w ramach której posłużono się metodą komparatystyki prawniczej Kötza i Zweigerta: 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 innych branych pod uwagę narzędzi badawczych należą 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*, Warszawa 2008.

analizy i krytyki piśmiennictwa, analizy i konstrukcji logicznej, badania dokumentów, monograficzne oraz obserwacyjne. Nie bez znaczenia okazały się również meta-językowo określone: 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. Heading Into the Future: Potencjalni beneficjenci prac projektowych

Moduł Heading into the Future nie posiada swojej specyficznej grupy beneficjentów, a w tym zakresie opiera się na liście takowych podmiotów stworzonej na potrzeby całości projektu. Mowa tutaj o oddzielnych katalogach dla każdego z obszarów (finanse, energetyka, ubezpieczenia, zarządzanie ludźmi w organizacji) oraz o wspólnej liście podmiotów naukowych mogących być zainteresowanymi wynikami prowadzonych analiz.

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. Heading Into the Future: Ochrona praw człowieka jako istotny element prac projektowych

Heading into the Future opiera na katalogu praw i wolności człowieka, który został stworzony na rzecz prac projektowych. Przyszłość oraz przyszłe zmiany w technologii, prawie oraz gospodarce nie mogą zapominać o wypracowanych standardach ochronnych. Mowa tutaj w szczególności o konstytucyjnej ochronie praw i wolności (Konstytucja Rzeczypospolitej Polskiej[11]) oraz

[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*

europejskiej ochronie praw człowieka (1. Unia Europejska – Karta praw podstawowych Unii Europejskiej[12]; 2. Rada Europy – Konwencja o ochronie praw człowieka i podstawowych wolności[13]). Projektowane zmiany powinny być zgodne, 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.

---

w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 Nr 78 poz. 483; 2001 Nr 28 poz. 319; 2006 Nr 200 poz. 1471; 2009 Nr 114 poz. 946).

[12] *Karta praw podstawowych Unii Europejskiej (Dz. Urz. 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).*

2. Każdy pozbawiony wolności nie na podstawie wyroku sądowego ma prawo odwołania się do sądu w celu niezwłocznego ustalenia legalności tego pozbawienia. O pozbawieniu wolności powiadamia się niezwłocznie rodzinę lub osobę wskazaną przez pozbawionego wolności. 3. Każdy zatrzymany powinien być niezwłocznie i w sposób zrozumiały dla niego poinformowany o przyczynach zatrzymania. Powinien on być w ciągu 48 godzin od chwili zatrzymania przekazany do dyspozycji sądu. Zatrzymanego należy zwolnić, jeżeli w ciągu 24 godzin od przekazania do dyspozycji sądu nie zostanie mu doręczone postanowienie sądu o tymczasowym aresztowaniu wraz z przedstawionymi zarzutami. 4. Każdy pozbawiony wolności powinien być traktowany w sposób humanitarny. 5. Każdy bezprawnie pozbawiony wolności ma prawo do odszkodowania".

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

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

toczy się postępowanie o wydalenie lub ekstradycję. 2. Każdy, kto został zatrzymany, powinien zostać niezwłocznie i w zrozumiałym dla niego języku poinformowany o przyczynach zatrzymania i o stawianych mu zarzutach. 3. Każdy zatrzymany lub aresztowany zgodnie z postanowieniami ustępu 1 lit. c) niniejszego artykułu powinien zostać niezwłocznie postawiony przed sędzią lub innym urzędnikiem uprawnionym przez ustawę do wykonywania władzy sądowej i ma prawo być sądzony w rozsądnym terminie albo zwolniony na czas postępowania. Zwolnienie może zostać uzależnione od udzielenia gwarancji zapewniających stawienie się na rozprawę. 4. Każdy, kto został pozbawiony wolności przez zatrzymanie lub aresztowanie, ma prawo odwołania się do sądu w celu ustalenia bezzwłocznie przez sąd legalności pozbawienia wolności i zarządzenia zwolnienia, jeżeli pozbawienie wolności jest niezgodne z prawem.

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

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

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

Zgodnie z art. 42 Konstytucji Rzeczypospolitej Polskiej: „1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na

zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu.".

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

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

Zgodnie z art. 6 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy ma prawo do sprawiedliwego i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony ustawą przy rozstrzyganiu o jego prawach i obowiązkach o charakterze cywilnym albo o zasadności każdego oskarżenia w wytoczonej przeciwko niemu sprawie karnej. Postępowanie przed sądem jest jawne, jednak prasa i publiczność mogą być wyłączone z całości lub części rozprawy sądowej ze względów obyczajowych, z uwagi na porządek publiczny lub bezpieczeństwo państwowe w społeczeństwie demokratycznym, gdy wymaga tego dobro małoletnich lub gdy służy to ochronie życia prywatnego stron albo też w okolicznościach szczególnych, w granicach uznanych przez sąd za bezwzględnie konieczne, kiedy jawność mogłaby przynieść szkodę interesom wymiaru sprawiedliwości. 2. Każdego oskarżonego o popełnienie czynu zagrożonego karą uważa się za niewinnego do czasu udowodnienia mu winy zgodnie z ustawą. 3. Każdy oskarżony o popełnienie czynu zagrożonego karą ma co najmniej prawo do:

a) niezwłocznego otrzymania szczegółowej informacji w języku dla niego zrozumiałym o istocie i przyczynie skierowanego przeciwko niemu oskarżeniu; b) posiadania odpowiedniego czasu i możliwości do przygotowania obrony; c) bronienia się osobiście lub przez ustanowionego przez siebie obrońcę, a jeśli nie ma wystarczających środków na pokrycie kosztów obrony, do bezpłatnego korzystania z pomocy obrońcy wyznaczonego z urzędu, gdy wymaga tego dobro wymiaru sprawiedliwości; d) przesłuchania lub spowodowania przesłuchania świadków oskarżenia oraz żądania obecności i przesłuchania świadków obrony na takich samych warunkach jak świadków oskarżenia; e) korzystania z bezpłatnej pomocy tłumacza, jeżeli nie rozumie lub nie mówi językiem używanym w sądzie".

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

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

Zgodnie z art. 49 Karty praw podstawowych Unii Europejskiej: „1. Nikt nie może zostać skazany za popełnienie czynu polegającego na działaniu lub zaniechaniu, który według prawa krajowego lub prawa międzynarodowego nie stanowił czynu zabronionego pod groźbą kary w czasie jego popełnienia. Nie wymierza się również kary surowszej od tej, którą można było wymierzyć w czasie, gdy czyn zabroniony pod groźbą kary został popełniony. Jeśli ustawa, która weszła w życie po popełnieniu czynu zabronionego pod groźbą kary, przewiduje karę łagodniejszą, ta właśnie kara ma zastosowanie. 2. Niniejszy

artykuł nie stanowi przeszkody w sądzeniu i karaniu osoby za działanie lub zaniechanie, które w czasie, gdy miało miejsce, stanowiło czyn zabroniony pod groźbą kary, zgodnie z ogólnymi zasadami uznanymi przez wspólnotę narodów. 3. Kary nie mogą być nieproporcjonalnie surowe w stosunku do czynu zabronionego pod groźbą kary".

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

Prawem do poszanowania życia prywatnego i rodzinnego.

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

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

Zgodnie z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób".

Prawem do ochrony danych osobowych.

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

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

Prawem do wolności opinii i informacji.

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

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

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

Prawem do wolności zgromadzeń i stowarzyszania się.

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

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

Zgodnie z art. 59 Konstytucji Rzeczypospolitej Polskiej: „1. Zapewnia się wolność zrzeszania się w związkach zawodowych, organizacjach społeczno-zawodowych rolników oraz w organizacjach pracodawców. 2. Związki zawodowe oraz pracodawcy i ich organizacje mają prawo do rokowań, w szczególności w celu rozwiązywania sporów zbiorowych, oraz do zawierania układów zbiorowych pracy i innych porozumień. 3. Związkom zawodowym przysługuje

prawo do organizowania strajków pracowniczych i innych form protestu w granicach określonych w ustawie. Ze względu na dobro publiczne ustawa może ograniczyć prowadzenie strajku lub zakazać go w odniesieniu do określonych kategorii pracowników lub w określonych dziedzinach. 4. Zakres wolności zrzeszania się w związkach zawodowych i organizacjach pracodawców oraz innych wolności związkowych może podlegać tylko takim ograniczeniom ustawowym, jakie są dopuszczalne przez wiążące Rzeczpospolitą Polską umowy międzynarodowe".

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

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

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

Zgodnie z art. 50 Karty praw podstawowych Unii Europejskiej: „Nikt nie może być ponownie sądzony lub ukarany w postępowaniu karnym za ten sam

czyn zabroniony pod groźbą kary, w odniesieniu do którego zgodnie z ustawą został już uprzednio uniewinniony lub za który został już uprzednio skazany prawomocnym wyrokiem na terytorium Unii".

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

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

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

Prawem do odszkodowania za bezprawne skazanie.

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

Prawem do odwołania w sprawach karnych.

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

Zgodnie z art. 2 Protokołu nr 7 do Konwencji o ochronie praw człowieka i podstawowych wolności: „1. Każdy, kto został uznany przez sąd za winnego popełnienia przestępstwa, ma prawo do rozpatrzenia przez sąd wyższej instancji jego sprawy, tak w przedmiocie orzeczenia o winie, jak i co do kary. Korzystanie z tego prawa, a także jego podstawy, reguluje ustawa. 2. Wyjątki od tego prawa mogą być stosowane w przypadku drobnych przestępstw, określonych w ustawie, lub w przypadkach, gdy dana osoba była sądzona w pierwszej instancji przez sąd najwyższy albo została uznana za winną i skazana w wyniku zaskarżenia wyroku uniewinniającego sądu pierwszej instancji".

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

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 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. Heading Into the Future: Uzasadnienie prowadzenia prac badawczych

Prawo, gospodarka i technologia powinna aktualnie skupiać się na dostrzegalnym postępie technicznym, technologicznym oraz cywilizacyjnym. Świat podlega nieustannym zmianom, które z punktu widzenia nauki wymagają badawczej refleksji. Nie inaczej dzieje się z modułem Heading into the Future. Ten specyficznie zdefiniowany obszar badawczy miał za zadanie dokonanie niestandardowego podejścia analitycznego, korzystając z wcześniej wypracowanych rezultatów projektowych, na rzecz zapobiegania przyczynom przyszłej przestępczości. W związku z powyższym badanie tego co przyszłe i nieznane oraz znajdowanie jasnych oraz logicznych rozwiązań, w tym zaleceń, stanowiło główne uzasadnienie modułu Heading into the Future.

ROZDZIAŁ II

Oszustwa finansowe – współczesne trendy

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

1. Analiza trendów dotyczących statystyk przestępstw finansowych w ostatnich latach

O tendencjach zmian oszustw finansowych można próbować wnioskować na podstawie aktualnych trendów i badań ankietowych. Dlatego poniżej przedstawiono wybrane wyniki badań ankietowych dotyczących przestępczości finansowej, zrealizowanych przez: brytyjską organizację Financial

[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.

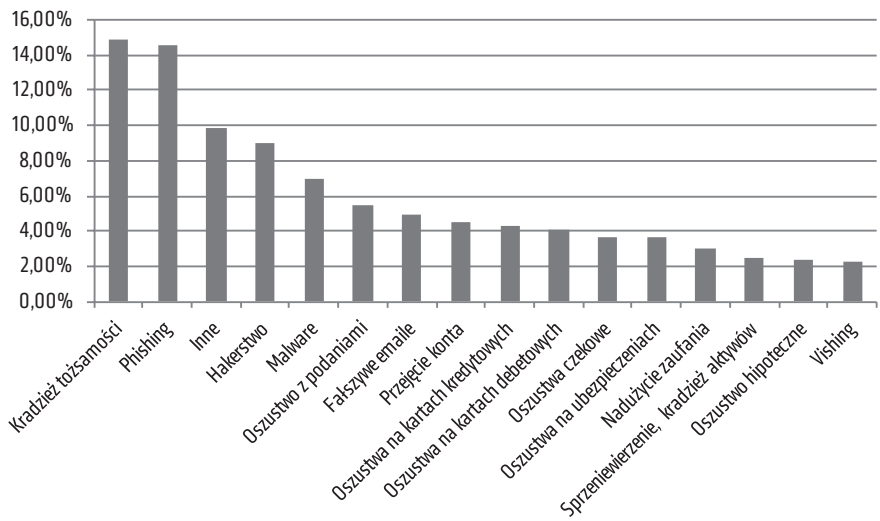
[3] Doktor fizyki teoretycznej Uniwersytetu Jagiellońskiego, zatrudniona na stanowisku adiunkta w Katedrze Rynków Finansowych, a wcześniej na stanowisku asystenta w Katedrze Ekonometrii i Badań Operacyjnych w Kolegium Ekonomii, Finansów i Prawa, Uniwersytetu Ekonomicznego w Krakowie, profesor wizytujący 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

Conduct Authority (badania przeprowadzono w Wielkiej Brytanii), polską organizację Konfederacja Przedsiębiorstw Finansowych w Polsce (badania przeprowadzono w Polsce) i w końcu badania dla całego świata przeprowadzone przez Ernst & Young.

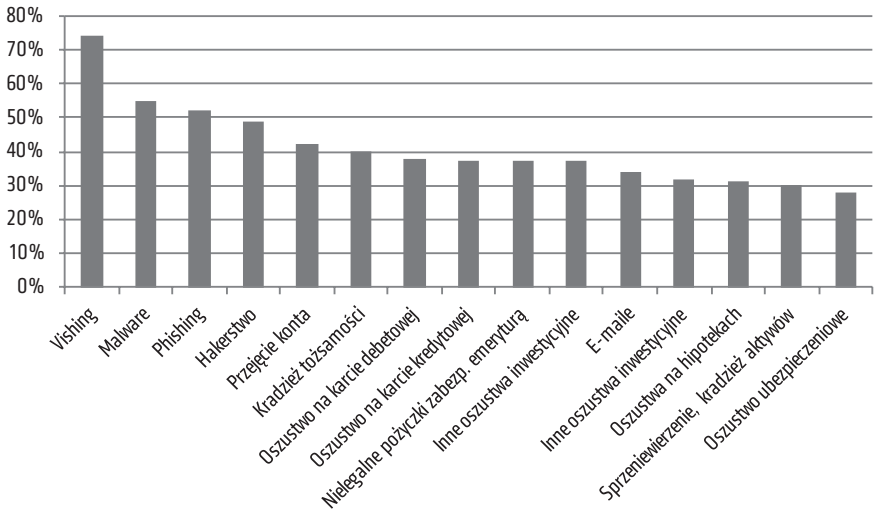
Mimo że dane są fragmentaryczne i niepełne, to pozwalają wyciągnąć pewne wnioski na temat zmian oszustw finansowych w Wielkiej Brytanii i w Polsce oraz potencjalnych kierunków na przyszłość. Zakładając, że rynek brytyjski jest bardziej otwarty i rozwinięty, można przypuszczać, że przynajmniej do pewnego stopnia tendencje obserwowane przez FCA mogą znaleźć w przyszłości odzwierciedlenie także na rynku polskim. Dlatego na rysunkach 1 i 2 pfokazano wyniki badań ankietowych nad subiektywnym poczuciem zagrożenia przestępczością finansową w Wielkiej Brytanii oraz tendencjami wzrostowymi oszustw finansowych.

Rysunek 1. Subiektywne postrzeganie zagrożenia różnymi formami przestępstw finansowych, Wielka Brytania, rok 2017 [% respondentów]



Źródło: opracowanie własne na podstawie *Financial Conduct Authority, Financial Crime: Analysis of Firms' Data*, https://www.fca.org.uk/publication/research/financial-crime-analysis-firms-data.pdf, *Chart 1: firms' assessment of the prevalence of frauds*, 2017, s. 8

Rysunek 2. Procent firm (netto), według których dany rodzaj przestępstwa finansowego wzrósł w roku 2017 [% respondentów]



Źródło: opracowanie własne na podstawie Financial Conduct Authority, *Financial Crime: Analysis of Firms' Data*, https://www.fca.org.uk/publication/research/financial-crime-analysis-firms-data.pdf, *Chart 4: proportion of firms that perceived the incidence of fraud increased or decreased, by fraud type*, 2017, s. 11

Jak wynika ze statystyk, ankietowani uważali, że w ostatnich lata przede wszystkim wzrosło zagrożenie wszelkimi rodzajami cyberataków: *vishing*, *malware*, *phishing*, hakerstwo, przejęcie konta klientów instytucji finansowych. Za najgroźniejsze uznali zaś kradzież tożsamości, *phishing*, hakerstwo oraz *malware*.

Dane z podobnych badań przeprowadzonych dla Polski porównano z wynikami firmy Ernst and Young, a opublikowanymi w publicznie dostępnych raportach: Ernst&Young FIDS Global Forensic Data Analytics Survey dla lat 2016 oraz 2018 (tabela 1). Jak wynika z zestawienia, w opinii respondentów polskich rośnie zagrożenie cyberatakami, ale procent osób obserwujących te ataki jest o połowę niższy niż średnia dla całego świata. Potwierdza to wcześniejsze spostrzeżenia, że należy spodziewać się wzrostu tych ataków w Polsce w kolejnych latach. Kolejnym trendem wzrostowym widocznym w tabeli 1 są nadużycia na kartach kredytowych i pranie brudnych pieniędzy.

Tabela 1. Obszary, w których w ostatnich 2 latach ryzyko wystąpienia nadużycia wzrosło (procent ankietowanych netto wierzący, że nastąpi wzrost) [% respondentów]

Rok	Organizacja	Cyberataki	Nadużycia wewnętrzne	Fałszowanie sprawozdań	Ryzyko M&A	Pranie pieniędzy	Ryzyko związane z inwestycjami	Korupcja	Nadużycia kart kredytowych	Nieautoryzowane transakcje na rachunkach klientów	Wyłudzenia kredytów
16	KPFP	31	31	29	29	26	20	9			
16	FDA	62	42	26	28	25	34	44			
17	KPFP	35	21	21		21			15	23	50
17	FDA										
18	KPFP	42	7	23		36		13	10	40	45
18	FDA	75	39	28	32	31	37	43	37	42	

Źródło: opracowanie własne na podstawie Związek Przedsiębiorstw Finansowych w Polsce, *Nadużycia w sektorze finansowym* za lata 2016, 2017, 2018, https://www.zpf.pl/pliki/raporty/ (niektóre dane szacowano). Dane do porównań częściowo pochodzą także z badania EY FIDS Global Forensic Data Analytics Survey 2016 oraz 2018

W tabeli 2 zaprezentowano skalę strat, jakie poniosły instytucje finansowe (banki, instytucje pożyczkowe i firmy leasingowe) objęte badaniami Konfederacji Przedsiębiorstw Finansowych w Polsce w latach 2017 oraz 2018. Jak wynika z tabeli 2, spadła liczba instytucji ze stratami poniżej 100 tys. zł, a wzrósł dwukrotnie odsetek klientów, których straty z powodu oszustw finansowych wynosiły ponad 10 mln zł. Wzrósł także, choć nieznacznie, odsetek strat w przedziale od 1 do 10 mln zł. Sugeruje to, aby oczekiwać dalszego wzrostu strat w kolejnych latach.

Tabela 2. Łączne straty poniesione przez instytucje finansowe w wyniku przestępstw finansowych [% respondentów]

Rok	Poniżej 100 tys	100–500 tys.	500 tys.–1 mln	1–10 mln	powyżej 10 mln
2017	17	27	17	29	5
2018	10	29	10	32	10

Źródło: opracowanie na podstawie: *Rysunek 7 Poniesione przez instytucje łączne straty w wyniku popełnionych nadużyć*, w: Związek Przedsiębiorstw Finansowych w Polsce, *Nadużycia w sektorze finansowym za rok 2018*, https://www.zpf.pl/pliki/raporty/

W tabeli 3 przedstwiono trzy najbardziej skuteczne metody walki z oszustwami finansowymi wśród respondentów badań Konfederacji Przedsiębiorstw Finansowych w Polsce. Przez okres 5 lat metody te otrzymywały najwyższe oceny co do ich skuteczności. Wszystkie wymagają zaangażowania ludzi i nie są oparte na systemach automatycznych. Sugeruje to problemy, jakie one rodzą, przynajmniej obecnie.

Tabela 3. Najskuteczniejsze metody walki z oszustwami finansowymi (skala ocen od 1 do 5)

Ocena	Wewnętrzny zespół	Wewnętrzne bazy danych	Weryfikacja danych na wejściu
2014	4.3	4.2	4.3
2015	4.33	4.26	4.15
2016	4.1	4.24	4.25
2017	4.7	4.13	4.05
2018	4.46	4.3	4.13

Źródło: opracowanie własne na podstawie Związek Przedsiębiorstw Finansowych w Polsce, *Nadużycia w sektorze finansowym za lata 2016, 2017, 2018*, https://www.zpf.pl/pliki/raporty/ (niektóre dane szacowano)

W tabelach 4 i 5 zaprezentowano wyniki badań Konfederacji Przedsiębiorstw Finansowych w Polsce za lata 2017 oraz 2018 dotyczące technik analitycznych, jakie stosują banki (raporty osobno analizują jeszcze firmy pożyczkowe oraz leasingowe, ale banki posiadają najszerszą paletę metod, z jakich korzystają). Jak wynika z tabel, wszystkie badane banki stosowały silniki reguł biznesowych, modele scoringowe, analizę sieci powiązań, *workflow* oraz raportowanie zgłoszeń. Tylko część stosowała modele predykcyjne czy *text-mining*.

Tabela 4. Techniki analityczne stosowane przez banki (procent banków) [%]

Ile używa	Silnik reguł biznesowych	Model scoringowy	Modele predykcyjne	Wykrywanie anomalii	Analiza sieci powiązań	Text-mining	Analiza geoprzestrzenna	Analiza publicznych danych	Workflow	Raportowanie	Jeden zintegrowany interfejs
2017	82	76	35	59	65	12	24	35	65	47	12
2018	100	100	57	86	100	57	86	86	100	100	57

Źródło: opracowanie własne na podstawie Związek Przedsiębiorst Finansowych w Polsce, *Nadużycia w sektorze finansowym za lata 2017, 2018*, https://www.zpf.pl/pliki/raporty/ (niektóre dane szacowano)

Jeżeli chodzi o ocenę skuteczności poszczególnych instrumentów przez banki, to najwyższą ewaluację skuteczności otrzymały silniki reguł biznesowych, wykrywanie anomalii, analiza sieci powiązań. Sugeruje to, że w niedalekiej przyszłości wszystkie banki będą stosowały wykrywanie anomalii, jest to bowiem metoda wysoko oceniana, a niestosowana jeszcze przez wszystkie banki.

Tabela 5. Ocena technik analitycznych stosowanych przez banki (skala 1–5)

Ocena	Silnik reguł biznesowych	Model scoringowy	Modele predykcyjne	Wykrywanie anomalii	Analiza sieci powiązań	Text-mining	Analiza geoprzestrzenna	Analiza publicznych danych	Workflow	Raportowanie	Jeden zintegrowany interfejs
2017	4.07	3.77	3.5	3.9	4	5	4	3.83	3.64	4.13	4.5
2018	4.4	3.9	3.8	4.5	4.3	3.3	3.7	3.5	3.6	3.4	3

Źródło: opracowanie własne na podstawie *Raporty Konfederacji Przedsiębiorstw Finansowych w Polsce, Nadużycia w sektorze finansowym za lata:* 2017, 2018, https://www.zpf.pl/pliki/raporty/ (niektóre dane szacowano)

2. Trendy na przyszłość wynikające z rozwoju technologii oraz internacjonalizacji

Aby określić kierunki zmian oszustw finansowych i metod ich wykrywania w przyszłości, oprócz danych statystycznych przeanalizowano różnorodne raporty instytucji zajmujących się przestępczością finansową. Jak z nich

wynika, w przyszłości należy spodziewać się większego rozdrobnienia przestępstw finansowych – przynajmniej część z nich będzie obejmować coraz więcej osób, ale zabierać im coraz mniejsze kwoty, co wymaga nowych technik wykrywania takich oszustw. Będą one także bardziej umiędzynarodowione. Dane finansowe takich przestępców są rozsiane po całym świecie, co będzie wymagało lepszej synchronizacji służb i ujednolicenia prawodawstwa, aby oszuści nie wykorzystywali różnic w systemach prawnych i braków koordynacji pomiędzy służbami nadzoru i wymiaru sprawiedliwości w różnych kraach.

Przestępcy będą także prawdopodobnie wykorzystywać wzrost liczby transakcji finansowych wykonywanych za pomocą telefonów komórkowych, czemu mogą nie być w stanie podołać systemy i serwery banków. Część transakcji finansowych może także być wykonywana za pomocą sieci *peer -to-peer*[5]. Oprócz tego, możliwe jest zagrożenie ze strony internetu rzeczy (ang. *Internet of Things*), gdzie do sieci będą podłączane słabo zabezpieczone urządzenia domowe[6].

Z uwagi na coraz większą wirtualizację życia, oszuści mogą także wykorzystać rosnące zakupy dokonywane przez internet, gdzie kupujący podaje nie tylko swoje dane personalne, ale także pełne dane kart kredytowych. Co prawda, instytucje finansowe starają się coraz lepiej je zabezpieczać, ale póki co nowe rozwiązania nie okazały się bezpieczniejsze, czego dobrym przykładem jest protokół EMV[7] (ang. *Europay, MasterCard, Visa*), który został zmanipulowany, zanim jeszcze karty trafiły do sklepów[8]. Co do zabezpieczeń opartych na danych biometrycznych, to istnieje ryzyko, że oszuści już obecnie pracują nad rozwiązaniami opartymi na sztucznej inteligencji, które będą w stanie uczyć się wyrazów twarzy, czytać z ust, replikować głos innej osoby, co pozwoli im jeszcze lepiej podszywać się pod inne osoby[9]. Z tego samego powodu należy spodziewać się wzrostu liczby ataków hakerskich, przykładem

---

[5] Lexis Nexis, *Future Financial Crime Risks*, listopad 2015, https://www.bba.org.uk/wp-content/uploads/2015/12/Future-Financial-Crime-Risks-DIGITAL-final.pdf (dostęp: 10.09.2019).

[6] CIFAS, *30 facts about fraud: past, present and future*, https://www.cifas.org.uk/insight/30-facts-about-fraud-past-present-future, (dostęp: 10.09.2019).

[7] STAR, *First Data, The Future of Fraud*, https://www.firstdata.com/downloads/pdf/STARFraudeBookFINAL.pdf (dostęp: 15.09.2019).

[8] Ibid.

[9] CIFAS, *30 facts about fraud…*, op. cit.

napadu hakerskiego jest kradzież miliarda dolarów z konta centralnego banku Bangladeszu, które znajdowało się w nowojorskim oddziale Rezerwy Federalnej USA. Kradzież miała miejsce w lutym 2016 r. i dokonano jej za pomocą fałszywych instrukcji w systemie SWIFT. Oprogramowanie hakerskie rozwija się równie dynamicznie jak zwykłe oprogramowanie, dostępne są aktualizacje i nowe programy[10]. Prawdopodobnie nie spadną także szkody wywoływane przez trojany i inne złośliwe oprogramowanie wysyłane do klientów banków. Można spodziewać się moduralnego malware, które oferuje więcej możliwości niż tylko natychmiastową kradzież pieniędzy z konta bankowego. Ransomware będzie oceniało możliwości finansowe ofiar i dostosowywało wielkość okupu[11]. Innym typem oszustwa, które może zyskiwać na popularności, jest autoryzowana płatność typu push (ang. *authorized push payment*), w ramach której posiadacz rachunku będzie oszukiwany i sam wykona przelew na konto oszusta. Aby uniknąć skutków włamań do systemów, instytucje finansowe mogą w przyszłości opierać swoją rachunkowość na technologii *blockchain*, która jest obecnie pod tym kątem testowana. Aby uniknąć włamań do sklepów internetowych, mogą one tworzyć własne aplikacje, za pomocą których będzie można dostać się do konta założonego w sklepie[12]. Dane będą transformowane w kod, aby zapobiegać nieautoryzowanemu dostępowi[13].

Innym potencjalnym zagrożeniem może być „sprytny pył" (ang. *smart dust*), czyli tranzystory wielkości cząsteczek kurzu, które będą umożliwiały przestępcom podsłuchiwać rozmowy telefoniczne, nagrać, co ktoś pisze na klawiaturze albo ukraść odciski palców[14].

Dużo zagrożeń może wynikać także z rozwoju sztucznej inteligencji. Nadmierne poleganie na algorytmach może powodować fałszywe poczucie bezpieczeństwa. Złodzieje mogą znaleźć słabości systemu i je wykorzystać, aby nie wywoływać alarmów w systemach monitorowania (zabranie kontroli

[10] National Crime Agency (Wielka Brytania), *National Strategic Assessment of serious and organized crime 2019*, https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file (dostęp: 20.09.2019).

[11] Ibid.

[12] STAR, *First Data*…, op. cit.

[13] National Crime Agency (Wielka Brytania), *National Strategic Assessment*…, op. cit.

[14] CIFAS, *30 facts about fraud*…, op. cit.

człowieka)[15]. A jeżeli kiedyś dojdzie do tego, że sztuczna inteligencja umożliwi komunikację za pomocą sygnałów elektronicznych (komunikacja za pomocą myśli), to nie istnieje na razie skuteczny sposób zabezpieczenia takiej komunikacji (aby romawiać z osobą, z którą chciało się rozmawiać[16]).

Agencje zajmujące się nadzorowaniem przestępstw finansowych ostrzegają także przed kryptowalutami, których rynki są na razie mało transparentne, a instytucje zajmujące się obrotem tymi walutami nie podlegają zabezpieczeniom bezpieczeństwa transakcji ani monitorowaniu przeciwko praniu brudnych pieniędzy lub finansowania terroryzmu (a jeżeli nawet dobrowolnie stosują pewne zabezpieczenia, to nie ma pewności, w jakim stopniu są one skuteczne). Również pierwsze emisje tokenów (ang. *initial coin offerrings*), choć przypominają pierwsze emisje publiczne spółek giełdowych, to są praktycznie nieuregulowane i nie podlegają kontroli instytucji nadzoru. Instytucje nadzoru mają także obawy przed wykorzystaniem do prania pieniędzy cennych metali[17].

Brytyjska instytucja FCA[18] ostrzega także przed oszustwami na portalach randkowych, gdzie oszuści mogą tworzyć fałszywe profile i usiłować wyłudzać pieniądze, oszustwami emerytalnymi, w których ofiarom proponuje się lepszy plan emerytalny niż mają obecnie, wzrostem (po latach przerwy) kradzieży pieniędzy z bankomatów oraz oszustwami mandatowymi, gdzie oszuści posiadając dane osobowe, tworzą fałszywe obciążenia kont mandatami, które są automatycznie ściągane z kont ofiar. Aby im zapobiegać, organizacja ta proponuje wdrożenie w bankach tzw. protokołu bankowego (ang. *banking protocol*), który upoważnia pracowników banków powiadomić policję, jeżeli nabrali podejrzeń, że osoba wypłaca pieniądze w banku, aby przekazać je oszustowi. Szczególnie jest to istotne w przypadku osób starszych albo po prostu naiwnych[19]. Analizuje się także zastosowanie sztucznej inteligencji

[15] T. Fasoyiro, J. Moller, *Financial crime outlook – key themes for 2019*, https://www.nortonrosefulbright.com/en/knowledge/publications/e28a5b6d/financial-crime-outlook-key-themes-for-2019, 2016 (dostęp: 18.09.2019).

[16] CIFAS, *30 facts about fraud…*, op. cit.

[17] National Crime Agency (Wielka Brytania), *National Strategic Assessment…*, op. cit.

[18] K. Peachey K., *Pension scams victims lost 91 000 GBP each*, https://www.bbc.com/news/business-45170408 (dostęp: 11.09.2019).

[19] CIFAS, *30 facts about fraud…*, op. cit.

do rozpoznawania na portalach randkowych, czatach, portalach społecznościowych oraz w smsach i e-mailach oszustów[20].

Praktycznie wszystkie instytucje są zgodne, że rośnie proceder przesyłania (i prania) pieniędzy za pomocą słupów (smerfów), co utrudnia identyfikację procederu, bo składa się on z wielu małych transakcji. Należy także oczekiwać wzrostu oszustw wewnątrz firm[21], które są szczególnie trudne do wykrycia – ponad 40% wykrytych spraw zostało zidentyfikowanych dzięki temu, że inny pracownik zgłosił nieprawidłowości przełożonym[22]. Podobnego trendu oczekuje się od *insider tradingu*[23], wykorzystywania adwokatów i księgowych do przenoszenia i ukrywania nielegalnych pieniędzy[24] oraz łapówkarstwa i korupcji szczególnie w przypadku dużych, międzynarodowych kontraktów w rentownych branżach (zasoby naturalne, szczególnie gaz i ropa naftowa, ale także projekty budowlane czy związane ze służbą zdrowia)[25].

Co do zapobiegania przestępstwom finansowym z powodu ich internacjonalizacji konieczna będzie współpraca coraz większej liczby krajów, aby prześledzić całą transakcję, określich sprawców i zlokalizować ukradzione aktywa, a służby wszystkich krajów będą nie tylko posiadały cyberpolicję[26], ale także cybsersądy[27] (sądy wyspecjalizowane w cyberprzestępczości). Będzie to wymagało inwestycji w infrastrukturę techniczną i w sztuczną inteligencję, która prawdopodobnie będzie samodzielnie wykonywała preprocesing alarmów i sygnałów[28] (póki co liczba prawdziwych oszustw wśród sygnałów często nie przekracza 10%[29]). Aby poprawić skuteczność systemów nadzoru i alarmów, sztuczna inteligencja będzie coraz lepiej identyfikowała transakcje wykonywane przez oszustów za pomocą kradzionych danych kart kredytowych – będzie w stanie powiązać klienta z typem produktów i usług, z jakich korzysta, i wyłapywać transakcje odbiegające od tego wzorca.

---

[20] Ibid.

[21] STAR, *First Data…*, op. cit.

[22] Ibid.

[23] National Crime Agency (Wielka Brytania), *National Strategic Assessment…*, op. cit.

[24] Ibid.

[25] Ibid.

[26] Lexis Nexis, *Future Financial Crime Risks…*, op. cit.

[27] CIFAS, *30 facts about fraud…*, op. cit.

[28] Lexis Nexis, *Future Financial Crime Risks…*, op. cit.

[29] IBM, *Fighting Financial Crime with AI*, https://www.ibm.com/downloads/cas/WKLQKD3W (dostęp: 20.09.2019).

Wzorce zachowań będą klasyfikowane do różnych grup i lokalizacji, w których klienci ogólnie zmieniają swoje zachowanie, co pozwoli lepiej je przewidywać w nietypowych sytuacjach (np. wyjazd na wakacje), co zmniejszy liczbę fałszywych alarmów[30].

Z uwagi na coraz bardziej zaawansowane technologie kradzieży tożsamości prawdopodobnie w przyszłości klienci będą musieli identyfikować się za pomocą danych biometrycznych. Z tego samego powodu prawdopodobnie klienci będą musieli stworzyć cyfrowe profile i zawsze identyfikować się za ich pomocą w jakimkolwiek kontakcie z instytucją finansową (aktulne zabezpieczenia nie będą wystarczające). Istnieje także ryzyko niezadowolenia klientów z coraz to bardziej skomplikowanych i czasochłonnych sposobów autoryzacji i autentykacji, przez co mogą oni uciekać do instytucji w innych jurysdykcjach, które będą stosowały mniej zabezpieczeń[31]. Jednak nadzór finansowy będzie starał się zmusić wszystkie te instytucje do przyjęcia tych samych regulacji i zasad walki z przestępczością, jakie obowiązują obecnie regularne i licencjonowane instytucje finansowe (np. dotyczy to nieregulowanych platform bankowych (ang. *alternative banking platforms*))[32]. Podobna sytuacja prawdopodobnie będzie miała miejsce w przypadku kasyn wirtualnych i wszystkich innych stron oferujących hazard (ujednolicenie przepisów między krajami i wdrożenie jednolitych procedur bezpieczeństwa)[33].

Wzrost liczby logowań do banków i liczby transakcji wynikających z korzystania z telefonów komórkowych do ich wykonywania oraz zakupów przez internet prawdopodobnie wymuszą aktualizację danych w instytucjach finansowych nie regularnie, co pewien czas, ale wywoływaną określonym zdarzeniem. Aby obniżyć koszty, hurtownie danych instytucji finansowych będą ze sobą powiązane, aby zapytania automatycznie korzystały ze wszystkich dostępnych danych w całym systemie. Może to obniżyć koszty wdrażania nowych systemów, które są i będą szczególnie dotkliwe dla małych instytucji,

[30] V. Chinner, *Artificial Intelligence And The Future Of Financial Fraud Detection*, „Forbes", 4.06.2018, https://www.forbes.com/sites/theyec/2018/06/04/artificial-intelligence-and-the-future-of-financial-fraud-detection/ (dostęp: 1.08.2019).

[31] Lexis Nexis, *Future Financial Crime Risks…*, op. cit.

[32] National Crime Agency (Wielka Brytania), *National Strategic Assessment…*, op. cit.

[33] C. Chambers-Jones, H. Hillman, *Financial Crime and Gambling in a Virtual World: A New Frontier of Cybercrime*, Edward Elgar, Cheltenham, Wielka Brytania 2014.

korzystających w przyszłości z rozwiązań oferowanych przez SupTech oraz RegTech[34].

Coraz popularniejszym narzędziem walki z przestępczością finansową mogą być grafowe bazy danych, ponieważ potrafią łączyć ze sobą wiele różnych punktów danych, czego nie potrafią relacyjne bazy danych[35]. Analiza grafów pozwala zidentyfikować, gdzie znajdują się najsilniejsze połączenia, w jakim są kierunku (np. między osobami), szczególnie między nodami niepowiązanymi ze sobą bezpośrednio (może to być użyteczne przy płatnościach granularnych).

Służby nadzoru finansowego będą także ograniczać tzw. ciemną stronę internetu (ang. *dark web*), która nie jest indeksowana za pomocą przeglądarek i jest tylko dostępna za pomocą sieci ToR (the Onion Router), Freenet, I2S.

Według Instytutu Bezpieczeństwa Komputerowego[36] w najbliższej przyszłości należy spodziewać się wzrostu siedmiu zagrożeń ze strony cyberprzestępczości:

1. Upychanie poświadczeń (ang. *credentials stuffing*), czyli ukradzione wcześniej dane metodą *brute force*, automatycznie są wykorzystywane do prób zalogowania się na kontach użytkowników.
2. Włamania do aplikacji służących do pracy grupowej (ang. *collaboration applications security*).
3. Trojany bankowe.
4. Włamania na urządzenia domowe (ang. *Internet of Things*).
5. Kryptografia kwantowa i próby jej złamania (ang. *quantum cryptography*).
6. *Phising*.
7. Autentykacja wieloczynnikowa i próby jej złamania (ang. *multifactor authentication*).

---

[34] T. Groenfeldt, *Taming the High Costs of Compliance With Tech*, „Forbes", 22.03.2018.

[35] S. Singh, *Using emerging tech to fight financial crime: the future is now*, https://www.corporatecomplianceinsights.com/the-emerging-technologies-key-to-strengthening-compliance-management/ (dostęp: 8.09.2019).

[36] J. Fruhlinger, *7 hot cybersecurity trends*, 11 marca 2019, https://www.csoonline.com/article/3262972/7-hot-cyber-security-trends-and-4-going-cold.html (dostęp: 20.09.2019).

3. Ryzyko podatkowe i metody zapobiegania mu w przyszłości – wyzwania i rekomendacje

Era globalizacji gospodarczej i towarzyszący jej wzrost digitalizacji, zwiększający się udział usług w łącznej wartości dodanej, który obecnie przekracza 70% ogółu działalności gospodarczej, a także bezprecedensowy przepływ informacji powodują fundamentalne i szybkie zmiany w całej gospodarce. Wymaga to od władz fiskalnych nieustannej uwagi zwróconej na nowe formy ucieczki od podatku. Trudności przysparza zastępowanie tradycyjnego przepływu finansowego przez systemy wirtualnych/cyfrowych walut, anonimowe blockchainy lub bankowość w chmurze, a także niezmiennie istniejące tzw. tradycyjne ryzyko determinujące to zjawisko[37]. Walka z nadużyciami podatkowymi wymaga współpracy międzynarodowej. Świadome tego władze fiskalne podejmują więc wspólne wysiłki. Wiedzą i wsparciem dzielą się organizacje międzynarodowe, tj. OECD, Międzyamerykańskie Centrum Administracji Podatkowych (*Inter-American Center of Tax Administration*, dalej CIAT), Wewnątrzeuropejska Organizacja Administracji Podatkowych (*Intra-European Organisation of Tax Administrations*, dalej IOTA) oraz Międzynarodowy Fundusz Walutowy (*International Monetary Fund*, dalej MFW)[38].

Od wielu lat szczególnym punktem zainteresowania władz UE, a także decydentów krajowych są oszustwa popełniane w ramach VAT. Wynika to z ekonomicznego znaczenia luki w tym podatku. Według Europejskiego Trybunału Obrachunkowego (dalej ETO) oszustwa karuzelowe w UE powodują

[37] Skomplikowane przepisy podatkowe, zróżnicowane systemy podatkowe, wysokie stawki podatków, zwolnienia i wydatki podatkowe, niedostatecznie rozpowszechniane informacje na temat wykorzystania zasobów pochodzących z podatków, brak integralności podatkowej obywateli, jurysdykcje o zerowym lub niskim opodatkowaniu, a także system finansowy, który umożliwia mobilizację środków w szybki i prosty sposób, proliferacja systemów podatkowych atrakcyjna dla inwestorów, trudności w kontrolowaniu cen transferowych powiązanych podmiotów.

[38] Wspólnym przedsięwzięciem wymienionych organizacji jest ankieta internetowa *International Survey on Revenue Administration*. Została opracowana w celu poprawy integralności danych i ich porównywalności między administracjami. Ma stanowić skuteczne wsparcie w budowaniu zdolności do wdrażania międzynarodowych standardów podatkowych, *International Survey on Revenue Administration* (ISORA), https://www.imf.org/en/Capacity-Development/Training/ICDTC/Courses/ISORA (dostęp: 4.08.2019).

straty we wpływach podatkowych rzędu 40–60 mld euro rocznie. Około 80% oszustw popełnianych jest przez zaledwie 2% zorganizowanych grup przestępczych. A swoista „inwestycja" w oszustwo związane z handlem emisją CO_2 w wysokości 100 mln euro w ciągu zaledwie kilku godzin pomnożona może być do nawet 600 mln euro[39]. Korzyści finansowe, jakie wynikają z popełnianych oszustw podatkowych, wyjaśniają fenomen tego zjawiska. Nierówna walka władz państwowych z tym procederem wciąż jest toczona. Trudności determinują nie tylko skala i rodzaj działań przestępczych, ale również to, że oszustwa w VAT stały się niemalże elementem na stałe wpisanym w „architekturę" współczesnych gospodarek. Eskalują w swych rozmiarach, obejmując podmioty spoza Unii Europejskiej: Dubaju, Szwajcarii, USA i Chin. Wśród głównych rodzajów transgranicznych oszustw popełnianych w VAT obecnie i w przyszłości wymienia się[40] np. oszustwa typu znikający podatnik (*missing trader fraud*) oraz oszustwa karuzelowe (*carousel fraud*). Ten dobrze znany od lat proceder, w ramach którego wykorzystywano głównie towary o małych rozmiarach i wysokiej wartości, teraz opiera się na towarach o niskiej wartości, których spożycie jest stosunkowo szybkie (np. produkty spożywcze), a także na produktach o charakterze niematerialnym, tj. kredyty węglowe, gaz i energia elektryczna, przetwarzanie w chmurze oraz telefonia internetowa i certyfikaty zielonej energii. Szybki i łatwy transfer tych produktów skutecznie utrudnia śledzenie transakcji. Kolejnym przykładem ryzyka w tym podatku są import oszustw i oszustwa związane z e-handlem powodowane istotnym wzrostem skali importowanych dóbr. Zwolnienia podatkowe, które przysługują pod pewnymi warunkami[41], wykorzystano w przypadku 144 milionów przesyłek (dane z 2015 r.), co stanowi wzrost o 300% w ciągu 15 lat. Kwota VAT, z której państwa członkowskie tym samym dobrowolnie zrezygnowały

[39] M. Lamensch, E. Ceci, *VAT fraud. Economic impact, challenges and policy issues*, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, European Parliament 2018, s. 10.

[40] Tax Administration 2017: Comparative Information on OECD and Other Advanced and Emerging Economies, OECD Publishing 2017, http://dx.doi.org/10.1787/tax_admin-2017-en, s. 58.

[41] Zwolnienie z VAT przysługuje w przypadku importu towarów z terytorium państwa trzeciego (spoza UE), jeżeli łączna wartość przesyłki nie przekracza 22 euro. Art. 51 *ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług* (*Dz.U. 2004 Nr 54 poz. 535 z późn. zm.*), opracowano na podstawie Dz.U. 2018. poz. 2174, 2193, 2215, 2244, 2354, 2392 2433; 2019 poz. 675, 1018.

z powodu zwolnienia, zasadniczo wzrosła. Oszustwa w postaci zaniżania wartości zgłaszanych do opodatkowania towarów stały się zatem powszechnym problemem. Z badania przeprowadzonego w 2016 r. przez *Copenhagen Economics*[42] wynika, że takich przesyłek było 65%. Oszacowane z tego tytułu straty mogą wynosić nawet 5 mld euro rocznie. Komisja Europejska twierdzi, że do 5% przesyłek zostało skontrolowanych. Sądzi się jednak, że straty mogą być znacznie większe. Wśród pozostałych oszustw dotyczących państw UE wymienia się również te, które związane są ze sprzedażą nowych samochodów jako używanych, w ramach których opodatkowana jest jedynie marża. Popełnianie oszustw determinowane jest również zróżnicowaniem stawek VAT, które stosowane są w krajach UE. .To sprzyja powstawaniu nieprawidłowości w zakresie kwalifikowania dostaw, do których stosowane są niezgodnie z prawem obniżone stawki VAT. Innym przykładem stosowanych przez podmioty nieuczciwych praktyk są oszustwa w sektorze leasingu samolotów. Chociaż nie dotyczą wielu podmiotów, to jednak determinują wysokie kwoty niezapłaconego VAT. Odliczenie VAT z tytułu importu towarów możliwe jest w sytuacji wykorzystania zakupionego towaru do celów biznesowych. Obserwuje się, że właściciele samolotów ubiegają się o 100% zwrot VAT, gdy samolot jest częścią firmy leasingowej. W niektórych przypadkach jednak importer wynajmuje samolot od samego siebie, ponieważ VAT należny od umowy leasingu jest niższy niż od VAT z tytułu importu samolotu.

Innym, poważnym wyzwaniem dla władz fiskalnych i struktur europejskich są powszechnie wykorzystywane przez kraje agresywne praktyki podatkowe. Szacuje się, że utracone w skali świata wpływy podatkowe z podatku dochodowego płaconego przez osoby prawne wynoszą 500–600 mld dolarów rocznie[43]. Wykorzystywanie rajów podatkowych do uzyskania korzyści finansowych, choć znane od co najmniej lat 30. XX wi., współcześnie obejmuje 100 państw na świecie. W samej UE aż jedna czwarta z nich wykazuje cechy raju podatkowego. Wśród nich są: Belgia, Cypr, Węgry, Irlandia, Luksemburg,

[42] B. Basalisco, J. Wahl, H. Okholm, *E-Commerce Imports into Europe: VAT and Customs Treatment* 2016, https://www.copenhageneconomics.com/publications/publication/e-commerce-imports-into-europe-vat-and-customs-treatment (dostęp: 8.08.2019).

[43] A. Cobham, P. Janský. *Measuring Misalignment: The Location of US Multinationals' Economic Activity versus the Location of their Profits*, „Development Policy Review", 2017, nr 37 (1), s. 91–110.

Malta i Holandia[44]. Według danych Międzynarodowego Funduszu Walutowego skala fantomowych bezpośrednich inwestycji w Luksemburgu[45] jest większa od ich liczby w Stanach Zjednoczonych i znacznie większa niż w Chinach. Podobnie w przypadku Holandii, która pod względem fantomowych inwestycji bezpośrednich stanowi drugie z kolei europejskie państwo. Jeśli uwzględni się Hongkong, Brytyjskie Wyspy Dziewicze, Bermudy, Singapur, Kajmany, Szwajcarię, Irlandię i Mauritius, to jedynie 10 gospodarek świata obsługuje ponad 85% fantomowych inwestycji.

Stosowane przez kraje strategie niszczą zatem podstawy opodatkowania w innych gospodarkach[46]. W dążeniu do ograniczenia zewnętrznego ryzyka nadużyć podatkowych i nieuczciwej konkurencji podatkowej władze europejskie w 2016 r. opublikowały tzw. czarną listę państw stosujących nieuczciwe praktyki, którą następnie zaktualizowano w 2017 r. W 2018 r. znacząca liczba jurysdykcji wdrożyła konkretne środki i działania (60 państw), a ponad 100 szkodliwych rozwiązań systemowych zostało usuniętych. Na podstawie przeglądu przeprowadzonego przez Komisję Europejską na czarnej liście znajduje się obecnie 15 krajów. Spośród nich 5 nie podjęło żadnych działań mających na celu dostosowanie swoich standardów przejrzystości podatkowej do norm międzynarodowych. Są to: Samoa Amerykańskie, Guam, Samoa, Trynidad i Tobago. Kraje, które jedynie częściowo wprowadziły nowe standardy i nadal znajdują się na liście to: Wyspy Dziewicze Stanów Zjednoczonych, Barbados, Zjednoczone Emiraty Arabskie i Wyspy Marshalla, Aruba, Belize, Bermudy, Fidżi, Oman, Vanuatu i Dominika. Aż 34 państwa, aby uniknąć umieszczenia na czarnej liście w 2020 r., choć zrealizowały wiele inicjatyw na rzecz spełniania międzynarodowych wymogów, to jednak prace powinny zakończyć do końca 2019 r. Wśród nich są: Albania, Anguilla, Antigua i Barbuda, Armenia, Australia, Bahamy, Bośnia i Hercegowina, Botswana, Brytyjskie Wyspy Dziewicze, Cabo Verde, Kostaryka, Curacao, Kajmany, Wyspy Cooka, Eswatini, Jordania, Malediwy, Mauritius, Maroko, Mongolia, Czarnogóra, Namibia,

[44] C. Remeur, *Listing of tax havens by the EU,* European Parliamentary Research Service, PE621.872, 2018, s. 2.

[45] Są to inwestycje realizowane wyłącznie w celu zminimalizowania wysokości podatków przedsiębiorstw działających na międzynarodowych rynkach.

[46] J. Damgaard, T. Elkjaer, N. Johannesen, *The Rise of Phantom Investments*, Finance & Development, International Monetary Fund, 2019, s. 12.

Macedonia Północna, Nauru, Niue, Palau, Saint Kitts i Nevis, Saint Lucia, Serbia, Seszele, Szwajcaria, Tajlandia, Turcja i Wietnam.

W ramach monitorowania działań realizowanych przez poszczególne państwa Komisja Europejska ściśle współpracuje z OECD[47]. Unijne kryteria są zgodne z międzynarodowymi standardami, których państwa członkowskie powinny przestrzegać. Wskazuje się zatem, aby spełniano standardy dotyczące automatycznej wymiany informacji i wymiany informacji na żądanie. W tym celu konieczne jest ratyfikowanie wielostronnej konwencji OECD lub podpisanie umów dwustronnych ze wszystkimi państwami członkowskimi, aby ułatwić wymianę informacji. Następnie kraje zobowiązane są do przestrzegania uczciwej konkurencji podatkowej. W krajach nie mogą obowiązywać szkodliwe systemy podatkowe, które są sprzeczne z zasadami kodeksu postępowania UE lub OECD. Państwa, w których nie jest stosowane opodatkowanie z zakresu podatku dochodowego od osób prawnych lub stosowane są zerowe stawki tego podatku, powinny wprowadzić odpowiednie wymogi dotyczące przejrzystości po to, aby przyjęte zasady opodatkowania nie zachęcały do tworzenia sztucznych struktur. Ostatni z warunków dotyczy wdrożenia minimalnych standardów OECD dotyczących erozji bazy i przenoszenia zysków (*Base Erosion and Profit Shifting* – BEPS). Współcześnie, ponad 130 krajów implementuje 15 inicjatyw mających na celu walkę z unikaniem podatków, poprawę spójności międzynarodowych przepisów podatkowych i zapewnienie przejrzystego otoczenia podatkowego. Obejmują one m.in. wyzwania podatkowe wynikające z cyfryzacji, reguły opodatkowania w zakresie kontrolowanych spółek zagranicznych, neutralizowanie skutków rozbieżności podatkowych wynikających ze stosowania hybrydowych podmiotów lub instrumentów, limitowanie w zakresie ograniczenia odliczeń odsetek czy szkodliwe praktyki podatkowe, ceny transferowe, raportowanie państw.

Można sądzić, że innowacyjne rozwiązania już dziś dostosowane technologicznie do zmieniającego się otoczenia w perspektywie czasu będą sprzyjać realizowaniu skutecznej polityki fiskalnej. Powinny również przyczynić się do poprawy funkcjonowania podmiotów gospodarczych w otoczeniu

[47] *Questions and answers on the EU list of non-cooperative tax jurisdictions,* European Commission – Fact Sheet, 12 March 2019, https://europa.eu/rapid/press-release_MEMO-19-1629_en.htm

prawno-gospodarczym, zmniejszając ciężar obecnych obowiązków związanych z rozliczaniem się z podatków. Wydaje się, że przytoczone rozwiązania wzmocnią pozycję uczciwie działających przedsiębiorców nie tylko w kraju, ale także na arenie międzynarodowej. Podmioty nastawione na popełnianie oszustw zaś skutecznie zniechęcą do podejmowania praktyk niezgodnych z prawem. Implementacja procedur i narzędzi, które niewątpliwie wpływają na wzrost możliwości analitycznych i kontrolnych organów skarbowych nie wystarczą jednak, jeśli pominięty zostanie aspekt systematycznego monitorowania i informowania społeczeństwa o skali zjawiska ucieczki od podatku. To stanowi nie tylko o transparentności prowadzonej polityki, proaktywnym podejściu do nieuczciwości podatników, ale także warunkuje społeczną aprobatę dla podejmowanych inicjatyw.

4. Przyszłość regulacji prawnych regulujących przestępczość finansową i jej zapobieganie

Regulacje prawne nie funkcjonują w próżni, ale należy je wpisywać w szerszy, złożony kontekst interpretacyjny wyznaczający pole powinnej analizy. Spoglądając na rynek finansowy w ujęciu komparatystycznym, dominujący jest obecnie model regulacji według wzorca amerykańskiego. Jak zauważa się w literaturze przedmiotu, jest to system liberalnej ekonomii, stanowiący podwaliny nowych form regulacji. Natomiast przykładem poszukiwania logiki regulacji i jej systematyzacji, czyli powstania prawa regulującego rynek finansowy w sposób absolutny, jest Francja. Niewątpliwie rola badań porównawczych zmierzających do wykazania wpływów i stosowania instrumentów w jednym systemie, pochodzących zaś z innej kultury prawnej pozwala lepiej zrozumieć zarówno praktykę, rolę instytucji nadzoru, jak i granice, jakie podmiot i przedmiot związany z regulacją mogą osiągnąć[48]. Dlatego **kreując nowe rozwiązania na rynku finansowym, warto spoglądać na rozwiązania innych państw i na zasadzie swoistego *benchmarkingu*** podpatrywać możliwe

[48] M. Lemonnier, *Model regulacji*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, 29.06.2019, https://sip.lex.pl/#/monograph/369380982/9 (dostęp: 8.08.2019).

konstrukcje prawne. Wyznaczając kierunek rozwoju regulacji prawnych dotyczących przestępstw na rynku finansowym w Polsce, należy zauważyć, że musi podążać on za rozwiązaniami generowanymi na poziomie Unii Europejskiej. Począwszy od pierwszej dekady XXI w., kiedy została podjęta decyzja o realizacji strategii lizbońskiej (do której włączono tzw. *Financial Services Action Plan*), rynek finansowy stał się przedmiotem szczególnego zainteresowania europejskiego prawodawcy. Widoczna stała się aktywność regulacyjna, która nadal sukcesywnie wzrasta, czego przejawem jest obejmowanie regulacją kolejnych sfer funkcjonowania europejskiego rynku finansowego, stanowiącego jedną z najważniejszych (o ile nie najważniejszą) części rynku wewnętrznego Unii Europejskiej[49]. W sposób oczywisty – poprzez naszą akcesję do Unii Europejskiej – **aktywność europejskiego prawodawcy przekłada się na stosowne działania ustawodawcy krajowego, celem wdrożenia i dostosowania właściwych w tym zakresie regulacji**. Jak zatem w przypadku każdego z państw członkowskich, ramy regulacji europejskich w obszarze rynku finansowego wyznaczają kształt regulacji prawa krajowego, w tym również i w obszarze przeciwdziałania przestępczości na rynkach finansowych. Stąd kształt rozwiązań przyjmowanych na poziomie krajowym i kierunek ich ewolucji jest silnie uwarunkowany działaniami prawodawcy unijnego. Spoglądając na ten obszar, widoczne jest, że najbardziej fundamentalną zmianą w polityce tworzenia ram prawnych funkcjonowania rynku finansowego w celu zapewnienia jego bezpieczeństwa i stabilności jest przyjęta zasada pełnej harmonizacji, która ma doprowadzić do jednolitości regulacji (*Single Rulebook*) we wszystkich państwach członkowskich UE. Dzięki ujednoliceniu prawa na szczeblu unijnym za pomocą dyrektyw maksymalnej harmonizacji i obowiązujących bezpośrednio rozporządzeń dokonuje się przebudowa europejskich ram regulacyjnych funkcjonowania rynku finansowego poprzez wzmocnienie nadzoru nad instytucjami finansowymi, harmonizację przepisów w zakresie adekwatności kapitałowej, podejmowania i prowadzenia działalności przez instytucje finansowe[50].

---

[49] T. Nieborak, *Unia Bankowa- w stronę bezpieczeństwa i stabilności rynku finansowego Unii Europejskiej?*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, 29.06.2019, https://sip.lex.pl/#/monograph/369380982/30 (dostęp: 9.08.2019).

[50] A. Jurkowska-Zeidler, *Jednolita regulacja (Single Rulebook)*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, 29.06.2019, https://sip.lex.pl/#/

Kontekst interpretacyjny dla kierunku, w którym podążają przyjmowane modele regulacji prawnych wyznacza m.in. unia bankowa. Jest to teoretycznie projekt adresowany jedynie do sektora bankowego, ale jego implikacje mają znacznie szerszy wymiar, zwłaszcza jeśli uświadomimy sobie, jak szeroki zakres problematyki rynku finansowego wypełnia właśnie działalność banków. Siłą rzeczy, wskutek powiązań istniejących na rynku finansowym oraz wśród instytucji finansowych, dotyka on także sektory pozabankowe[51]. W ujęciu modelowym unia bankowa składa się z trzech elementów: I. jednolitego zbioru przepisów, II. jednolitego mechanizmu nadzorczego, III. jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji. Nadzór odbywa się w ramach połączonej struktury, którą tworzą – ściśle ze sobą współpracujące, kierujące się jednolitymi wysokimi standardami i wymogami – organ ponadnarodowy (Europejski Bank Centralny) i krajowe organy nadzorcze. Z perspektywy Unii Europejskiej należy zatem zauważyć, że w obszarze funkcjonowania sektora bankowego obserwuje się przesunięcie punktu ciężkości z zasady prymatu nadzoru kraju macierzystego na rzecz scentralizowanego nadzoru jednolitego ze strony Europejskiego Banku Centralnego (co w założeniu zapewniać ma pełniejszy przepływ informacji nadzorczych, sprawniejsze procedury postępowania). Wyraźne ramy wymogów ostrożnościowych i prowadzenia działalności w sektorze finansowym powinny być zatem oparte na silnych systemach nadzoru, czynnościach wyjaśniających i sankcjach. W tym celu **organy nadzorcze powinny zostać wyposażone przez ustawodawcę w wystarczające uprawnienia do działania oraz powinny móc korzystać z systemów równych, nieuchronnych i odstraszających sankcji za wszelkie przewinienia finansowe, przy czym sankcje te powinny być skutecznie egzekwowane**[52]. Zastanawiając się nad możliwymi i koniecznymi ścieżkami rozwoju uregulowań dotyczących problematyki przestępczości na rynku finansowym, konieczne jest zatem m.in. **dalsze doskonalenie i wzmacnianie regulacji dotyczących nadzoru poprzez ulepszanie stosownych procedur i narzędzi, jakie mają właściwe organy, a także tworzenie adekwatnej archi-**

monograph/369380982/26 (dostęp: 8.08.2019

[51] J. Monkiewicz, *Uwagi końcowe*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, 29.06.2019,https://sip.lex.pl/#/monograph/369380982/22 (dostęp: 8.08.2019).

[52] Preambuła MAR.

tektury organów nadzoru, w ramach której dochodzi do rozlokowania ich kompetencji. Na gruncie krajowym szczególna rola w obszarze nadzoru nad rynkiem finansowym przypada Komisji Nadzoru Finansowego, do której ustawowych zadań należy m.in.: sprawowanie nadzoru nad rynkiem finansowym (określonym w art. 1 ust. 2 u.n.r.f.), podejmowanie działań służących prawidłowemu funkcjonowaniu tego rynku, podejmowanie działań mających na celu rozwój rynku finansowego i jego konkurencyjności, przedsiębranie działań nakierowanych na wspieranie rozwoju jego innowacyjności, jak i podejmowanie działań edukacyjnych oraz informacyjnych w zakresie funkcjonowania rynku finansowego, jego zagrożeń oraz podmiotów na nim funkcjonujących w celu ochrony uzasadnionych interesów uczestników rynku finansowego. Celem nadzoru jest zapewnienie: prawidłowego funkcjonowania rynku finansowego, jego stabilności, bezpieczeństwa oraz przejrzystości i zaufania do niego, a także ochrony interesów uczestników tego rynku również poprzez rzetelną informację dotyczącą jego funkcjonowania, przez realizację celów określonych w szczególności w: u.p.b., ustawie o nadzorze ubezpieczeniowym i emerytalnym[53], ustawie o nadzorze uzupełniającym nad instytucjami kredytowymi, zakładami ubezpieczeń, zakładami reasekuracji i firmami inwestycyjnymi wchodzącymi w skład konglomeratu finansowego[54], u.n.r.k., u.s.k.o.k. oraz u.u.p.

W obszarze regulacji prawnych dotyczących rynku finansowego istotne jest, aby były one swoistą **odpowiedzią na dynamiczny charakter i rozwój rynków finansowych**, stąd również **przystosowane do zachodzących przeobrażeń tak technicznych, jak i w wymiarze gospodarczym**. Skoro przestępstwa będą popełniane zawsze – kwestią realną pozostają działania mające na celu maksymalne ograniczanie ich rozmiaru, co stanowi niewątpliwy obowiązek statuowany po stronie władz publicznych (w obszarze stanowienia prawa, ale i jego stosowania, egzekwowania). Chodzi o to, **aby organizacja rynku finansowego była skonstruowana w sposób zapewniający jak najszersze bezpieczeństwo uczestnikom tegoż rynku**. Wymaga to

[53] *Ustawa z dnia 22 maja 2003 r. o nadzorze ubezpieczeniowym i emerytalnym (tekst jedn.: Dz.U. 2019 poz. 207).*

[54] *Ustawa z dnia 15 kwietnia 2005 r. o nadzorze uzupełniającym nad instytucjami kredytowymi, zakładami ubezpieczeń, zakładami reasekuracji i firmami inwestycyjnymi wchodzącymi w skład konglomeratu finansowego (tekst jedn. Dz.U. 2016 poz. 1252 z późn. zm.).*

stworzenia infrastruktury instytucjonalnej świadczenia usług finansowych przez podmioty dopuszczone do tego rodzaju działalności. W konsekwencji w ramach organizacji rynku finansowego*:*

1. określa się podmioty uprawnione do wykonywania usług finansowych;
2. wskazuje się na warunki podejmowania i wykonywania przez nie działalności;
3. dopuszcza się w formie zezwolenia do prowadzenia tej działalności lub zabrania się jej wykonywania[55].

Dlatego – zastanawiając się nad kierunkiem rozwoju regulacji prawnych w analizowanym zakresie – należy mieć pełną świadomość, że nawet najbardziej wyszukane i doskonałe przepisy nie będą wystarczające bez wsparcia w obszarze podnoszenia świadomości społecznej. Konieczne jest zatem **zintensyfikowanie działań o charakterze edukacyjnym w obszarze możliwych przestępstw na rynku finansowym**. Należy uznać, iż mają one **istotne znaczenie dla redukowania podatności wiktymologicznej potencjalnych ofiar**. Mamy w tym zakresie oparcie w stosownym ustawodawstwie, sięgając do wyliczonych w art. 4 ust. 1 pkt 4 u.n.r.f. kompetencji KNF (podejmowanie działań edukacyjnych i informacyjnych w zakresie funkcjonowania rynku finansowego, jego zagrożeń oraz podmiotów na nim funkcjonujących w celu ochrony uzasadnionych interesów uczestników). Powinno się to przekładać na dalsze, jakże konieczne, podnoszenie świadomości prawnej społeczeństwa w obszarze istniejących zagrożeń, jak i istniejących regulacji prawnych. Są to zagadnienia na tyle istotne, że powinny znaleźć swoje odzwierciedlenie już chociażby na poziomie scenariuszy lekcji wychowawczych w szkole podstawowej[56], gdyż należy mieć świadomość, że już w tym wieku dzieci zaczynają mieć zakładane konta w banku i wchodzić w świat analizowanej problematyki. Należy się zatem zgodzić ze stwierdzeniem, że **podnoszenie świadomości społecznej z zakresu ekonomii, ale również prawa** (karnego,

[55] C. Kosikowski, *Nowe prawo rynku finansowego Unii Europejskiej*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, 29.06.2019, https://sip.lex.pl/#/monograph/369380982/5 (dostęp: 7.08.2019).

[56] Należy podkreślić stosowne działania, jakie w tym zakresie podejmuje KNF; zob. np.: J. Banach, A. Jarmuszyńska, M. Zdrojewski, *Pierwsze kroki na rynku finansowym. Scenariusze lekcji*, KNF Warszawa 2019; P. Stangenberg, *Scenariusze lekcji z zakresu ryzyka związanego z inwestowaniem na rynkach kapitałowych i terminowych. Materiały edukacyjne dla środowiska szkolnego*, KNF, Warszawa 2019.

administracyjnego, finansowego) może i powinno być skuteczną **formą przeciwdziałania szeroko pojętej przestępczości finansowej**[57]. Z całą pewnością są to zagadnienia, które nie mogą być marginalizowane. Wykazują one także ścisłą korelację z **cyberprzestępczością na rynku finansowym**. Stale postępujący rozwój techniki, który ma sprzyjać poszerzaniu komfortu osób korzystających z usług finansowych, przekłada się jednocześnie na wzrost skali zagrożeń i ryzyk związanych z cyberprzestępczością, szczególnie w obszarze bankowości elektronicznej (pojęcie mające rozległy zakres zastosowania, obejmuje szerokie spektrum elektronicznych form kontaktu, wśród których można wyodrębnić bankowość internetową, *home-banking*, telefoniczną, samoobsługową oraz inne kanały dostępu do konta, np. poprzez telewizję). Przestępstwa związane z bankowością elektroniczną realizują przede wszystkim znamiona ustawowe ogólnych typów czynów zabronionych określonych w k.k., w szczególności w rozdziale XXXIII *Przestępstwa przeciwko ochronie informacji*. Zachowanie sprawcy może także wypełniać ustawowe znamiona innych czynów zabronionych, stypizowanych w przepisach zawartych m.in. w rozdziale XXIII k.k. *Przestępstwa przeciwko wolności*, np. w art. 190a § 2 k.k., czy też w rozdziale XXXV k.k. *Przestępstwa przeciwko mieniu*, np. w art. 287 k.k. (oszustwo komputerowe). Należy zauważyć, że katalog czynów zabronionych popełnianych w bankowości elektronicznej nie ogranicza się do przestępstw kodeksowych, odpowiedzialność karna bowiem może wynikać również z ustaw szczególnych, np. jeżeli w związku z elektronicznym przetwarzaniem danych w obrocie bankowym dojdzie do naruszenia ustawowo chronionej tajemnicy, np. tajemnicy bankowej[58] (patrz omówiony już w części pierwszej niniejszego opracowania art. 171 ust. 5 u.p.b. przewidujący odpowiedzialność karną za nieuprawnione ujawnienie lub wykorzystanie informacji stanowiących tajemnicę bankową). Z uwagi na znaczną rozpiętość form działania przestępczego w obszarze wykorzystującym nowoczesne technologie należy stwierdzić, że wraz z rozwojem nowo-

[57] W. Pływaczewski, *Od redaktora*, w: W. Pływaczewski (red.), *Przeciwdziałanie patologiom na rynkach finansowych. Od edukacji ekonomicznej po prawnokarne środki oddziaływania*, Warszawa 2015, s. 14

[58] M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, KNF, Warszawa 2014, s. 28–32.

czesnych technologii pojawiają się i nowe zagrożenia, których skala będzie narastała, chociażby ze względu na dalszy dynamiczny rozwój internetu i związany z tym powszechny dostęp zapewniający anonimowość osobom działającym w sieci, w tym również przestępcom[59]. Nie ulega wątpliwości, że zwłaszcza tutaj nie pomogą nawet najbardziej wyszukane regulacje prawne bez wystarczającego stopnia społecznej świadomości co do ochrony przed szkodliwym oprogramowaniem czy ochroną przed phishingiem[60]. **Szczególnie istotna**, wyznaczona ustawowym obszarem kompetencji, jest tutaj **rola KNF**. Przejawia się ona zarówno poprzez **dedykowane kampanie społeczne**, np.: „Zadbaj o swoje bezpieczeństwo w sieci", ale również nakierowane na niniejszą problematykę rekomendacje i wytyczne. Identyfikując ryzyka w niniejszym obszarze, należy mieć pełną świadomość nieustającego zagrożenia ze strony *malware* (rozumiane szeroko jako szkodliwe oprogramowanie). Narasta również korzystanie przez przestępców z mechanizmów właściwych socjotechnice, co oznacza konieczność stałego szkolenia pracowników instytucji finansowych celem podnoszenia ich kompetencji w tym obszarze (patrz szerzej rozważania zawarte w dalszej części dotyczące kontroli wewnętrznej i zarządzania w ramach przedsiębiorstw). Słusznie zauważa się, że katalog działań przestępców stale się poszerza, stąd należy nakierować się np. na nowoczesne techniki autoryzacji, takie jak biometria (odcisk palca, tęczówka oka, naczynia krwionośne palca, rozpoznawanie twarzy, geometria dłoni, głos, podpis odręczny) czy biometryka behawioralna (Project Abacus – sztuczna inteligencja jest w stanie zidentyfikować zestaw kluczowych czynników autoryzujących każdego z nas: sposób korzystania z telefonu połączony z metodą mówienia, pisania, chodzenia, z lokalizacją użytkownika, co łącznie przekłada się na unikalną wartość)[61]. Jednocześnie wprowadzanie odpowiednich roz-

[59] Ibid., s. 33.

[60] *Phishing* to jedno z najpoważniejszych zagrożeń dla klientów internetowych usług sektora finansowego. Jest to przestępcza metoda oszustwa, dystrybuowana z wykorzystaniem poczty elektronicznej, gdzie klient jest wprowadzany w błąd poprzez fałszywą informację sugerującą, że pochodzi ona od instytucji finansowej, poprzez co klient logując się na taka fałszywą stronę, przekazuje przestępcom swoje dane do logowania. Szerzej: R. Balkowski, *Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady*, KNF, Warszawa 2018, s. 34; R.W. Kaszubski, Ł. Obzejta, *Przestępstwa na kartach płatniczych*, w: *Karty płatnicze w Polsce*, Warszawa 2012, s. 377–422.

[61] R. Balkowski, *Bezpieczeństwo systemów teleinformatycznych…*, op. cit., s. 38–40.

wiązań technicznych oznacza konieczność stosownych reakcji na poziomie normatywnym, gdyż muszą mieć one przecież swoje umocowanie w postaci odpowiednich podstaw prawnych.

Formułując uwagi na przyszłość, należy podkreślić **konieczność intensyfikowania współpracy służb i instytucji z sektorem prywatnym**, która może być prowadzona nie tylko w obszarze przeciwdziałania przestępczości, lecz również wspomagać jej zwalczanie. Niezwykle istotna jest możliwość pozyskiwania przez organy ścigania informacji pozostających w posiadaniu lub możliwych do uzyskania przez organizacje przedstawicielskie reprezentujące przedsiębiorców (zobacz uwagi na temat *whistelblowing* w rozdziale: Transforming People and Organizations). Prowadzenie tego rodzaju współpracy może polegać również na tworzeniu baz danych, rejestrów przez poszczególne podmioty i wyposażaniu organów ścigania w dostęp do nich (zgodny z zasadami ochrony danych osobowych i innych niezbędnych procedur w tym zakresie). Sektor prywatny może być partnerem dla organów ścigania w zakresie wykorzystania specjalistycznej wiedzy i prowadzenia wspólnych programów szkoleniowych, wypracowywania skutecznych instrumentów przeciwdziałania nieprawidłowościom, a także określania metod działania wykorzystywanych przez sprawców przestępstw czy monitorowania trendów przestępczości. Dlatego tak istotne jest tworzenie różnego rodzaju platform współpracy[62].

W obszarze poruszanej problematyki szczególną uwagę należy skupić na założeniach „Programu przeciwdziałania i zwalczania przestępczości gospodarczej na lata 2015–2020". Przeciwdziałanie i zwalczanie przestępczości na rynkach finansowych (przynależnych do obszaru przestępczości gospodarczej) ze względu na wielość obszarów jej występowania, skalę zagrożenia, wysokość powodowanych strat, a także często międzynarodowy charakter stanowi jedno z największych wyzwań dla służb, organów i instytucji realizujących działania w odniesieniu do różnych form przestępczej działalności. Zadanie to wymaga realizacji celów, takich jak:

[62] 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. z 2015 r. poz. 1069), s. 29.

1. **Usprawnienie systemu przeciwdziałania i zwalczania przestępczości finansowej** (w tym zwiększenie skuteczności działań koordynacyjnych). Poszczególne służby, organy i instytucje tworzą własne bazy danych/ewidencje/rejestry służące realizacji ich zadań ustawowych, dlatego istotne jest wzmacnianie współpracy i wymiany informacji pomiędzy nimi. Konieczne jest międzyinstytucjonalne podejście (prowadzenie np. wspólnych szkoleń umożliwiających wymianę doświadczeń, z udziałem sędziów, prokuratorów, przedstawicieli służb i instytucji zaangażowanych w realizację zadań w tym zakresie oraz ekspertów zewnętrznych). Sięgając chociażby do wielokrotnie już przywoływanego MAR: ponieważ nadużycia na rynku finansowym mogą mieć miejsce w różnych krajach i na różnych rynkach, od właściwych organów należy we wszystkich okolicznościach, oprócz wyjątkowych sytuacji, wymagać współpracy i wymiany informacji z innymi właściwymi organami i organami regulacyjnymi[63].
2. **Zwiększenie skuteczności instrumentów przeciwdziałania i zwalczania przestępczości finansowej w odniesieniu do poszczególnych obszarów jej występowania.**
3. **Zwiększenie wykorzystania pozaoperacyjnych metod** przeciwdziałania i zwalczania tej formy przestępczości.
4. **Rozwój współpracy międzynarodowej i wdrażanie międzynarodowych standardów.**
5. *Last but not least*: **podniesienie skuteczności systemu pozbawiania sprawców korzyści z nielegalnego procederu** w zakresie zabezpieczania, ewidencjonowania, zarządzania i ostatecznie odzyskiwania mienia pochodzącego z przestępstw. Skoro podstawowym motywem popełniania większości przestępstw jest korzyść majątkowa, odbieranie jej jest niezwykle dotkliwą dla przestępców metodą zwalczania tejże przestępczości. Oczywiście praktyczna realizacja tego zadania wymaga przetwarzania posiadanych informacji, identyfikowania korzyści majątkowych; co uwarunkowane jest sprawnością systemu współdziałania i wymiany informacji pomiędzy podmiotami zaangażowanymi w proces odzyskiwania mienia oraz od efektywności prowadzenia śledztw

[63] Preambuła MAR.

finansowych, rozumianych jako zbieranie, kontrolowanie, kompletowanie, przetwarzanie i analizowanie danych finansowych na rzecz egzekwowania prawa. Działania te wymagają wyposażenia właściwych organów ścigania w uprawnienia do dostępu do informacji prawnie chronionych, w zakresie niezbędnym do wykonywania zadań mających na celu zwalczanie przestępczości, w tym podczas wykonywania czynności operacyjnorozpoznawczych[64]. Szczególne znaczenie ma tutaj art. 145k ustawy o policji[65], zgodnie z którym Komenda Główna Policji wykonuje zadania krajowego biura do spraw odzyskiwania mienia, o którym mowa w art. 1 ust. 1 decyzji Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotyczącej współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem (Dz. Urz. UE L 332 z 18.12.2007, str. 103). Współpraca ta odbywa się na zasadach i warunkach określonych w ustawie z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej[66].

Dodatkowo należy przywołać wytyczne ze Strategii Bezpieczeństwa Wewnętrznego Unii Europejskiej na lata 2015–2020, zgodnie z którymi **należy skonsolidować istniejące narzędzia ustawodawcze, a wszystkie państwa członkowskie powinny sprawniej stosować, a także spójnie, konsekwentnie, skutecznie i w pełni wdrażać obowiązujące instrumenty**. W stosownych przypadkach należy również **opracować nowe narzędzia, w tym informatyczne** na podstawie szczegółowej oceny potrzeby i wartości dodanej takich narzędzi, po to by wzmocnić dziedzinę bezpieczeństwa wewnętrznego Unii Europejskiej. Oznacza to, iż należy **zacieśnić współpracę i szerzej dzielić się sprawdzonymi rozwiązaniami z kluczowymi państwami trzecimi i podmiotami partnerskimi w zakresie aspektów bezpieczeństwa będących**

[64] Opracowano na podstawie elementów warunkujących skuteczność systemu przeciwdziałania i zwalczania przestępczości gospodarczej. *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. z 2015 r. poz. 1069)*, s. 35–36.

[65] *Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn.: Dz.U. 2019 poz. 161 z późn. zm.).*

[66] *Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (tekst jedn.: Dz.U. 2018 r. poz. 484 z późn. zm.).*

przedmiotem wspólnego zainteresowania, w szczególności w dziedzinie współpracy operacyjnej i wymiarów sprawiedliwości w sprawach karnych. Należy również usprawnić **wymianę i zwiększyć dostępność informacji, zwłaszcza poprzez zapewnienie interoperacyjności poszczególnych systemów informacyjnych** i wspieranie najtrafniejszego wyboru stosownego kanału wymiany informacji w ramach obowiązujących przepisów. Należy również **wzmocnić współpracę operacyjną, skuteczniej zapobiegać czynom przestępczym i prowadzić dochodzenia w ich sprawie, ze szczególnym naciskiem na zorganizowaną przestępczość finansową i konfiskatę mienia pochodzącego z działalności przestępczej**. Ponadto należy zwiększać **możliwości w zakresie szkolenia, finansowania, badań i innowacji**, zwłaszcza poprzez dalszy rozwój niezależnej polityki bezpieczeństwa przemysłowego, m.in. w takich dziedzinach jak kontrola graniczna, interoperacyjność sprzętu wykorzystywanego do ochrony oraz organy ścigania, rozwijać i propagować dostępność i wykorzystywanie solidnych i bezpiecznych technologii informacyjno-komunikacyjnych w celu zwiększenia bezpieczeństwa cybernetycznego Unii Europejskiej[67].

5. Przyszłe metody ilościowe stosowane w wykrywaniu przestępstw finansowych

Metody ilościowe, które w przyszłości mogą być stosowane szerzej niż obecnie (z uwagi na ich użyteczność i elastyczność), to nowe kształty neuronów, samoorganizujące się mapy i algorytmy genetyczne.

Sieci neuronowe posiadają strukturę, na którą składają się neurony połączone synapsami. Kształt i zachowanie neuronu można dowolnie modyfikować, a badania idą w kierunku uzyskania pewnej porównywalności z neuronami mózgu człowieka. Dlatego oprócz reakcji synaps modelowane są dodatkowe reakcje tkanki otaczającej neuron, a także dodatkowe czynniki wpływające na siłę reakcji neuronu, np. poprzedni stan aktywacji.

[67] Projekt konkluzji Rady w sprawie odnowionej strategii bezpieczeństwa wewnętrznego Unii Europejskiej na lata 2015–2020, Bruksela 10 czerwca 2015, (9798/15).

Samoorganizujące się mapy to sieci neuronów, z którymi kojarzy się współrzędne w n-wymiarowej przestrzeni danych. Uczenie tego rodzaju sieci polega na zmianie konfiguracji współrzędnych neuronów tak, aby dążyły one do rezultatu zgodnego ze strukturą danych wejściowych i wyników. Sieci rozpinają się wokół zbiorów danych, dopasowując do nich swoją strukturę.

Algorytmy genetyczne wywodzą się wprost z genetyki i teorii sekwencjonowania genomu oraz fenotypów. Osobniki, a więc np. poszczególne transakcje finansowe, są kodowane w postaci chromosomów i określone są jako punkty w przestrzeni poszukiwań. Populacja jest zbiorem osobników o określonej liczebności. Chromosomy, czyli łańcuchy, stanowią uporządkowane ciągi genów, np. uporządkowane chronologicznie ciągi obserwacji transakcji giełdowych od poszczególnych maklerów. Długość chromosomów uzależniona jest od warunków zadania, np. od liczby zleceń wykonanych w imieniu klientów w danym dniu. Gen, czyli pojedynczy element genotypu, a w szczególności chromosomu, może być nazywany cechą lub detektorem. Fenotyp jest zestawem wartości odpowiadających danemu genotypowi. Allel to wartość danej cechy. Locus wskazuje miejsce położenia danej wartości w łańcuchu. W algorytmie genetycznym na początku odbywa się losowy wybór transakcji (chromosomów) do początkowej próby. Chromosomy są reprezentowane przez binarne ciągi danych o określonej długości. Następnie ocenia się przystosowanie osobnika w populacji na podstawie funkcji dostosowania. Jeśli spełniony jest warunek zatrzymania, to następuje zapamiętanie najlepszego chromosomu (transakcji). Jeśli nie, następuje selekcja osobników (ciągów transakcji) zgodnie z mechanizmem przeżycia. Osobnik o najwyższym stopniu przystosowania pomnoży swój materiał genetyczny. Natomiast osobniki o najniższym stopniu przystosowania powinny być wyeliminowane z procesu prokreacji. W kolejnym etapie stosuje się operacje genetyczne krzyżowania i mutacji. Krzyżowanie polega na wymianie fragmentu genotypu pomiędzy dwoma osobnikami. Proces ten odbywa się z założonym wcześniej prawdopodobieństwem. Mutacja polega na zmianie wartości pojedynczego genu na przeciwny z ustalonym prawdopodobieństwem. Osobniki (chromosomy) otrzymane w wyniku działania operatorów genetycznych wchodzą w skład nowej populacji, która automatycznie staje się populacją bieżącą dla danej iteracji. Dla każdej następnej iteracji oblicza się wartość funkcji przystosowania i sprawdza się warunek zatrzymania.

Jeśli warunek zatrzymania nie jest spełniony, dalej przechodzi się do selekcji i kolejnych etapów algorytmu. Jeśli warunek jest spełniony, wyprowadza się wynik w postaci chromosomu o największej wartości funkcji przystosowania lub inaczej funkcji celu. W klasycznej optymalizacji parametrów modelu jej odpowiednikiem jest logarytm funkcji wiarygodności.

Bibliografia

Balkowski R., *Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady*, KNF, Warszawa 2018.

Banach J., Jarmuszyńska A., Zdrojewski M., *Pierwsze kroki na rynku finansowym. Scenariusze lekcji*, KNF, Warszawa 2019.

Basalisco B., Wahl J., Okholm H., *E-Commerce Imports into Europe: VAT and Customs Treatment*, https://www.copenhageneconomics.com/publications/publication/e-commerce-imports-into-europe-vat-and-customs-treatment 2016

Chambers-Jones C., Hillman H., *Financial Crime and Gambling in a Virtual World: A New Frontier of Cybercrime*, Edward Elgar, Cheltenham, Wielka Brytania 2014.

Chinner V., *Artificial Intelligence And The Future Of Financial Fraud Detection*, „Forbes", 4.06.2018, https://www.forbes.com/sites/theyec/2018/06/04/artificial-intelligence-and-the-future-of-financial-fraud-detection/ (dostęp: 1.08.2019).

CIFAS, *30 facts about fraud: past, present and future*, https://www.cifas.org.uk/insight/30-facts-about-fraud-past-present-future (dostęp: 10.09.2019).

Cobham A., Janský P., *Measuring Misalignment: The Location of US Multinationals' Economic Activity versus the Location of their Profits*, "Development Policy Review" 2017, nr 37 (1), s. 91–110.

Damgaard J., Elkjaer T., Johannesen N., *The Rise of Phantom Investments*, Finance & Development, International Monetary Fund 2019.

Fasoyiro T., Moller J., *Financial crime outlook – key themes for 2019*, https://www.nortonrosefulbright.com/en/knowledge/publications/e28a5b6d/financial-crime-outlook-key-themes-for-2019, 2016 (dostęp: 18.09.2019).

Fruhlinger J., *7 hot cybersecurity trends*, 11 marzec 2019, https://www.csoonline.com/article/3262972/7-hot-cyber-security-trends-and-4-going-cold.html (dostęp: 20.09.2019).

Górnisiewicz M., Obczyński R., Pstruś M., *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, KNF, Warszawa 2014.

Groenfeldt T., *Taming the High Costs of Compliance With Tech*, "Forbes", 22.03.2018, https://www.forbes.com/sites/tomgroenfeldt/2018/03/22/taming-the-high-costs-of-compliance-with-tech (dostęp: 1.09.2019).

IBM, *Fighting Financial Crime with AI*, https://www.ibm.com/downloads/cas/WKLQKD3W (dostęp: 20.09.2019).

International Survey on Revenue Administration (ISORA), https://www.imf.org/en/Capacity-Development/Training/ICDTC/Courses/ISORA (dostęp: 4.08.2019)

Jurkowska-Zeidler A., *Jednolita regulacja (Single Rulebook)*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*,Wolters Kluwer, https://sip.lex.pl/#/monograph/369380982/26

Kaszubski R. W., Obzejta Ł., *Przestępstwa na kartach płatniczych*, w: *Karty płatnicze w Polsce*, Warszawa 2012. S. 377–424.

Kosikowski C., *Nowe prawo rynku finansowego Unii Europejskiej*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, https://sip.lex.pl/#/monograph/369380982/5

Lamensch M., Ceci E., *VAT fraud. Economic impact, challenges and policy issues*, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, European Parliament 2018.

Lemonnier M., *Model regulacji*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, https://sip.lex.pl/#/monograph/369380982/9

Lexis Nexis, *Future Financial Crime Risks*, listopad 2015, https://www.bba.org.uk/wp-content/uploads/2015/12/Future-Financial-Crime-Risks-DIGITAL-final.pdf (dostęp: 10.09.2019).

Monkiewicz J., *Uwagi końcowe*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, https://sip.lex.pl/#/monograph/369380982/22

National Crime Agency (Wielka Brytania), *National Strategic Assessment of serious and organized crime 2019*, https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file (dostęp: 20.09.2019).

Nieborak T., *Unia Bankowa – w stronę bezpieczeństwa i stabilności rynku finansowego Unii Europejskiej?*, w: *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, https://sip.lex.pl/#/monograph/369380982/30

Peachey K., *Pension scams victims lost 91 000 GBP each*, https://www.bbc.com/news/business-45170408 (dostęp: 11.09.2019).

Pływaczewski W., *Od redaktora*, w: W. Pływaczewski (red.), *Przeciwdziałanie patologiom na rynkach finansowych. Od edukacji ekonomicznej po prawnokarne środki oddziaływania*, Warszawa 2015, s. 19–36.

Questions and answers on the EU list of non-cooperative tax jurisdictions, European Commission – Fact Sheet, 12 March 2019, https://europa.eu/rapid/press-release_MEMO-19-1629_en.htm

Remeur C., *Listing of tax havens by the EU,* European Parliamentary Research Service, PE621.872, 2018.

Singh S., *Using emerging tech to fight financial crime: the future is now*, https://www.corporatecomplianceinsights.com/the-emerging-technologies-key-to-strengthening-compliance-management/ (dostęp: 8.09.2019).

Stangenberg P., *Scenariusze lekcji z zakresu ryzyka związanego z inwestowaniem na rynkach kapitałowych i terminowych. Materiały edukacyjne dla środowiska szkolnego*, KNF, Warszawa 2019.

STAR-First Data, *The Future of Fraud*, https://www.firstdata.com/downloads/pdf/STARFraudeBookFINAL.pdf (dostęp: 15.09.2019).

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

Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług, o podatku od towarów i usług (Dz.U. 2004 Nr 54 poz. 535 z późn. zm.).

ROZDZIAŁ III

Panel: Możliwe przyczyny i rodzaje przestępczości w przyszłości oraz przygotowania prewencyjne w obszarze energetyki

Samochody osobowe – rozwój rynku i wynikające stąd zagrożenia interesu skarbu państwa związane z przestępczością w obszarze obrotu paliwami ciekłymi

PIOTR KWIATKIEWICZ[1]

1. Wprowadzenie

Problematyka opracowania została skoncentrowana na kwestiach związanych z charakterystyką motoryzacji w Polsce w segmencie aut osobowych i jej odzwierciedleniem w popycie na paliwa węglowodorowe, a także energię elektryczną. Badanym aspektem są potencjalne kierunki zmian wynikające z ewolucji rynku samochodowego oraz dające o sobie znać tendencje rozwojowe (np. ekspozycja elementów ekologicznych, elektromobilność itp.). Identyfikacja ich stanowi podstawę do określenia potencjalnego obszaru działań przestępczych związanych z obrotem paliwami ciekłymi. Punktem wyjścia dla poszukiwań stała się charakterystyka struktury zarejestrowanych pojazdów w Polsce w połowie 2019 r., włączywszy w to import aut nowych i używanych, natomiast odniesienia – obowiązujące oraz wprowadzane regulacje prawne, a także sytuacja panująca w ościennych państwach unijnych. Szczególne znaczenie ze względu na istniejący potencjał gospodarczy przypisano tu Republice Federalnej Niemiec (dalej RFN), która uchodzi też za potentata branży i prekursora zachodzących w niej zmian. Przyjęte założenia nie pozostały bez wpływu na dobór perspektywy metodologicznej oraz narzędzi badawczych. Wśród nich istotne miejsce należy przypisać analizie

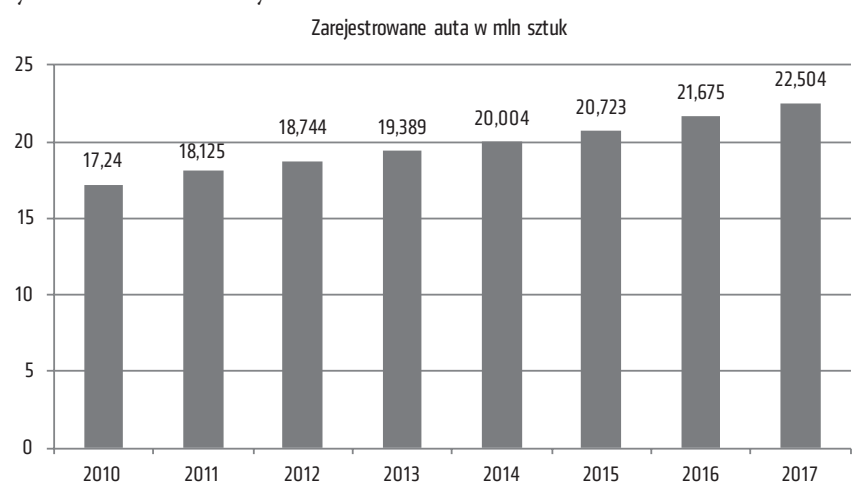
[1] Doktor habilitowany, inżynier, profesor Uniwersytetu Zielonogórskiego, kierownik Pracowni Polityki Energetycznej i Bezpieczeństwa. Zajmuje się szeroko pojętym bezpieczeństwem energetycznym z szczególnym uwzględnieniem logistyki paliwowej. W kręgu zainteresowań naukowych znajdują się tez relacje między rynkami paliwowymi a sytuacją polityczną w państwach producenckich sekotora oil&gas.

instytucjonalno-prawnej oraz zestawieniom statystycznym. Interdyscyplinarny wymiar dociekań pozwolił na stosowanie rozwiązań komparatystycznych właściwych dla wskazanego obszaru poszukiwań.

2. Stan obecny

W Polsce na początku 2018 r. zarejestrowane były 23 mln pojazdów samochodowych[2]. Dynamika tempa wzrostu nieznacznie zmieniła się od początku dekady. Największa różnica r./r. wyniosła 337 tys. Odnotowano ją między 2013/2014, kiedy przybyło 615 tys. pojazdów, a 2015/16 – 952 tys. nowych rejestracji. Odpowiada to średniej rocznej na poziomie oscylującym wokół 750 tys. aut. Oznacza to zwiększenie od początku dekady liczby samochodów osobowych o ponad 5 mln, a przy utrzymaniu dotychczasowego trendu – o ponad 7 mln aut do końca 2019 r. Można przyjąć założenie, zgodnie z którym rynek definiowany liczbą egzemplarzy w segmencie samochodów osobowych powiększa się od 2015 r. w tempie 3,8% r./r.

Rysunek 1. Wzrost liczby samochodów w Polsce od 2010 r.



Źródło: opracowanie własne

[2] 22 504 000 stan na 31.12.2017 r. – dane Polski Związek Przemysłu Motoryzacyjnego, https://www.pzpm.org.pl/pl/content/download/2591/10569/file/park%20pojazdow%20PL%201990_2017.pdf (dostęp: 23.07.2019).

Zmiana ma charakter tak ilościowy, jak i jakościowy. Ten ostatni dotyczy wieku oraz standardu aut. Istotnym elementem omawianych przeobrażań jest wymiana modeli na pojazdy nowszych generacji.

W 2010 r. w Polsce wyrejestrowywano niewiele ponad 220 tys. samochodów. W okresie kolejnych pięciu lat liczba ta podwoiła się[3]. Nie ma żadnych okoliczności, które wskazywałyby na możliwość odwrócenia tego trendu. Według szacunków bardzo pokaźna liczba pojazdów, które od lat nie jeżdżą po drogach, znajduje się w Centralnej Ewidencji Pojazdów i Kierowców (dalej – CEPiK – przypadek P.K.). Są to zwykle auta rodzimej produkcji z czasów PRL oraz te powstałe w „bratnich" państwach socjalistycznych. Przeważają „małe" i „duże" Fiaty, a dalej: Polonezy, Syreny, Wartburgi, Trabanty etc. Łączna ich liczba przekracza 6 mln sztuk[4]. Z dużą dozą prawdopodobieństwa duża ich część fizycznie już nie istnieje, a zachowane egzemplarze są w stanie nierokującym powrotu do ruchu ulicznego. Sytuacja ta nie pozostaje bez wpływu na ocenę struktury wiekowej samochodów w Polsce. Zniekształca ją, czyniąc starszą, niż jest w rzeczywistości. Jest to czynnik, który musi być uwzględniany w prognozach dotyczących zapotrzebowania na poszczególne rodzaje paliw. Proces związany z eliminacją z ewidencji pojazdów aut nieużytkowanych temu sprzyja. Istnieją jednak bariery administracyjne, które spowalniają go i skutecznie wykluczają możliwość objęcia nim wszystkich samochodów niejeżdżących po drogach. Ograniczeniem pozostaje uzyskanie dla nich przez właściciela statusu zabytkowego – kolekcjonerskiego[5]. Sprzymierzeńcem wysiłków na rzecz likwidacji dyferencji między liczbą pojazdów w rejestrach a rzeczywistą są przepisy ubezpieczeniowe, w tym ustawowy obowiązek posiadania polisy OC[6], a w przyszłości procedowany

---

[3] Pojazdy wyrejestrowane w Polsce w latach 2007–2014, http://www.cepik.gov.pl/documents/76251/76577/Pojazdy+wyrejestrowane+w+latach+2007+-+2014/4573be44-fc4c-4d7e-88d1-4d7e978f0590

[4] *Maluchy, Polonezy i Syreny w rządowym rejestrze – czy naprawdę jeździmy starymi gratami?*, https://www.auto-swiat.pl/wiadomosci/aktualnosci/maluchy-polonezy-i-syreny-w-rzadowym-rejestrze-czy-naprawde-jezdzimy-starymi-gratami/5m7bzos

[5] *Ustawa z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym* definiuje pojazd zabytkowy jako ten, *który na podstawie odrębnych przepisów został wpisany do rejestru zabytków lub znajduje się w wojewódzkiej ewidencji zabytków, a także pojazd wpisany do inwentarza muzealiów, zgodnie z odrębnymi przepisami (Dz.U. 1997 Nr 98 poz. 602, art. 2 pkt. 39).*

[6] *Ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych.*

projekt zakładający nakładanie kar na właścicieli, którzy w okresie 30 dni od nabycia pojazdu nie zrejestrowali go[7].

Wyrejestrowywanie pojazdów łączące się najczęściej z ich utylizacją lub eksportem jest ogniwem nadmienianego procesu zastępowania starszych generacji pojazdów nowszymi. Podobnie rzecz się ma z rejestracją samochodów dotąd nieużytkowanych w Polsce. Dotyczy to aut fabrycznie nowych, jak i pochodzących z importu egzemplarzy używanych. W 2018 r. było ich ponad 1,16 mln[8], a w I kwartale 2019 r. ponad 360 tys.[9] Liczba pojazdów, które po raz pierwszy zyskały możliwość poruszania się po drogach, wynosiła odpowiednio 531 889 i 139 809[10], co może uchodzić za odzwierciedlenie dynamiki zmian zachodzących w strukturze wiekowej samochodów osobowych w Polsce[11].

Także w przypadku importu samochodów używanych bardzo czytelny jest element dający się określić mianem przejścia do kolejnej generacji technologicznej pojazdów. Jest on z jednej strony naturalnym procesem związanym z konsekwencjami ograniczonej czasem pracy amortyzacji i trwałością aut, natomiast z drugiej postępem technicznym i towarzyszącą temu zmianą obowiązujących standardów. Nieznacznie, lecz systematycznie rośnie udział procentowy sprowadzanych aut młodszych niż 4 lata[12].

---

[7] F. Trusz, *Rejestracja pojazdu w Polsce. Senat przegłosował nowe przepisy. Aż 1000 zł kary za spóźnienie*, http://moto.pl/MotoPL/7,88389,25004523,rejestracja-pojazdu-w-polsce-senat-przeglosowal-nowe-przepisy.html

[8] *Pojazdy zarejestrowane w podziale na rodzaje w poszczególnych miesiącach w 2018 roku*, http://www.cepik.gov.pl/documents/76251/76577/Pojazdy+zarejestrowane+w+2018+r.+rodzajami+%28pdf%29/da4673c2-2775-47e6-9a24-97132d226de1

[9] *Pojazdy zarejestrowane w podziale na rodzaje w kolejnych miesiącach 2019 roku*, http://www.cepik.gov.pl/documents/76251/76577/Pojazdy+zarejestrowane+w+2019+r.+rodzajami+%28pdf%29/18f1b9d6-e121-4670-aa75-b9ed43c44036

[10] *Branża motoryzacyjna. Raport kwartalny PZPM i KPMG nr2/2019*, https://www.pzpm.org.pl/pl/content/download/9371/53964/file/SUMMARY_Raport%20KPMG%20i%20PZPM_Bran%C5%BCa%20motoryzacyjna.%20Automotive%20Industry%20Q2%202019.pdf

[11] Wielkości ta nie uwzględnia reeksportu. Dotyczy to nie tylko wywozu aut używanych, gdzie dominuje kierunek ukraiński, ale też w przypadku samochodów nowych państw unijnych. Pułapka reeksportu, czyli jak importerzy pompują statystyki, a dilerzy zyski ze sprzedaży samochodów, http://moto.pl/MotoPL/7,88389,22938485,pulapka-reeksportu-czyli-jak-importerzy-pompuja-statystyki.html

[12] *Import używanych samochodów osobowych do Polski w latach 2003–2016*, https://www.pzpm.org.pl/Rynek-motoryzacyjny/Import-uzywanych-samochodow/Import-samochodow-uzywanych-wg-MF/Import-uzywanych-samochodow-osobowych-do-Polski-w-latach-2003-2016

W wymiarze ilościowym bilans jest wyraźnie dodatni. Znacznie więcej aut jest rejestrowanych w Polsce niż wycofywanych. Oznacza to przyrost konsumpcji paliw w najbliższych latach i to w tempie wyższym niż procentowy wzrost liczby użytkowanych samochodów. Wynika on z jakościowego charakteru zmiany i charakterystyki technicznej nowych modeli aut: cięższych, większych i lepiej wyposażonych od swych poprzedników.

Od 2016 r. coraz wyraźniejsza staje się tendencja redukcji importu aut osobowych z silnikami wysokoprężnymi. Jest ona widoczna także w przypadku pojazdów fabrycznie nowych. W rezultacie zmian preferencji nabywców udział samochodów napędzanych jednostką o zapłonie samoczynnym został zredukowany do poziomu oscylującego wokół 30%. Nadmieniony spadek odnotowano także w innych państwach unijnych. Jest on, co warto podkreślić, wyższy niż w Polsce[13] i niezmiennie od 2014 r. przekracza pułap 40%. Wielkość ta musi być brana pod uwagę w prognozach dotyczących sprowadzania do Polski aut używanych. Szczególnie w kontekście polityki ekologicznej w Niemczech, Beneluksie oraz we Francji czy Włoszech, a więc z tych członków Wspólnoty, z których najczęściej są one importowane do Polski. Wzrost troski o środowisko naturalne, z którego zanieczyszczeniem są kojarzone samochody z silnikami zasilanymi olejem napędowym, przekładający się m.in. na ceny tych pojazdów, co nie pozostaje bez wpływu na preferencje zakupowe w uboższych społeczeństwach regionu Europy Środkowo-Wschodniej. Obawy przed zmianą struktury rynku pod względem typu wykorzystywanego paliwa na rzecz ostatniego z wymienionych nie są bezpodstawne[14]. Oznacza to potencjalny wzrost zainteresowania paliwami do jednostek dieslowskich o wyższych parametrach jakościowych.

[13] *Passenger Car Fleet by Fuel Type*, https://www.acea.be/statistics/article/Passenger-Car-Fleet-by-Fuel-Type

[14] W 2018 r. sprowadzono do Polski milion używanych aut. Ponad połowa pochodziła z Niemiec, https://businessinsider.com.pl/motoryzacja/samochody-uzywane-sprowadzone-do-polski-w-2018-r-raport-samar/n63k6nc

3. Perspektywy

a) Czynniki endogeniczne

W perspektywie krótko- i średnioterminowej nadmieniona powyżej zmiana generacyjna pojazdów w Polsce przy jednoczesnym wzroście liczby samochodów będzie stymulowała popyt na paliwa ciekłe. Dotyczyć będzie w zbliżonych proporcjach benzyn silnikowych i oleju napędowego. Z czasem jednak należy przyjąć za pewnik narastanie dyferencji w popycie charakteryzujące się wzrostem zapotrzebowania na pierwsze z wymienionych i spadek konsumpcji ostatniego. Tempo, jak i dynamika tego procesu będą postępować stosownie do wzrostu roli czynnika proekologicznego w świadomości społecznej oraz przepisach prawnych. W nadmienionych procesach nietrudno dostrzec konsekwencje zmian, które zaszły na rynku samochodów osobowych, a także transformacji, jaką rozpoczęło wprowadzenie nowych rodzajów napędu. Zwraca tu uwagę rosnący udział samochodów o napędzie hybrydowym. Raporty koncentrują się wyłącznie na typach plug-in (*Plug-in Hybrid Electric Vehicles* – PHEV), tu zestawienia r./r. sięga 29%[15]. W ocenie przyszłego popytu na paliwa istotne miejsce należy przypisać pojazdom o napędzie spalinowo-elektrycznym nieposiadającym możliwości podłączenia do ładowarek (*Hybrid Electric Vehicles* – HEV). Ich udział na rynku wtórnym jest coraz wyraźniejszy. W sierpniu 2019 r. w najpopularniejszym serwisie internetowym z ogłoszeniami motoryzacyjnymi sięgał 2%[16], dla pojazdów nowych było to już ponad 12%[17]. Utrzymanie tego trendu będzie skutkowało wspomnianym spadkiem udziału samochodów osobowych z jednostkami napędowymi o zapłonie samoczynnym na rzecz pojazdów zasilanych benzynami silnikowymi, a w dalszej kolejności LPG, CNG, a potencjalnie także paliw na bazie etanolu.

---

[15] Globenergia, *Liczba samochodów elektrycznych w polsce stale rośnie*, https://globenergia.pl/liczba-samochodow-elektrycznych-w-polsce-stale-rosnie-96-pojazdow-zarejestruja-firmy/

[16] *2213 samochodów a 101 353 w ofercie*, https://www.otomoto.pl/osobowe/?search%5Bfilter_enum_fuel_type%5D%5B0%5D=hybrid&search%5Bbrand_program_id%5D%5B0%5D=&search%5Bcountry%5D=

[17] *322 samochody z 2536 pojazdów w ofercie dealerów*, https://www.otomoto.pl/osobowe/nowe/?search%5Bfilter_enum_fuel_type%5D%5B0%5D=hybrid&search%5Bbrand_program_id%5D%5B0%5D=&search%5Bcountry%5D=&l=1

Nie wydaje się, by preferencje wynikające z u„Ustawy o elektromobilności i paliwach alternatywnych”[18] czy procedowane rozporządzenie zakładające dopłaty do samochodów elektrycznych[19] mogły cokolwiek zmienić. Skala dofinansowania pozwala na wykorzystanie jej jedynie w przypadku aut najmniejszych o niewielkim zasięgu. Może stanowić co najwyżej dodatkowy bodziec stymulujący wzrost zainteresowania pojazdami zasilanymi energią elektryczną.

Analizując czynniki oddziaływania na rynek wewnętrzny, należy brać pod uwagę także czynniki kulturowe. Zmienną, której nie można bagatelizować, jest stosunek kolejnych pokoleń do posiadania pojazdu[20]. Poważną barierą pozostaje tzw. pokolenie Y, czyli osoby urodzone w latach 80. i na początku lat 90. XX w. Opracowania analityczne z obszaru HR wskazują brak poczucia wspomnianej potrzeby[21]. Zważywszy na coraz istotniejszą pozycję, jaką przedstawiciele tej grupy wiekowej zajmują na rynku pracy, okoliczność ta nie będzie bez znaczenia dla liczby pojazdów poruszających się po polskich drogach. Podobnie należy interpretować także wzrost znaczenia dbałości o środowisko naturalne oraz związany z tym styl życia mający coraz szersze grono sympatyków nie tylko wśród młodszych generacji.

Za czynnik endogeniczny musi uchodzić także prawodawstwo unijne i kierunki jego zmian, co wynika z członkostwa Polski w strukturach Wspólnoty. Zwraca uwagę coraz wyraźniej eksponowana przez niemal wszystkie jej organy, włącznie z Komisją Europejską, troska o środowisko naturalne i konieczność przeciwdziałania dalszym zmianom klimatycznym. Znajduje to swoje odzwierciedlenie w stanowionych regulacjach dotyczących dopuszczalnych norm emisji spalin. Determinują one prace w przemyśle motoryzacyjnym, tak w obszarze projektowo-konstrukcyjnym pojazdów, jak

---

[18] *Ustawa z dnia 11 stycznia 2018 r. o elektromobilności i paliwach alternatywnych (Dz.U. 2018 poz. 317)*.

[19] *Budżet dopłaci tylko do małych aut elektrycznych*, https://www.prawo.pl/prawo/doplata-do-zakupu-malych-aut-elektrycznych-w-polsce,446082.html

[20] B. Hysa, *Zarządzanie różnorodnością pokoleniową*, „Zeszyty Naukowe Politechniki Śląskiej – Zarządzanie i organizacja”, 2016, z. 97, https://www.polsl.pl/Wydzialy/ROZ/ZN/Documents/z97/30_po_rec_034_Hysa.pdf

[21] S. Stachowska, *Oczekiwania przedstawicieli pokolenia Y wobec pracy i pracodawcy*, „HRM”, 2012, nr 2 – *Zarządzanie zasobami ludzkimi*, http://www.ipiss.com.pl/wp-content/uploads/downloads/2015/01/ZZL_2-2012_Stachowska-S_33-56.pdf

i wytwórców paliwa. Kierunki zachodzących przeobrażeń widoczne są już na etapie wniosków dotyczących zmian bądź wręcz zastąpienia istniejących przypisów[22]. Bazowe wytyczne zostały już określone w kwietniu 2019 r.[23] Zakładają one m.in. konieczność wprowadzenia przez producentów samochodów osobowych rozwiązań zapewniających redukcję wytwarzanego podczas spalania CO_2 o 35% w stosunku do i tak restrykcyjnych wymogów mających obowiązywać w 2021 r., czyli od 85 g/km[24]. Przejściowo w 2020 r. będzie to 95 g/km. Obecnie zgodnie z normą Euro-6 wynoszą one do 130 gr/km. Zmianą, jaka nastąpi w 2021 r., jest ograniczenie o 35%, czyli tyle, o ile zmniejszono wymogi maksymalnej emisji CO_2 w latach 2001–2017[25]. Standardy te spełniać każdy producent, a podane wielkości będą odnoszone jako średnia do całej sprzedawanej floty. Przekroczenie ich będzie niosło za sobą konieczność uiszczenia dodatkowej opłaty w wysokości 95 euro za gram przekroczenia normy od każdego sprzedanego egzemplarza. Kryterium 85 gr/km CO_2 prawdopodobnie nie spełnia żaden model z gamy nowych aut spalinowych trafiających do klientów. Utrzymanie ich wymaga bowiem przeciętnego zużycia paliwa na poziomie ok. 4 litrów dla samochodów benzynowych i 3,5 litra dla diesli. Nawet napęd standardowy hybrydowy nie zapewnia takich osiągów[26]. Uzyskanie ich możliwe jest tylko przez modele plug-in oraz pojazdy elektryczne, które w trakcie jazdy nie wytwarzają CO_2. Nadmieniane 35 gr/km w 2021 roku zostanie obniżone o kolejne 15% do 2025 roku i o 30% do 2030 r.. Biorąc pod uwagę istniejące rozwiązania techniczne, oznaczałoby

---

[22] Np. Wniosek – *Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (WE) nr 715/2007 w sprawie homologacji typu pojazdów silnikowych w odniesieniu do emisji zanieczyszczeń pochodzących z lekkich pojazdów pasażerskich i użytkowych (Euro 5 i Euro 6) oraz w sprawie dostępu do informacji dotyczących naprawy i utrzymania pojazdów, https://ec.europa.eu/transparency/regdoc/rep/1/2019/PL/COM-2019-208-F1-PL-MAIN-PART-1.PDF*

[23] *Reducing CO_2 emissions from passenger cars*, https://ec.europa.eu/clima/policies/transport/vehicles/cars_en

[24] *Rozporządzenie Komisji (UE) 2016/646 z dnia 20 kwietnia 2016 r. zmieniające rozporządzenie (WE) nr 692/2008 w odniesieniu do emisji zanieczyszczeń pochodzących z lekkich pojazdów pasażerskich i użytkowych (Euro 6).*

[25] *From laboratory to road: A 2018 update,* https://theicct.org/publications/laboratory-road-2018-update

[26] M. Gis, *Unia Europejska przycina emisję CO_2. Pociągnie to za sobą niższe zużycie paliwa*, http://moto.pl/MotoPL/7,88389,23277145,unia-europejska-przycina-emisje-co2-pociagnie-to-za-soba-nizsze.html

to koniec produkcji aut spalinowych w UE przeznaczonych do poruszania się po drogach państw członkowskich bądź niebotyczny wzrost ich cen.

Doraźnie przyjęte regulacje oznaczają całkowitą rewolucję na rynku motoryzacyjnym. Wzmocniony zostanie tzw. *downsizing*, czyli zastępowanie większego układu napędowego takim o mniejszej pojemności, a nierzadko i zredukowanej w stosunku do poprzedniej wersji liczbie cylindrów. Obniży się litraż samochodów, a ich silniki będą znakomicie bardziej wydajne, tj. stosunek kW/cm^3 zwiększy się w stosunku do stanu obecnego. Modernizacje i zmiany konstrukcyjne jednostek napędowych niosą za sobą większe wymogi dotyczące jakości paliwa i niższą tolerancję na te niespełniające wymogów.

b) Czynniki egzogeniczne

Czynnikiem o kluczowym znaczeniu dla tego, co się dzieje na rynku samochodowym w Polsce, pozostaje oddziaływanie otoczenia zewnętrznego, a w szczególności sytuacji ekonomiczno-społecznej w państwach członkowskich Wspólnoty. Zupełnie szczególne miejsce wśród nich zajmują Niemcy, a w dalszej kolejności kraje Beneluksu, Francja oraz Włochy. Wpływ ten jest nie tylko konsekwencją nadal istniejących różnic w poziomie życia i dochodach mieszkańców, lecz także poniekąd wynikającą ze wskazanego czynnika inspiracją[27]. W rezultacie z tego obszaru pochodzi przytłaczająca większość importu tak nowych, jak i używanych samochodów osobowych.

Istotne znaczenie w analizowanym kontekście należy przypisać panującym tam nastrojom gospodarczym oraz społecznym. Pierwszy przypadek odpowiada za ilościowy, a w dalszej kolejności jakościowy wymiar strony podażowej[28]. Natomiast drugi, włączywszy w to kontekst ideologiczno-kulturowy, pozostaje determinantem popytu. Decyduje o preferencjach nabywców,

---

[27] Procesem zupełnie naturalnym, a polegającym na budowie wzorców naśladowczych na podstawie społeczeństwa, które osiągnęło status uznany za cel – S. Bodys, *Zmiana wzorców konsumpcji w Polsce na tle innych krajów europejskich,* w: *Transformacja gospodarcza w Polsce,* red. M. Geise, J. Oczki, D. Piotrowski, Bydgoszcz 2016, s. 85–98.

[28] Wynika to z pozycji, jaką zajmuje przemysł samochodowy we wskazanych państwa. Za przykład może posłużyć dofinansowanie, z jakiego korzystali obywatele Niemiec przy pozbyciu się starego i zakupie nowego auta po 2008 roku, gdy gospodarka kraju spowolniła i rząd starał się stymulować rozwój najważniejszych sektorów. P. Nowak, *Funkcjonowanie sektora motoryzacyjnego w okresie kryzysu w latach 2008–2009,* „Prace Komisji Geografii Przemysłu", 2011, nr 17, s. 182.

odzwierciedlając ich nastawienie, mody, trendy czy wyobrażenia na temat przyszłości.

Analizując czynniki wpływu na rynek motoryzacyjny w Polsce, mające swoją lokalizację poza jej obszarem, należy zwrócić uwagę na przybierający na sile brak akceptacji w wymienionych państwach Wspólnoty dla pojazdów szczególnie uciążliwych dla środowiska. Ma to swoje odzwierciedlenie w przepisach unijnych, regulacjach krajowych, ale i w lokalnych prawach stanowionych przez samorządy[29]. Standardem stało się uzależnianie wysokości taryf od rodzaju paliwa, pojemności silnika, a nawet ciężaru samochodu. W przypadku tego samego modelu zasilanego benzyną i dieslem różnica może być nawet dwukrotna na niekorzyść ostatniego z wymienionych. Wynika to z rodzaju nośnika energii, a także z samych właściwości konstrukcyjnych pojazdów z silnikiem wysokoprężnym, tj. masy pojazdu i dla tej samej mocy większej niż w przypadku samochodu z zapłonem iskrowym jednostki napędowej. Dyferencja w opłatach wykazuje też znaczącą dynamikę wzrostową. Zniechęca to dotychczasowych użytkowników takich pojazdów do ich utrzymywania. Pokaźna część generowanego tym sposobem rynku wtórnego trafia na eksport, m.in. do Polski.

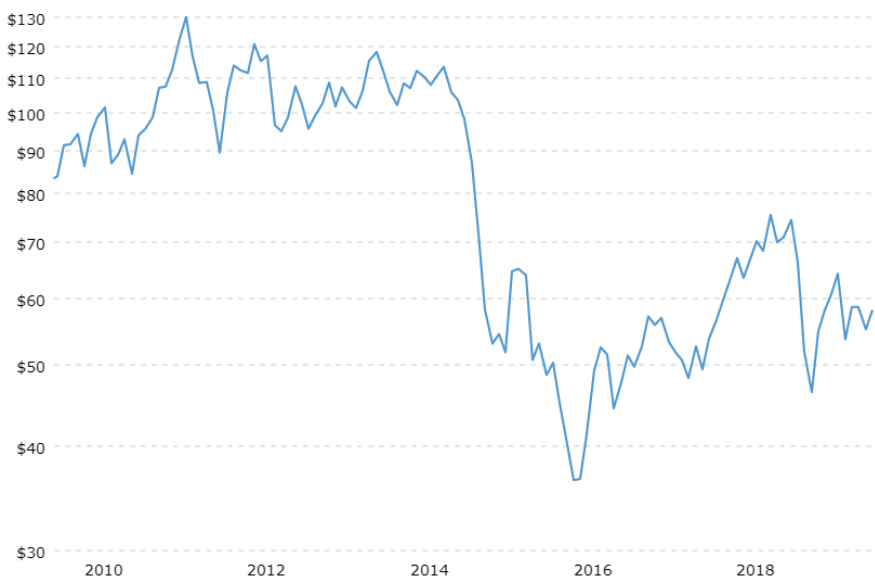
Elementem oddziaływania zewnętrznego na rynek pozostają także rozwiązania techniczne. Ich dostępność na rynku docelowym rzutuje na popularność danego typu pojazdów czy też modeli. I tu eksponowane miejsce zajmują kwestie logistyczne, a w dalszej kolejności także tzw. czynnik środowiskowy, np. obecność instalacji CNG nie będzie atutem podażowym, jeśli w okolicy potencjalnego klienta nie znajduje się stacja tankowania sprężonym „błękitnym paliwem", serwis dokonujący napraw określonych urządzeń itd. W kontekście przestępczości paliwowej okoliczność ta ma istotne znaczenie. Rzadko w przypadku oferty z rynku wtórnego takie wyposażenie dodatkowe ma swoje odbicie w cenie. Stąd też auta te są chętnie nabywane, a ich napływ do Polski systematycznie rośnie.

Jednym z poważniejszych bodźców wpływających na rynek motoryzacyjny w Polsce, tak jak i całej Wspólnocie, pozostają światowe ceny ropy naftowej. Po odreagowaniu spadków z drugiej połowy 2008 i 2009 r. w latach 2010–2014

[29] W przypadku Holandii jednym z elementów kształtowania kosztów jest lokalizacja pojazdu, https://www.traxall.nl/en/news/car-taxes-in-the-netherlands/

ukształtowały się one na poziomie, którego średnie wartości oscylują w przedziale 55–65 USD/bbl. Uwzględniając czynnik inflacyjny, oznacza to spadek kursu surowca. Prognozy na najbliższe lata zakładają utrzymanie tego trendu. Są to jednak symulacje oparte przede wszystkim na narzędziach ekonomicznych. W ocenie ryzyka nie w pełni uwzględnia się inne czynniki. Przykład pożaru rafinerii należących do Aramco oraz napięcie w regionie cieśniny Ormuzd we wrześniu 2019 r. są sygnałem potencjalnych zagrożeń wynikających z braku stabilności w tej części świata. Ich oddziaływanie na rynek, nawet w wymiarze czysto propagandowym, jest jednym z najpoważniejszych elementów hamujących spadek cen naftowych i panujące na rynkach surowcowych napięcie.

Rysunek 2. Kurs ropy naftowe (brent) w latach od 2010 r. w transakcjach spotowych



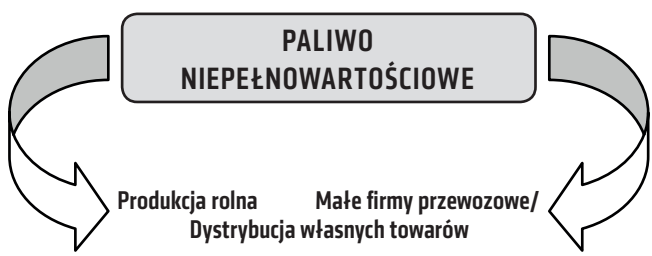
Źródło: World Bank, www.wordbank.org

4. Zmiany na rynku a ewolucja zagrożeń związanych z przestępczością w obszarze paliw płynnych

a) Olej napędowy i benzyny silnikowe

Przewidywany wzrost importu używanych aut o napędzie dieslowskim przyczyni się do większego niż dotąd zużycia oleju napędowego. Będą to jednak samochody nowszych generacji, bardziej wrażliwe na jakość paliw niż te wyposażone w silniki wysokoprężne starszego typu. Domieszki gorszych gatunkowo cieczy węglowodorowych pozbawionych uszlachetniaczy nie stanowią alternatywnego rozwiązania. Stąd też nie wydaje się prawdopodobne, by popularne przez przerabianie oleju opałowego i stałe dostawy jego do punktów zbytu miały rację bytu. Nawet państwowe koncerny naftowe (PKN Orlen) mają poważny problem ze sprostaniem wymaganiom, jakie nakładają producenci pojazdów na jakość paliw[30]. Uzyskanie wymaganego efektu poza przemysłowymi instalacjami jest bardzo trudne. Wspomniany proceder przestępczy polegający na fałszowaniu produktu zapewne dalej będzie kontynuowany, lecz jego oferta podażowa znacznie zawężona. Z dużą dozą prawdopodobieństwa ukierunkowana zostanie na gospodarstwa rolne i dysponujące starszego typu pojazdami niewielkie firmy transportowe bądź świadczące takie usługi, dystrybuując samodzielnie swoje produkty.

Rysunek 3. Obszary potencjalnej dystrybucji paliwa niepełnowartościowego



Źródło: opracowanie własne

[30] Co wynika pośrednio z procesu technologicznego związanego nie tyle z rafinacją, co metodami wzbogacania produktu.

Zagrożenie wprowadzenia na rynek paliw nieznanego pochodzenia i obrót nimi jest nierozerwalnie związane z nierejestrowanym importem. Wobec monitorowania cystern i specjalistycznych naczep w systemie geolokalizacyjnym, do którego wgląd mają uprawnione do tego służby, ryzyko to zostało wydatnie zredukowane[31]. Wyłączenie rejestratora dopuszczalne jest tylko wtedy, kiedy nie jest on załadowany[32]. Łączy się to jednakże z potencjalnym rozszczelnieniem systemu kontroli. Obciążony pojazd tylko pozornie łatwo odróżnić, a brak uruchomionego urządzenia jest sygnałem dla kontroli drogowych. W przypadku załadunku częściowego wizualnie staje się to praktycznie niemożliwe.

Potencjalna luka w nadzorze istnieje także za sprawą wystąpienia okoliczności, które zostały wskazane przez prawodawcę jako te legalizujące wyjęcie spod monitoringu pojazdów przystosowanych do przewozu paliw[33]. Zagrożenie nieewidencjonowanym importem czy też sprzedażą paliw płynnych generowane jest przez brak konieczności uwidaczniania pojazdu przewożącego towar między magazynami/miejscami składu należącymi do tej samej firmy[34]. Możliwości wykorzystania tej swobody przez podmioty wprowadzające do sprzedaży olej napędowy czy benzyny silnikowe, łamiąc przepisy, są znaczące i nie powinny być ignorowane[35].

Zwraca też uwagę możliwość częściowej neutralizacji niezwykle wysokich kar związanych z nieprawidłowościami w transporcie paliw. Państwo nakłada je na podmioty koncesjonowane. Brak licencji w tym przypadku stawia przewożącego w odmiennej sytuacji prawnej, a jego odpowiedzialność finansowa jest niższa[36].

Nieewidencjonowane wprowadzanie do sprzedaży detalicznej paliw na masową skalę w praktyce ściśle wiąże się z funkcjonowaniem stacji niefranczyzowych. Wynika to z ich niczym nieskrępowanej samodzielności handlowej.

---

[31] *(Dz.U. 2017 poz. 708), ustawa z dnia 9 marca 2017 r. o systemie monitorowania drogowego i kolejowego przewozu towarów oraz obrotu paliwami opałowymi art. 12.1.*

[32] Ibid., art. 10.b 2.

[33] Ibid. art. 7b. 1.

[34] Ibid. art. 3.7.

[35] Wyłącznie przewozów międzynarodowych przewidziany z art. 3.8 nie rozwiązuje problemu.

[36] *Dz.U. 2018 poz. 1481 ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o transporcie drogowym oraz niektórych innych ustaw , załącznik 3 pkt 1.*

Swobody, której nie posiadają punkty korzystające z sieciowego znaku. Te bowiem pozostają pod rygorystycznym nadzorem tego, kto im go udzielił, co jest pochodną troski o zachowanie obowiązujących standardów jakościowych przez daną markę. W przypadku sektora paliwowego integralną częścią takich porozumień jest zwykle stały podgląd elektroniczny zbiorników franczyzobiorcy przez franczyzodawcę. Monitorowana jest ilość paliwa, wielkość sprzedaży itd. Kontrola online w istocie wyklucza możliwość uzupełniania bez wiedzy ośrodka kontrolującego zbiorników dystrybucyjnych. W BP decyzja o kierowaniu dostaw jest podejmowana przez centrum zaopatrzeniowe na podstawie analizy odczytów[37]. Podobnych narzędzi używają także pozostałe koncerny oferujące przedsiębiorcom sprzedaż pod swoim szyldem. Pozasieciowe stacje paliw nie mają żadnej kurateli tego typu. Standardowo kontrole i inspekcje handlowe w odniesieniu do infrastruktury sprzedażowej koncentrują się na tym, czy dystrybutory posiadają aktualne certyfikaty i czy wskazania ich liczników pokrywają się ze stanem faktycznym. Żaden podmiot zewnętrzny nie sprawdza na bieżąco stanu ich zbiorników i nie ma nawet możliwości technicznej, by to robić bez instalacji odpowiedniej aparatury pomiarowo-nadawczej. Zmiana przepisów prawnych w tym obszarze na pewno sprzyjałaby uszczelnieniu rynku. Wymagałaby jednakże powołania ośrodka monitorującego oraz wprowadzenia wymogu doposażenia stacji paliwowych we właściwe urządzenia służące do tego celu.

Nadmienione sugestie dotyczące regulacji prawnych utrudniłby także stosowany na stacjach pozafranczyzowych proceder przestępczy polegający na dodawania do paliw uszlachetniaczy w postaci mieszanek substancji nienadających się do tego celu lub w ilościach wykraczających poza obowiązujące normy. Koncept przestępstwa jest bardzo czytelny. Sprowadza się do zastosowania jako ulepszacza rozpuszczalników dostępnych po cenach kilkukrotnie niższych niż benzyny silnikowe czy oleje napędowe. Im więcej zmiesza się ich z pełnowartościowym paliwem, tym zysk z tytułu różnic cenowych między cieczami jest wyższy[38]. Identycznie rzecz się ma z aplikowaniem do paliw

[37] *STACJE PARTNERSKIE BP – jak to działa?* „Na stacji paliw" Nr 2 (3), kwiecień-czerwiec 2016, s. 4 i 5, https://nastacjipaliw.pl/downloads/nsp/nr2-2016.pdf?utm_source=landing_w2&utm_medium=www&utm_campaign=NSP%20nr%203

[38] Odnotowano nawet przypadek, w którym producent rozpuszczalnika sprzedawał go już nie jako uszlachetniacz, lecz paliwo, *Opolski producent rozpuszczalnika sprzedawał go na*

w zbiornikach dystrybucyjnych biokomponentów w ilościach tworzących wartość handlową. Dotyczy to przede wszystkich estrów metylowych w przypadku zasilania silników wysokoprężnych i etanolu dla pojazdów o zapłonie iskrowym. Prowadzona w lipcu 2019 r. zmiana *ustawy o biokomponentach i biopaliwach ciekłych* jest okolicznością sprzyjającą intensyfikacji występowania takich przestępstw [39].

b) Autogaz

Odrębną kategorię przestępstw paliwowych kojarzonych w znaczącej mierze również ze stacjami niefranczyzowymi stanowią te dotyczące handlu płynnym gazem. LPG jest mieszaniną propanu (C_3H_8) i butanu (C_4H_{10}). By zapewnić możliwie najlepszą pracę silnika latem, ich stosunek powinien odpowiadać w przybliżeniu proporcji 4:6, natomiast zimą 6:4, co pośrednio wynika też z przepisów prawa[40]. Te regulują głownie charakterystykę spalania. W rezultacie sprawa stosunku jednego do drugiego węglowodoru jest daleko nieprecyzyjna. Jakość paliwa jest tu w znaczącej mierze zależna od warunków atmosferycznych. Biorąc pod uwagę istniejące różnice w ich cenie, większy udział tańszego składnika niesie za sobą konkretne profity finansowe dla sprzedawcy zaniżającego zawartość droższego. Okolicznością, która może stanowić dodatkowy bodziec do popełniania przestępstw w handlu płynnym gazem samochodowym, pozostaje różnica akcyzowa. To samo paliwo wykorzystywane do celów grzewczych jest zwolnione z tego podatku, a autogaz – nie. Wejście w posiadanie pierwszego i dystrybucja go jako drugiego pozwala na generowanie dużego zysku i ułatwia konkurencję cenową z otoczeniem businessowym dopuszczającym się takiego czynu dystrybutora. Kwestia przestępczości paliwowej w obszarze autogazu wydaje się być szczególnie istotna w kontekście utrzymującego się od dwóch dekad wzrostu liczby pojazdów przystosowanych do wykorzystania tego typu zasilania. Rzecz dotyczy bowiem już 14% wszystkich zarejestrowanych w Polsce

stacje jako olej napędowy, „Nowa trybuna opolska" 30.05.2016 r., https://nto.pl/opolski-producent-rozpuszczalnika-sprzedawal-go-na-stacje-jako-olej-napedowy/ar/10160794

[39] *Dz.U. 2019 poz. 1527, ustawa z dnia 19 lipca 2019 r. o zmianie ustawy o biokomponentach i biopaliwach ciekłych oraz niektórych innych ustaw.*

[40] *Dz.U. 2016 poz. 540 Rozporządzenie Ministra Energii z dnia 14 kwietnia 2016 r. w sprawie wymagań jakościowych dla gazu skroplonego (LPG).*

samochodów osobowych[41]. Na dodatek pojazdów, których właściciele zakładają ponadprzeciętny przebieg roczny, co ma swoje bezpośrednie przełożenia na udział procentowy sprzedaży paliw do aut z silnikiem o zapłonie iskrowym. Sygnałem do niepokoju jest spadek rejestrowanej sprzedaży tego paliwa przy jednoczesnym zwiększeniu liczby pojazdów z niego korzystających[42].

c) Inne

Nowe regulacje prawne wymuszające na producentach samochodów podaży modeli po *downsizingu* czy wzmocnienie w strukturze ofertowej pojazdów typu *plug-in* oraz elektrycznych to jeden z możliwych scenariuszy rozwoju sytuacji na rynku. Jego ziszczenie się tożsame jest z redukcją, a długoterminowo nawet i eliminacją nowych aut spalinowych. Nie jest to jednakże jedyna dająca się przewidzieć droga rozwoju rynku motoryzacyjnego.

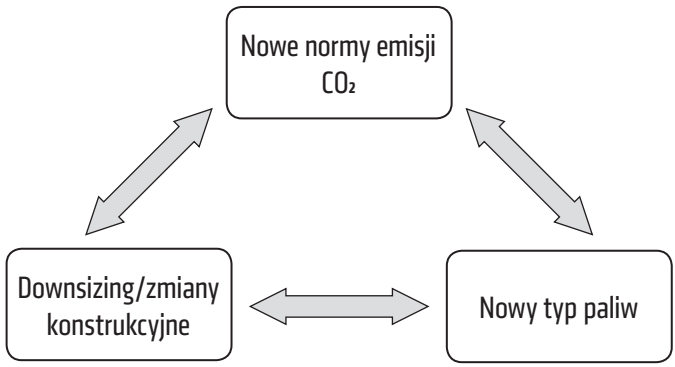
Alternatywą do zmniejszania kubatury jednostek napędowych potencjalnie mogłyby być oczywiście nowe konstrukcje. Nie wydaje się jednak możliwe, by istniały już gotowe do wdrożenia tego typu rozwiązania i nie były realizowane. Trudno bowiem wyobrazić sobie, aby którykolwiek z koncernów dysponujący takim autem nie zechciał wykorzystać go po to, by zyskać przewagę nad konkurencją i zdominować rynek. Informacje o projektach i prototypach aut o standardach, do których przyzwyczaił się współczesny rynek, a zużywających średnio mniej niż 4 litry benzyny czy też 3,5 diesla pojawiają się cyklicznie od lat. Droga od auta koncepcyjnego do uruchomiania produkcji jest długa i sceptycyzm dotyczący finalizacji takich przedsięwzięć jest zasadny. Wynika z dotychczasowych doświadczeń wdrożeniowych i przejawia się w braku na rynku takich pojazdów. Jeśli bariery dotyczące konstrukcji nowego typu jednostek napędowych nie rokują pomyślnie, należy brać poważnie pod uwagę możliwość zmian w składzie paliwa płynnego wykorzystywanego w silnikach spalinowych.

---

[41] *Raport: ile aut z LPG jeździ po polskich drogach?, https://www.auto-swiat.pl/wiadomosci/aktualnosci/raport-ile-aut-z-lpg-jezdzi-po-polskich-drogach/7hceycp*

[42] *LPG w Polsce w 2018 r. wg POGP*, https://gazeo.pl/informacje/wiadomosci/LPG-w-Polsce-w-2018-r.-wg-POGP,wiadomosc,10313.html

Rysunek 4. Możliwe kierunki zmian w motoryzacji związane z obniżeniem dopuszczalnej emisji CO_2



Źródło: opracowanie własne

W tym wymiarze pytaniem otwartym pozostaje sposób zabezpieczenia interesu Skarbu Państwa w przypadku upowszechnienia zmian. Dotychczasowe definicje paliw wynikające z interpretacji aktów ustawodawczych[43] oraz przepisów skarbowych[44] pozostawiają pewne luki, łącząc produkt z instalacją wykorzystywaną do jego wytwarzania[45]. Nie wydaje się to jednak perspektywiczne rozwiązanie. Okoliczność, w której w charakterze paliwa zostanie wykorzystana substancja niemająca dotąd takiego zastosowania, nie urosła jeszcze do rangi problemu, niemniej jednak jego wystąpienie pozostaje kwestią czasu. Zważywszy na popularność rozwiązań stosowanych w Ameryce Południowej, należy brać pod uwagę adaptację rozwiązań technicznych wykorzystujących etanol, zyskujący coraz szersze grono zwolenników, także w Stanach Zjednoczonych[46].

Kontekst zastosowania nietypowych paliw czy dodatków do nich można uznać za obecny także w niszowym, lecz dynamicznie rozwijającym się obszarze specjalistycznych tuningów silnikowych. Upodobania kreowane

[43] Np. *ustawa z dnia 11 stycznia 2018 r. o elektromobilności i paliwach alternatywnych, ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 1997 Nr 54 poz. 348), ustawa z dnia 25 sierpnia 2006 r. o biokomponentach i biopaliwach ciekłych (tekst jedn.: Dz.U. 2018 poz. 1344).*

[44] *Ustawa z dnia 6 grudnia 2008 r. o podatku akcyzowym art. 89, ust. 14 (Dz.U. 2009 Nr 3 poz. 11).*

[45] *Prawo energetyczne (Dz.U. z 2018 r., poz. 755, z późn. zm.)* art. 3 ust. 10e.

[46] *Ethanol Fuel Basics*, https://afdc.energy.gov/fuels/ethanol_fuel_basics.html

i upowszechniane przez kulturę masową są silnym bodźcem kształtowania rynku, a motoryzacja eksponuje ten proces. W zamożnych społeczeństwach europejskich, do których należy zaliczyć także i rodzime samochody, za sprawą swej powszechności utracił nadany mu przed wiekiem czysto utylitarny charakter. Okoliczność ta przyczyniła się do rosnącej popularności samochodów modernizowanych dla potrzeb hobbysty. Wśród nich zwracają uwagę pojazdy przystosowane do nielegalnych wyścigów drogowych, czy tzw. dryftu. Nierzadko ich właściciele starają się podnieść moc silnika, dodając ciecze z dużą zawartością tlenu przyśpieszające spalanie (nitrometan, eter tert -butylometylowy) czy też podnoszące liczbę oktanową, poprawiające gęstość mieszanki lub jej schłodzenie. Marginalny wymiar zjawiska nie powinien być lekceważony, gdyż determinowany jest popkulturą i nie sposób przewidzieć tempa i kierunków, w których będzie zmierzał. Zwraca uwagę jego precedensowy charakter polegający na aktywizacji użytkowników pojazdu do poszukiwania optymalnej dla ich potrzeb mieszanki paliwowej.

6. Zakończenie

Zmiany, jakie zachodzą na rynku samochodów osobowych i ich tempo, pozostaną kluczowym czynnikiem kształtowania konsumpcji paliw płynnych w Polsce. Zwraca uwagę wzrost liczby pojazdów zarejestrowanych w naszym kraju przy jednoczesnej przybierającej na sile dynamice usuwania przez właścicieli z ewidencji starszych aut. Jest to symptom szybko dokonującej się zmiany ich generacji. Wraz z nią istotnej modyfikacji ulega także specyfika popytowa, co znajdzie swoje odzwierciedlenie w działaniach prowadzonych z pominięciem obowiązujących przepisów prawnych. Stąd wynika konieczność ich systematycznej nowelizacji tak, by podejmowane wysiłki legislacyjne wychodziły naprzeciw temu, co daje się określić mianem branżowego *signum temporis*. Równie istotnym elementem pozostaje uzupełnienie występujących w istniejącym systemie nieprecyzyjności, które stanowią potencjalne zagrożenie dla interesu Skarbu Państwa.

Wśród obszarów szczególnego ryzyka wystąpienia zjawisk związanych z procederem przestępczym w sferze nieewidencjonowanego obrotu paliwami płynnymi istotne miejsce zajmuje rolnictwo. Podmioty aktywne w zakresie

produkcji rolnej pozostają oferentem wprowadzanych nielegalnie dodatków bio z jednej strony, a z drugiej odbiorcą dystrybuowanych detalicznie i półhurtowo lekkich olejów opałowych wykorzystywanych niezgodnie z ich przeznaczeniem. Zważywszy na dłuższy niż w obszarach miejskich czas użytkowania pojazdów samochodowych i maszyn, sektor ten pozostanie ze względu na zmiany technologiczne jedynym, obok budownictwa, bastionem absorbcji gorszych jakościowo produktów.

Eksponowane miejsce w dystrybucji wprowadzanych nielegalnie do obrotu nośników węglowodorowych oraz wszelkich dodatków do nich oraz uszlachetniaczy zajmują pozafranczyzowe stacje. Brak stałego monitoringu elektronicznego na zasadzie online tego typu obiektów przez ośrodek zewnętrzny generuje zagrożenia wykorzystywania ich do procederów uszczuplających wpływy budżetowe państwa. Ograniczenia możliwości nieewidencjonowanego transportu wprowadzone za sprawą systemu SENT wydatnie zwiększyły szansę wykrycia przewozu takich produktów. Nie wyeliminowały ich jednak zupełnie. Istniejące w tej mierze zwolnienia związane z przemieszczaniem ładunku między magazynami czy wyjęcie spod obowiązku monitoringu części podmiotów nadal pozostawiają taką możliwość.

W przypadku węglowodorowych paliw ciekłych poważnym problemem sprzyjającym praktykom uszczuplającym wpływy budżetowe pozostaje handel autogazem. Zbyt daleka swoboda w zakresie udziału poszczególnych składników w produkcie, różnice w opodatkowaniu z tytułu zastosowania przy jednoczesnej ograniczonej możliwości kontroli jakościowych to elementy, które wydatnie osłabiają szczelność systemu.

Zagadnieniem ciągłej aktualizacji regulacji prawnych związanych z paliwami ciekłymi są nowe rozwiązania techniczne, które sprzyjają powstaniu nowych mieszanek i typów nośników. Dynamika tego procesu nasila się wraz ze zmianami norm emisyjnych i nie sposób postrzegać jej inaczej niż w kategoriach rozwiązań przyszłości.

Bibliografia

Bodys S., Zmiana wzorców konsumpcji w Polsce na tle innych krajów europejskich, w: *Transformacja gospodarcza w Polsce*, red. M. Geise, J. Oczki, D. Piotrowski, Bydgoszcz 2016.
http://moto.pl/
http://www.cepik.gov.pl
http://www.ipiss.com.pl/
https://afdc.energy.gov/
https://businessinsider.com.pl/
https://ec.europa.eu/
https://ec.europa.eu/
https://gazeo.pl/
https://globenergia.pl/
https://nastacjipaliw.pl/
https://nto.pl/
https://theicct.org/
https://www.acea.be /
https://www.auto-swiat.pl/
https://www.otomoto.pl/
https://www.polsl.pl/
https://www.prawo.pl/
https://www.pzpm.org.pl/
https://www.pzpm.org.pl/
https://www.traxall.nl/
Nowak P., *Funkcjonowanie sektora motoryzacyjnego w okresie kryzysu w latach 2008–2009*, „Prace Komisji Geografii Przemysłu", 2011, nr 17.
Rozporządzenie Komisji (UE) 2016/646 z dnia 20 kwietnia 2016 r. zmieniające rozporządzenie (WE) nr 692/2008.
Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (WE) nr 715/2007.
Rozporządzenie Ministra Energii z dnia 14 kwietnia 2016 r. w sprawie wymagań jakościowych dla gazu skroplonego (LPG) (Dz.U. 2016, poz. 540).
STACJE PARTNERSKIE BP – jak to działa? „Na stacji paliw" Nr 2 (3), kwiecień-czerwiec 2016.
Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 1997 Nr 54 poz. 348).
Ustawa z dnia 6 grudnia 2008 r. o podatku akcyzowym (Dz.U. 2009 Nr 3 poz. 11).
Ustawa z dnia 9 marca 2017 r. o systemie monitorowania drogowego (Dz.U. 2017 poz. 708).
Ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o transporcie drogowym (Dz.U. 2018 r. poz. 1481).

Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. 1997 r. Nr 98 poz. 602).

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

Ustawa z dnia 11 stycznia 2018 r. o elektromobilności i paliwach alternatywnych (Dz.U. 2018 poz. 317).

Ustawa z 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. 2018 r. poz. 755).

Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy o biokomponentach i biopaliwach ciekłych oraz niektórych innych ustaw (Dz.U. 2019 poz. 1527).

Ustawa z dnia 25 sierpnia 2006 r. o biokomponentach i biopaliwach ciekłych (Dz.U. 2018 poz. 1344).

ROZDZIAŁ IV

Cyberterroryzm jako nowe wyzwanie dla branży ubezpieczeń w Polsce.

Koncepcja finansowania ryzyka cyberterroryzmu w formie partnerstwa publiczno-prywatnego państwa i sektora ubezpieczeń

GRZEGORZ STRUPCZEWSKI[1]

1. Istota i przyczyny zjawiska cyberterroryzmu

Kluczowym wymiarem bezpieczeństwa w XXI w. będzie model aktywnej współpracy między sektorem publicznym i prywatnym. Dużo wyższa dynamika współdziałania, często w czasie rzeczywistym, stanie się koniecznością, by skutecznie bronić kluczowe systemy i dane przed stale doskonalonymi, wyrafinowanymi atakami cyberprzestępców.

Cyberterroryzm można zdefiniować jako wykorzystanie systemów informatycznych do atakowania infrastruktury krytycznej lub innych obiektów należących do instytucji publicznych celem uzyskania efektu przymusu lub zastraszenia społeczeństwa lub władz państwa[2]. Dorothy Denning, ekspert w dziedzinie cyberbezpieczeństwa, uważa, że cyberterroryzm jest bezprawnym atakiem lub groźbą ataku na komputery, sieci lub systemy informatyczne mający na celu zastraszenie lub wymuszenie na rządzie lub ludziach daleko idących ustępstw. Jednocześnie dodaje, iż za atak cyberterrorystyczny można uznać jedynie akt, który powoduje bezpośrednie szkody człowiekowi, jego mieniu lub przynajmniej wywołuje panikę i budzi strach[3]. Niezwykle trafnie

---

[1] Doktor nauk ekonomicznych, adiunkt w Katedrze Zarządzania Ryzykiem i Ubezpieczeń Uniwersytetu Ekonomicznego w Krakowie. Zainteresowania naukowe koncentrują się wokół ekonomicznych i regulacyjnych aspektów cyberbezpieczeństwa, ryzyka cybernetycznego i zarządzania nim, a także ubezpieczeń cybernetycznych.

[2] J. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington D.C. 2002.

[3] D.E. Denning, *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, Washington, 23 maja 2000, www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf (dostęp: 4.09.2019).

ujmuje to Rafał Kołodziejczyk, mówiąc, że cyberterroryzm polega na wykorzystaniu cyberprzestrzeni do działań terrorystycznych[4].

Ataki cyberterrorystyczne mogą być wymierzone w różne cele, które można jednak podzielić na trzy zasadnicze grupy[5]:

- informatyczne systemy wojskowe, przechowujące m.in. informacje o planowanych ruchach i rozmieszczeniu wojsk oraz broni, systemach łączności czy prowadzonych badaniach nad nowymi rodzajami uzbrojenia;
- informatyczne systemy państwowej infrastruktury krytycznej, czyli systemy: finansowe, wytwarzania i dystrybucji energii, telekomunikacyjne, transportowe;
- informatyczne systemy przedsiębiorstw, przechowujące informacje strategiczne, takie jak np.: dane o kontrahentach, stosowanych technologiach i pracach badawczo-rozwojowych, plany rozwoju, strategie marketingowe, dane finansowo-księgowe.

Szukając przyczyn zjawiska cyberterroryzmu, należy przyjrzeć się motywom działania terrorystów. Mają one zwykle charakter polityczny (promocja ideologii, postaw lub wartości politycznych; rywalizacja międzypaństwowa), religijny (promocja idei religijnych, nawracanie, walka z „niewiernymi", zemsta za obrazę religii), gospodarczy (kradzież istotnych danych biznesowych i technologii, zakłócenie ciągłości działania w celu uzyskania przewagi i korzyści ekonomicznych), ekonomiczny (spowodowanie strat w atakowanym obiekcie, wymuszenie okupu) i społeczny (protest przeciwko określonym problemom społecznym).

Natomiast odrębną kwestią jest próba wytłumaczenia, co sprawia, że grupy terrorystyczne wybierają cyberprzestrzeń do realizacji swoich przestępczych celów. Piotr Sienkiewicz wskazuje sześć podstawowych przyczyn, dla których terroryści przenoszą swoją aktywność do sfery cyber[6]:

---

[4] R. Kołodziejczyk, *Nowa odsłona terroryzmu – cyberterroryzm*, „Rocznik Bezpieczeństwa Międzynarodowego", 2017, wol. 11, nr 2, s. 149.

[5] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, Akademia Obrony Narodowej, Warszawa 2002, s. 21.

[6] P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009.

- niski koszt w porównaniu z działaniami z użyciem środków rzeczowych,
- transgraniczność oznaczająca łatwość dosięgnięcia celów w dowolnym miejscu na świecie,
- gwarancja całkowitej anonimowości napastników w sieci, co daje im możliwość manipulowania informacją oraz utrudnia państwom odparcie ataku,
- minimalne ryzyko wykrycia i udaremnienia przygotowywanego ataku,
- możliwość ataku na kluczowe systemy wrogiego państwa bez ofiar śmiertelnych (zarówno po stronie zamachowców, jak i poszkodowanych),
- większy efekt propagandowy.

W niniejszym opracowaniu przyjęto założenie, że ryzyko cyberterroryzmu ma cechy podobne do klasycznego terroryzmu, przez co te dwa ryzyka można traktować łącznie. Cyberterroryzm zawiera się w pojęciu terroryzmu, jest jego subkategorią. Analogia do ryzyka terrorystycznego, zdaniem autora, jest uzasadniona. Cyberatak, podobnie do ataku terrorystycznego, ma cechy ryzyka katastroficznego (niska częstość, wysoka dotkliwość strat), ryzyka dynamicznego (ewoluuje wraz z postępem technicznym i zmianami cywilizacyjnymi), ryzyka fundamentalnego (masowy zasięg działania) i ryzyka antropogenicznego (jest rezultatem celowego działania człowieka). Występowanie zamachów cyberterrorystycznych i terrorystycznych jest efektem zjawiska przestępczości zorganizowanej, a w skrajnych przypadkach – efektem rywalizacji państw narodowych[7]. W segmencie szkód katastroficznych można wręcz mówić o konwergencji tych dwóch rodzajów ryzyka. Coraz częściej narzędziem realizacji ataków terrorystycznych są systemy IT, a z drugiej

[7] Atak terrorystyczny na kluczowe obiekty w USA w 2001 r. spowodował interwencją zbrojną USA na terenie Afganistanu i Iraku. Analogicznie, administracja Prezydenta USA Donalda Trumpa przypisała odpowiedzialność za globalny atak ransomware *WannaCry* z 2017 r. hakerom pracującym na zlecenie rządu Korei Północnej, określając ten incydent jako akt wojny. Definiowanie poważnych cyberataków, inspirowanych przez rządy państw narodowych, jako wrogie działania wojenne zapowiedziały już USA, Unia Europejska i NATO. Źródło: P. Muncaster, *EU to declare cyber-attacks "Act of War"*, „Info-Security Magazine", 31.10.2017, https://www.infosecurity-magazine.com/news/eu-to-declare-cyber-attacks-act-of/ (dostęp: 2.09.2019).

strony – zasięg, motywy i dotkliwość ataków hakerskich przypomina zjawisko terroryzmu[8].

2. Skala zjawiska cyberterroryzmu na świecie i w Polsce

W okresie od 2014 do 2018 r. zanotowano łącznie 4340 ataków terrorystycznych na całym świecie[9]. Większość z nich (87%) miała miejsce na Środkowym Wschodzie, w Afryce Północnej, Azji Południowej i Afryce Subsaharyjskiej, podczas gdy w Europie odnotowano zaledwie 100 incydentów. Zamachy terrorystyczne kosztowały życie ponad 32 tys. ludzi, w tym 418 osób w Europie. Około połowa (54%) z wymienionej liczby zamachów spowodowała straty materialne, z czego 14% zdarzeń przyniosło poważne szkody o wartości przekraczającej 1 mln USD. Siedem ataków spowodowało jednostkowe straty ekonomiczne wynoszące ponad 10 mln USD. Najtragiczniejszym aktem terroru w tym okresie był zamach bombowy na rosyjski samolot linii MetroJet nad Egiptem w październiku 2015 r. Zginęły wszystkie 224 osoby na pokładzie[10].

O ile dane na temat terroryzmu są szeroko dostępne, dużo trudniej określić skalę zjawiska cyberterroryzmu. Brakuje globalnych danych przekrojowych pozwalających uchwycić dominujący trend. Częściej spotyka się opisy pojedynczych incydentów. Nie ma także konsensusu co do tego, które z nich kwalifikować jako cyberterroryzm. Często jest to kwestia subiektywnej oceny.

Największy jak dotąd cyberatak, który śmiało można określić jako cyberterror, to globalna kampania *ransomware WannaCry* w 2017 r., która przyniosła straty ekonomiczne szacowane na 4 mld USD[11]. Administracja Prezydenta

---

[8] *Global cyber terrorism incidents on the rise*, Marsh & McLennan Insights, 2018, https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html (dostęp: 2.09.2019).

[9] *Terrorism threat & mitigation report 2018*, Pool Re, 2018, https://trac.poolre.co.uk/tmr-2018/DataCentre (dostęp: 4.09.2019).

[10] *Katastrofa rosyjskiego samolotu na Półwyspie Synaj. Nikt nie przeżył wypadku*, Onet.pl, 31.10.2015 r., https://wiadomosci.onet.pl/swiat/egipt-katastrofa-rosyjskiego-samolotu-nikt-nie-przezyl-wypadku/z6zvv3 (dostęp: 4.09.2019).

[11] Na podstawie: *Total WannaCry losses pegged at $4 billion*, Reinsurance News, 25.09.2017 r., https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/ (dostęp: 14.08.2019).

USA Donalda Trumpa przypisała odpowiedzialność za ten atak hakerom pracującym na zlecenie rządu Korei Północnej.

W 2007 r. mieszkańcy Estonii przekonali się, że cyberataki mogą być narzędziem walki pomiędzy dwoma państwami. Decyzja władz Tallina o przeniesieniu pomnika Armii Czerwonej na obrzeża stolicy rozsierdziła Rosjan, którzy tłumnie manifestowali przed ambasadą Estonii w Moskwie. W międzyczasie nastąpiło hakowanie stron – parlamentu estońskiego, banków, ministerstw, gazet oraz innych mediów. Niewielkie państwo bałtyckie zmagało się z problemami przez kilkanaście dni. Usunięcie skutków kosztowało je kilkanaście milionów dolarów[12].

W połowie grudnia 2014 r. w mediach pojawiły się informacje o włamaniach do systemów komputerowych operatora południowokoreańskich elektrowni jądrowych *Korea Hydro and Nuclear Power Co Ltd*[13]. Do ataków hakerskich przyznał się jeden z użytkowników Twittera, który zażądał wyłączenia trzech reaktorów jądrowych starszej generacji. Użytkownik ten, który twierdził, że jest przywódcą mającej siedzibę na Hawajach grupy sprzeciwiającej się energetyce atomowej, zagroził, że jeśli reaktory nie zostaną wyłączone, to umieści w sieci kolejne dokumenty wykradzione operatorowi. Chociaż władze Korei Południowej zapewniają, że ich 23 reaktory atomowe są bezpieczne, wiadomość ta zelektryzowała cały świat, a wydarzenie to pokazało, jak wielkie zagrożenie stanowi cyberterroryzm.

Eksperci z brytyjskiej organizacji pozarządowej Information Security Forum przewidują, że cyberterroryzm stanie się głównym zagrożeniem już w 2020 r.[14] Spodziewana eskalacja tego zjawiska jest pochodną wzrostu podatności współczesnej gospodarki na zagrożenia cyfrowe. Ataki cyberterrorystyczne mogą prowadzić do wielorakich konsekwencji, zarówno finansowych, jak i niefinansowych, takich jak np.:

---

[12] *Największe ataki hakerskie w historii*, serwis informacyjny Orange, 8.04.2019, https://www.orange.pl/poradnik/twoj-internet/najwieksze-ataki-hakerskie-w-historii/ (dostęp: 4.09.2019).

[13] *Hakerski atak na elektrownie atomowe. „Poważna sytuacja"*, PAP, 23.12.2014, https://www.polskieradio24.pl/5/3/Artykul/1333485,Hakerski-atak-na-elektrownie-atomowe-Powazna-sytuacja (dostęp: 5.09.2019).

[14] *Cyberterroryzm już za dwa lata będzie głównym zagrożeniem*, Business Insider Polska, 1.04.2018, https://businessinsider.com.pl/wiadomosci/cyberterroryzm-glownym-zagrozeniem-juz-w-2020-roku/p2jql6x (dostęp: 4.09.2019).

- kradzież i przechwytywanie newralgicznych informacji,
- ujawnienie poufnych informacji (w tym danych osobowych),
- zniszczenie (usunięcie) danych o kluczowym znaczeniu,
- straty materialne,
- paraliż przedsiębiorstw prywatnych i instytucji państwowych,
- paraliż komunikacyjny,
- blokowanie stron internetowych,
- wzrost popularności i potencjału grup terrorystycznych.

Widmo cyberterroryzmu zagraża głównie mocarstwom, jednak atak może zostać skierowany również na średnie i małe kraje demokratyczne, które wykazują zaangażowanie w różnego rodzaju konflikty zbrojne, religijne czy gospodarcze. Polska jako sojusznik USA w walce z terroryzmem islamskim zalicza się do krajów potencjalnie zagrożonych, choć stopień tego zagrożenia jest trudny do oszacowania. Niepokoić może wysoka aktywność organizacji Państwa Islamskiego ISIS w cyberprzestrzeni[15].

3. Czy cyberterroryzm jest ubezpieczalny?

Stopień zagrożenia atakami terrorystycznymi, w tym cyberterroryzmem, wymaga zastosowania działań adekwatnych do zagrożeń typu katastroficznego. Zarządzanie katastrofami powinno opierać się na zintegrowanym podejściu obejmującym cały proces, na który składają się cztery etapy: zapobieganie, gotowość, reakcja i odbudowa[16]. Ważną rolę do odegrania ma tutaj również sektor ubezpieczeń, który zapewniając ochronę ubezpieczeniową w zakresie różnych ryzyk katastroficznych, może przyczynić się do złagodzenia negatywnego wpływu katastrof na państwo, jego gospodarkę i obywateli. Cyberterroryzm jest jednak ryzykiem, którego ubezpieczenie stanowi poważne wyzwanie, analogicznie do ryzyka terroryzmu. Obecnie na polskim rynku ubezpieczeń nie istnieje możliwość uzyskania ochrony ubezpieczeniowej

[15] *Pentagon pracuje nad izolacją ISIS w cyberprzestrzeni*, portal Euroislam.pl, 29.04.2016, https://euroislam.pl/pentagon-pracuje-nad-izolacja-isis-w-cyberprzestrzeni/ (dostęp: 4.09.2019).

[16] *Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Rada Europejska, (Dz. Urz. UE nr 2010/C 115 z dnia 4 maja 2010 r., s. 25).

przed ryzykiem cyberterroryzmu. Nawet specjalistyczne ubezpieczenia cybernetyczne nie obejmują tego ryzyka. Dlaczego tak się dzieje?

Naturalnym obszarem zastosowań ubezpieczeń są bowiem zdarzenia występujące stosunkowo często, generujące umiarkowane szkody, niezależne od siebie, których statystyczny rozkład prawdopodobieństwa jest stabilny w czasie i możliwy do określenia na podstawie dostępnych danych. Ryzyka katastroficzne, do których zalicza się terroryzm i cyberterroryzm, burzą ten porządek. Wypadki, takie jak atak terrorystyczny na ważne obiekty w USA w 2001 r. zachwiały globalnym rynkiem ubezpieczeniowym i reasekuracyjnym, doprowadzając do postawienia fundamentalnych pytań o ubezpieczalność takich ryzyk[17].

W 1982 r. Baruch Berliner sformułował kryteria ubezpieczalności ryzyka, które od tego czasu zyskały ogromne uznanie jako narzędzie analizy ryzyka w działalności ubezpieczeniowej[18]. Są one podzielone na trzy grupy – kryteria aktuarialne, rynkowe i społeczne. W kategorii aktuarialnej ryzyko zostanie zakwalifikowane jako ubezpieczalne, jeśli cechuje się niezależnością i losowością występowania, maksymalna suma ubezpieczenia będzie pod kontrolą ubezpieczyciela, a wartość oczekiwana szkody utrzyma się na umiarkowanym poziomie. Ryzyko powinno wykazywać cechy masowości i nieznaczny stopnień asymetrii informacji. Ryzyko cyberterroryzmu nie spełnia większości z tych wymogów. Zespół kryteriów rynkowych koncentruje się wokół składki ubezpieczeniowej i limitów odpowiedzialności. Parametry te powinny być ustalone na takim poziomie, aby pokryć oczekiwane wypłaty odszkodowań, nie narażając ubezpieczyciela na ryzyko niewypłacalności, a z drugiej strony – spełnić oczekiwania klientów odnośnie zakresu ochrony ubezpieczeniowej i akceptowalnej wysokości składki. Jeśli chodzi o ryzyko cyberterroryzmu, w warunkach zagrożenia wysokimi szkodami katastroficznymi koszt ubezpieczenia terrorystycznego musiałby być stosunkowo wysoki. Ostatnia grupa kryteriów B. Berlinera to kryteria społeczne. Stawiają one wymóg, by ochrona ubezpieczeniowa od danego ryzyka nie stała w sprzeczności z polityką publiczną, systemem prawnym, normami społecznymi. Ubezpieczenie

[17] A. Gray, *Cyber risks too big to cover, says Lloyd's insurer*, Financial Times, 5.02.2015, https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de (dostęp: 20.11.2018).

[18] B. Berliner, *Limits of Insurability of Risks*, Wyd. Prentice-Hall, Englewood Cliffs, New York 1982.

nie powinno stwarzać zachęt do dokonywania czynów niezgodnych z prawem lub niepożądanych społecznie. Wydaje się, iż ubezpieczenie terrorystyczne jest zgodne z tymi wytycznymi.

W sytuacji dyskusyjnej ubezpieczalności ryzyka terroryzmu Martin Eling i Werner Schnell[19] postulują przyjęcie przez państwo aktywnej roli stymulującej rynek ubezpieczeń terrorystycznych po to, by stworzyć możliwość ubezpieczenia szkód spowodowanych cyberterroryzmem. Kolejnym argumentem wspierającym ideę zaangażowania państwa w zapewnienie ubezpieczalności tych ryzyk jest fakt, iż podstawą zarządzania katastrofami przez Unię Europejską jest zasada odpowiedzialności państwa za zapewnienie swoim obywatelom koniecznej ochrony z myślą o istniejących rodzajach ryzyka i zagrożeniach[20].

Kontynuując powyższy wątek, należy w tym miejscu postawić pytanie, w jakiej formie państwo może uczestniczyć w komercyjnym rynku ubezpieczeń. Na podstawie obserwacji istniejących rozwiązań w zakresie asekuracji ryzyka i finansowania jego negatywnych skutków można wskazać kilka rozwiązań modelowych. Uporządkowane według rosnących nakładów finansowych ze strony budżetu państwa przedstawia się następująco[21]:

1. Brak zaangażowania państwa – szkody zostają pokryte przez odszkodowania ubezpieczeniowe, a osoby nieubezpieczone nie otrzymują żadnej rekompensaty od państwa. W realiach współczesnych ustrojów politycznych i systemów społeczno-gospodarczych panujących w większości rozwiniętych krajów świata to skrajne podejście do roli państwa ma niewielkie szanse praktycznej realizacji. Podstawą zarządzania katastrofami przez Unię Europejską jest bowiem zasada odpowiedzialności państwa za zapewnienie swoim obywatelom koniecznej ochrony przed różnymi zagrożeniami.
2. Państwo nakłada obowiązek ubezpieczenia od skutków katastrof, a poszkodowani, którzy nie wykupili ubezpieczenia, nie otrzymują

[19] M. Eling, W. Schnell, *What do we know about cyber risk and cyber risk insurance?*, „The Journal of Risk Finance", 2016, wol. 17 (5), s. 474–491.

[20] *Program sztokholmski…*, op. cit., s. 25.

[21] Na podstawie: V. Bruggeman, M. Faure, T. Heldt, *Insurance against catastrophe: Government stimulation of insurance markets for catastrophic events*, „Duke Environmental Law & Policy Forum", 2012, nr 23, s. 185–241, https://scholarship.law.duke.edu/delpf/vol23/iss1/6 (dostęp 27.08.2019), s. 384.

żadnej rekompensaty od państwa. Jako dodatkowe wsparcie mogą wystąpić w tej formie dopłaty do składek ubezpieczeniowych finansowane z budżetu państwa. Jest to rozwiązanie stosowane np. w segmencie ubezpieczeń rolnych w celu utrzymania kosztu ubezpieczeń na akceptowalnym dla rolników poziomie. Ubezpieczenia upraw i zwierząt gospodarczych od różnych ryzyk naturalnych są objęte systemem dopłat do składki również w Polsce[22]. Dzięki subsydiom tworzy się szansę rozwoju potencjału lokalnego rynku ubezpieczeń, co prowadzi m.in. do wzrostu świadomości ubezpieczeniowej i budowania dojrzałej kultury ryzyka. Należy jednak dążyć do stopniowego ograniczania dopłat, które zaburzają rynkowy system impulsów popytowo-podażowych[23].

3. Państwo jako pożyczkodawca ostatniej instancji – w razie wystąpienia poważnego incydentu rząd zapewnia dostęp do zwrotnych środków z budżetu państwa na pokrycie kumulacji roszczeń odszkodowawczych wobec sektora ubezpieczeń. Wykorzystane środki powinny zostać zwrócone w ciągu kilku kolejnych lat. Rozwiązanie to towarzyszy zwykle utworzeniu programu ubezpieczeń ryzyk katastroficznych, gdzie równorzędnym celem jest minimalizacja obciążeń dla budżetu państwa i podatników (np. pool reasekuracji ryzyka terroryzmu w Wielkiej Brytanii *Pool Re*). Z drugiej strony wiadomo jednak, że bez gwarancji państwa nie uda się zapewnić finansowania programu w razie zdarzeń ekstremalnych.
4. Państwo jako ubezpieczyciel bezpośredni – rząd może całkowicie przejąć asekurację ryzyka na zasadzie wyłączności, pozostawiając ewentualnie sektorowi prywatnych ubezpieczeń rolę uzupełniającą. Odpowiada wtedy za cały proces obsługi ubezpieczenia, samodzielnie ustalając stawki ubezpieczeniowe, procedury zawierania umów i warunki ubezpieczenia. Model ten jest często spotykany w krajowych systemach ubezpieczeń społecznych. W obszarze ubezpieczeń majątkowych należy do rzadkości, choć dobrym przykładem mogą tu być Izrael

[22] Zob. *ustawa z dnia 7 lipca 2005 r. o ubezpieczeniach upraw rolnych i zwierząt gospodarskich (Dz.U. 2017 poz. 2047 z późn. zm.)*.

[23] M.F. Grace, R.W. Klein, P.R. Kleindorfer, *Homeowners insurance with bundled catastrophe coverage*, „Journal of Risk and Insurance", 2004, wol. 71 (3), s. 351–379.

oraz Hiszpania. Rząd izraelski pokrywa szkody w mieniu powstałe wskutek aktów terroru ze środków zgromadzonych w specjalnym Funduszu Odszkodowawczym, który jest zasilany z części wpływów z podatków majątkowych. Wypłaty pokrywają w pełni nie tylko szkody bezpośrednie, ale także utracone korzyści[24]. Natomiast w Hiszpanii od 1941 r. działa państwowa instytucja ubezpieczeniowa *Consorcio de Compensacion de Seguros* (CCS), której zadaniem jest ubezpieczanie różnych ryzyk katastroficznych (przyrodniczych i antropogenicznych), znajdujących się w zakresie ochrony sprzedawanych przez sektor prywatny ubezpieczeń majątkowych i osobowych. CCS działa zatem w segmencie rynku, który nie jest atrakcyjny dla ubezpieczycieli komercyjnych z uwagi na zbyt wysokie ryzyko. Państwo, reprezentowane przez CCS, zapewniając nielimitowaną kwotowo ochronę (m.in. od ryzyka terroryzmu), stanowi niezwykle istotny element rynku ubezpieczeń. CCS nie korzysta z reasekuracji[25].

5. Państwo zapewnia *quasi*-finansowanie nadwyżkowe dla poszkodowanych, tj. rekompensuje szkody katastroficzne, które przekroczyły limity odpowiedzialności zapewniane przez ubezpieczycieli prywatnych.
6. Państwo jako reasekurator ostatniej instancji – zobowiązanie rządu (zazwyczaj wynikające z przepisów ustawy) do pokrycia szkód ubezpieczeniowych, zaistniałych w wyniku poważnej katastrofy, jeśli ich zagregowana wartość przekroczy ustalony pułap. Pula wsparcia rządowego może być limitowana z góry lub nieograniczona. W praktyce model ten występuje w powiązaniu z kompleksowym programem ubezpieczeń i reasekuracji ryzyka.
7. Państwo w pełni rekompensuje straty poszkodowanych – po wystąpieniu katastrofy państwo rozpoczyna procedurę zgłaszania szkód, ich szacowania i weryfikacji. Następnie tworzone są zbiorcze wykazy poszkodowanych, którym rząd za pośrednictwem wyznaczonych

[24] *National terrorism risk insurance programmes of OECD countries with government participation*, OECD International Platform on Terrorism Risk Insurance, 2019, https://www.oecd.org/daf/fin/insurance/Terrorism-Risk-Insurance-Country-Comparison.pdf (dostęp: 16.07.2019).

[25] *Terrorism risk insurance in OECD countries*, „Policy Issues in Insurance" Nr 9, 2005, Wyd. OECD, Paryż, s. 73.

instytucji przekazuje zapomogi i rekompensaty. System pomocy poszkodowanym może kierować się sformalizowanymi zasadami lub jedynie doraźnymi decyzjami uprawnionych władz. Na prawo do rekompensaty ze środków publicznych nie wpływa posiadanie własnej polisy ubezpieczeniowej.

W odniesieniu do zagrożeń terrorystycznych nie ma jednego, uniwersalnego rozwiązania. Wybór zastosowanego podejścia często uzależniony jest od czynników społeczno-politycznych, a nie ekonomicznych. Kierując się jednak kryterium ekonomicznym i rachunkiem opłacalności, należy poszukiwać takich rozwiązań, których wykorzystanie opiera się na racjonalnych przesłankach. W zarządzaniu ryzykami katastroficznymi przyjmuje się, że metoda ubezpieczeniowa należy do najbardziej efektywnych, a jednocześnie – przy spełnieniu warunków pełności i powszechności – także najbardziej skutecznych z punktu widzenia pewności kompensacji[26]. W dalszej części opracowania przyjęto zatem założenie o wyborze metody ubezpieczeniowej do finansowania ryzyka terroryzmu, a głównym celem dalszych rozważań będzie znalezienie optymalnego mechanizmu wsparcia ze strony państwa.

4. Partnerstwo publiczno-prywatne branży ubezpieczeń i państwa w ramach programów ubezpieczeń terrorystycznych

Przyjmowanie ryzyk i łączenie ich w jednorodne portfele (ang. *pooling risks*) jest istotą działalności ubezpieczeniowej i reasekuracyjnej. Im większy portfel, tym mniejsze sumaryczne ryzyko mierzone wariancją łącznej wartości szkód i niższa składka indywidualna, a prawdopodobieństwo ruiny ubezpieczyciela zmierza do zera. Pojedyncze towarzystwo ubezpieczeń ma jednak ograniczone możliwości rozbudowy portfela ryzyk, co wynika z posiadanej liczby klientów i udziału w rynku. Tam, gdzie rynek ubezpieczeń nie jest wystarczająco rozwinięty, jak ma to miejsce w przypadku ubezpieczeń cybernetycznych, szanse zbudowania odpowiednio licznego portfela są jeszcze mniejsze. Dlatego w uzasadnionych sytuacjach podejmuje się działania zaradcze mające na celu

[26] K. Jajuga, *Koncepcja ryzyka i proces zarządzania ryzykiem – wprowadzenie*, w: *Zarządzanie ryzykiem*, red. K. Jajuga, Wydawnictwo PWN, Warszawa 2007, s. 31.

zwiększenie portfela ubezpieczeń, a przez to stabilizację warunków funkcjonowania towarzystw ubezpieczeń w obszarze działalności technicznej. Mowa tu m.in. o tworzeniu pooli ubezpieczeniowych lub reasekuracyjnych[27], co może odbywać się z inspiracji państwa (a czasem i z jego bezpośrednim udziałem) jako rozwiązanie obligatoryjne lub dobrowolne, lub w sposób spontaniczny jako inicjatywa „oddolna" uczestników rynku ubezpieczeń. Istniejące na świecie poole ubezpieczeń obejmują ryzyka katastrof naturalnych, terroryzmu, awarii nuklearnych, szkód lotniczych, katastrof ekologicznych – a więc ryzyka, których ubezpieczalność jest problematyczna[28]. Poole ubezpieczeniowe stanowią często główną oś, wokół której budowane są narodowe programy ubezpieczeń katastroficznych, w szczególności dla ryzyk terrorystycznych.

Rozwiązaniem problemu niedostępności ubezpieczenia od ryzyka cyberterroryzmu może być powołanie publicznego poolu ubezpieczeniowego[29] z wielopoziomową strukturą finansowania wypłat odszkodowań, w tym z państwem w roli reasekuratora ostatniej instancji.

Ciężkoogonowy, prawoskośny rozkład ryzyka terrorystycznego stanowi poważne wyzwanie dla towarzystw ubezpieczeń w aspekcie gromadzenia środków własnych, które byłyby adekwatne do potencjalnych szkód katastroficznych. Stworzenie poolu ubezpieczeniowego pod egidą państwa może stanowić rozwiązanie tego problemu, choć wciąż pozostaje pewien stopnień ryzyka utraty wypłacalności[30]. Rzecz w tym, iż koncentrując się na finansowaniu ryzyka o rozkładzie ciężkoogonowym, publiczne poole ubezpieczeń

---

[27] Przez „pool ubezpieczeniowy (reasekuracyjny)" rozumie się porozumienie ubezpieczycieli (reasekuratorów) w celu kolektywnego pokrywania lub wyrównywania ryzyka ze wspólnego, scentralizowanego funduszu. Fundusz ten tworzony jest ze zdecentralizowanych składek wnoszonych przez wszystkich członków poolu. Członkowie poolu nie tracą swojej niezależności. Celem poolu jest zwiększenie pojemności ubezpieczeniowej (reasekuracyjnej) dostępnej na rynku. Por.: G. Kraut, *A fair pool sharing mechanism for illiquid catastrophe risk markets*, Munich Risk and Insurance Center Working Paper Nr 19, grudzień 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262574 (dostęp: 19.07.2019).

[28] *Different forms of cooperation between insurance companies and their respective impact on competition*, Komisja Europejska, Bruksela 2016, , http://ec.europa.eu/competition/sectors/financial_services/KD0216918ENN.pdf (dostęp: 19.07.2019), s. 6.

[29] Pisząc o poolu ubezpieczeniowym, autor jednocześnie ma na myśli pool reasekuracyjny. Jeśli taka konotacja nie zachodzi, będzie to wyraźnie wynikało z tekstu i logiki wywodu.

[30] P.R. Kleindorfer, R.W. Klein, *Regulation and Markets for Catastrophe Insurance*, w: M.R. Sertel, S. Koray (red.), *Advances in Economic Design*, Wydawnictwo Springer, Berlin 2003, s. 277.

katastroficznych są niemal predestynowane do zmagania się z deficytem środków własnych zwłaszcza wtedy, gdy ma miejsce zdarzenie ekstremalne lub trudny do przewidzenia wypadek o nierejestrowanej wcześniej skali (tzw. *black swan*)[31]. Większość istniejących pooli przynajmniej raz w swojej historii stanęła wobec sytuacji niedoboru funduszy na obsługę roszczeń, co wymagało dokapitalizowania ze środków publicznych[32]. To tłumaczy, dlaczego w narodowych programach ubezpieczeń różnych ryzyk katastroficznych tak ważnym uczestnikiem jest państwo, które przyjmuje na siebie realizację funkcji gwarancyjnej. Jej realizacja polega na przyjmowaniu przez państwo – w przypadkach uzasadnionych interesem społecznym – roli gwaranta zobowiązań ubezpieczeniowych lub reasekuratora ostatniej instancji dla szkód ekstremalnych. Jak trafnie zauważa George Priest, w obliczu strat katastroficznych (a takie może wyrządzić zamach cyberterrorystyczny) niemal zawsze uznaje się, iż ich wielkość i masowy charakter wymuszają jakąś formę reakcji rządu w ramach funkcji gwarancyjnej – czy to w formie pomocy *ex post*, czy też regulacji *ex ante*[33].

Jak dotąd w żadnym kraju nie został stworzony narodowy program ubezpieczeń *stricte* od ryzyka cyberterroryzmu. Natomiast obserwuje się, iż w niektórych krajach istniejące już wcześniej programy ubezpieczeń terrorystycznych zostają stopniowo poszerzane o to nowe ryzyko. Przykładem może być Wielka Brytania (Pool Re), Francja (GAREAT), Belgia, Hiszpania, RPA i Australia[34], jak również amerykański TRIP. Poniżej zostanie zamieszczona krótka prezentacja najważniejszych aspektów organizacji wybranych programów ubezpieczeń terrorystycznych z udziałem państwa. Będzie to dobry przyczynek do dyskusji nad kształtem przyszłego, rekomendowanego przez autora narodowego programu ubezpieczeń terroryzmu i cyberterroryzmu.

Po tragicznym ataku terrorystycznym z 11 września 2001 r. w USA w niektórych państwach powstały różnego rodzaju rozwiązania ubezpieczeniowe

---

[31] C. Kousky, R. Cooke, *Explaining the failure to insure catastrophe risks*, „The Geneva Papers on Risk and Insurance – Issues and Practice", 2012, wol. 37, s. 206–227.

[32] J. McAneney i in., *Government-sponsored natural disaster insurance pools: A view from down-under*, „International Journal of Disaster Risk Reduction", 2016, wol. 15, s. 1–9.

[33] G.L. Priest, *The government, the market, and the problem of catastrophic loss*, „Journal of Risk and Uncertainty", 1996, wol. 12, s. 219–237.

[34] *Cyber risk pool*, Europe Economics, 21.02.2017, Londyn, http://www.europe-economics.com/publications/cyber_risk_pool.pdf (dostęp: 2.07.2019).

z udziałem państwa[35] jako odpowiedź na zawieszenie ubezpieczalności ryzyka terroryzmu. Ich celem było – w zgodzie z interesem społecznym – podtrzymanie możliwości ubezpieczenia ryzyka terroryzmu. Wtedy powstał amerykański program *Terrorism Risk Insurance Program* (TRIP) zbudowany na zasadzie koasekuracji sektora prywatnego i rządu federalnego, co jest rzadko spotykanym rozwiązaniem. W programie tym nie występuje zasada wzajemności ryzyka pomiędzy towarzystwami ubezpieczeń, dlatego nie można go traktować jako klasyczny pool. W istocie TRIP to prosty mechanizm partycypacji państwa w finansowaniu ubezpieczonych strat. Udział własny pojedynczego towarzystwa ubezpieczeń w szkodach spowodowanych przez atak terrorystyczny wynosi 20% składki przypisanej brutto, a po przekroczeniu tego pułapu – rząd partycypuje w wypłaconych odszkodowaniach w 85%[36]. Uruchomienie wypłat z TRIP następuje dopiero wtedy, gdy ubezpieczone szkody całego sektora przekroczą 120 mln USD. Maksymalna wartość wypłaconych odszkodowań przez wszystkich ubezpieczycieli w ciągu roku kalendarzowego z tytułu ataku terrorystycznego nie może przekroczyć 27,5 mld USD[37] [NAIC 2019]. Dnia 27 grudnia 2016 r. amerykański Departament Skarbu wydał jednoznaczne wytyczne, zgodnie z którymi ubezpieczenia cybernetyczne mieszczą się w zakresie pojęcia „ubezpieczenie majątkowe i wypadkowe" (ang. *property and casualty insurance*), a tym samym podlegają ustawie o Ubezpieczeniu Ryzyka Terrorystycznego z 2002 r. (TRIA). Oznacza to również, że wszystkie polisy cybernetyczne, niezależnie od zakresu ochrony, zostały objęte publicznym programem ubezpieczeń terrorystycznych TRIP z rządowymi gwarancjami pokrycia roszczeń ubezpieczeniowych[38]. Towarzystwa ubezpieczeń z kolei zobowiązuje to do oferowania ubezpieczeń cybernetycznych obejmujących zakresem ochrony ryzyko cyberterroryzmu. Gdy wystąpi incydent uznany przez rząd federalny za akt terroryzmu[39], a z tytułu

[35] Australia, Belgia, Dania, Francja, Holandia, Niemcy, USA, Wielka Brytania.

[36] Według stanu na 2016 r. W kolejnych latach udział ten będzie stopniowo malał aż do 80%.

[37] Według stanu na 2016 r. W kolejnych latach kwota ta będzie stopniowo podnoszona aż do 37,5 mld USD w 2020 r.

[38] W 2020 r. rząd federalny pokryje 80% szkód ubezpieczeniowych przekraczających pułap 200 mln USD, jeśli doszło do nich w wyniku aktu terroryzmu (a także aktu cyberterroryzmu).

[39] Uznanie zdarzenia za akt terroru wymaga spełnienia następujących przesłanek: decyzja Sekretarza Skarbu, Sekretarza Bezpieczeństwa Wewnętrznego lub Prokuratora Generalnego, zagrożenie dla życia ludzkiego, mienia lub infrastruktury na terenie USA, łączna wartość

posiadanego przez poszkodowanego cyberubezpieczenia będzie przysługiwać wypłata odszkodowania, ciężar płatności całości lub części odszkodowania przejmie na siebie państwo w ramach TRIA.

Australijski Pool Reasekuracyjny (ARPC) to powołany przez rząd Australii na mocy ustawy o ubezpieczeniu terrorystycznym z 2003 r. (*Terrorism Insurance Act*) program reasekuracyjny zapewniający pokrycie ryzyka terroryzmu dla posiadaczy nieruchomości komercyjnych pod warunkiem, że wykupili oni ubezpieczenie mienia lub ubezpieczenie przerwy w działalności. Korzystanie z poolu jest dla towarzystw ubezpieczeń dobrowolne i wiąże się z opłatą stanowiącą ustaloną część składki ubezpieczeniowej (od 2,6% do 16,0% w zależności od lokalizacji przedmiotu ubezpieczenia). W momencie wystąpienia ataku terrorystycznego i po stwierdzeniu tego faktu przez rządowy dekret, ubezpieczone szkody podlegają finansowaniu w ramach wielopoziomowego Programu. Najniższe szkody pokrywa sam ubezpieczony w ramach franszyzy redukcyjnej. Następna warstwa obejmuje zagregowane straty zatrzymane przez całą branżę ubezpieczeniową do poziomu 200 mln USD. Po przekroczeniu tej granicy rozpoczyna się odpowiedzialność ARPC – najpierw w ramach udziału własnego do 285 mln USD, a potem w ramach programu retrocesji do górnego limitu 3,065 mld USD. Zatem można powiedzieć, że „grubość" warstwy reasekuracji zapewnianej przez ARPC wynosi ok. 3,3 mld USD. W razie poważnego ataku terrorystycznego szkody przekraczające powyższą kwotę, jednak nie wyższe niż 10 mld USD, pokrywa skarb państwa na mocy gwarancji wypłacalności Programu zawartej w ustawie[40].

Program Ubezpieczeń i Reasekuracji Ryzyka Aktów Terrorystycznych (GAREAT) został uruchomiony w 2002 r. we Francji w formie poolu reasekuracyjnego, do którego mogą należeć towarzystwa ubezpieczeń prowadzące ubezpieczenia majątkowe na rynku francuskim[41]. Dzieli się na dwa

szkód przekracza 5 mln USD. Źródło: *Terrorism Risk Insurance Program. Statutes, regulations and interim guidance*, U.S. Department of the Treasury, 2019, https://www.treasury.gov/about/organizational-structure/offices/Domestic-Finance/Financial-Institutions/TRIP/Pages/TRIP_regulations.aspx (dostęp: 19.08.2019).

[40] *Media fact sheet*, Australian Reinsurance Pool Corporation (ARPC), 2018, https://arpc.gov.au/wp-content/blogs.dir/3/files/2018/07/Media-Fact-Sheet-JULY-18.pdf (dostęp: 12.07.2019).

[41] W 2016 r. *GAREAT* liczył ok. 220 członków. Źródło: *France – Terrorism Risk Insurance Programme*, OECD, 2016, s. 5, https://www.oecd.org/daf/fin/insurance/France-Terrorism-Risk-Insurance-2016.pdf (dostęp: 14.07.2019).

podprogramy: obowiązkowy Program Reasekuracji Dużych Ryzyk[42] (suma ubezpieczenia 20 mln euro lub większa) oraz dobrowolny Program Reasekuracji Małych i Średnich Ryzyk[43] (suma ubezpieczenia poniżej 20 mln euro). Koncentrując uwagę na reasekuracji dużych ryzyk, warto pokazać strukturę finansowania szkód ubezpieczeniowych. Obejmuje ona trzy poziomy[44]:

1. Reasekuracja zapewniana wzajemnie przez członków poolu do poziomu 500 mln euro (łączne szkody ubezpieczeniowe w okresie jednego roku kalendarzowego) na zasadzie udziału własnego cedentów (tak więc GAREAT nie finansuje tych szkód).
2. Reasekuracja ryzyka pozyskana na rynku globalnym na bazie umowy nadwyżki szkód ponad priorytet wynoszący 500 mln euro, maksymalnie do limitu odpowiedzialności 2,66 mld euro (zatem „grubość" warstwy retrocesji wynosi 2,16 mld euro). W razie wypadku odszkodowania są wypłacane ze środków GAREAT zgromadzonych ze składek reasekuracyjnych.
3. Reasekuracja nadwyżki szkód ponad 2,66 mld euro[45] (w skali roku kalendarzowego), bez górnego limitu odpowiedzialności, zapewniana przez CCR[46] dzięki gwarancjom rządu francuskiego.

Składka reasekuracyjna pobierana przez Program od towarzystw ubezpieczeń wynosi od 12% do 18% składki ubezpieczeniowej. Warto przypomnieć, że we Francji ubezpieczenie terrorystyczne jest obowiązkowo dodawane do każdej umowy ubezpieczenia mienia od pożaru oraz do ubezpieczeń komunikacyjnych. Ubezpieczyciele należący do GAREAT mają obowiązek cedować wszystkie ryzyka ze swoich portfeli ubezpieczeń, dla których sumy ubezpieczenia są równe lub wyższe od 20 mln euro. Jest to zatem reasekuracja obligatoryjna[47].

---

[42] *GAREAT Large Risks Section.*

[43] *GAREAT Small- and Medium-Sized Risk Section.*

[44] *Membership of the 2019 GAREAT Large Risk pool (LR) and GAREAT Small and Medium-sized Risk pool (SMR) for Lloyd's Insurance Company S.A. (Lloyd's Brussels) and Lloyd's Underwriters*, Lloyd's Market Bulletin Nr Y5221, 2019, s. 6, https://www.lloyds.com%2F~%2Fmedia%2Ffiles%2Fthe-market%2Fcommunications%2Fmarket-bulletins%2F2018%2F12%2Fy5221.pdf (dostęp: 14.07.2019).

[45] Kwota ta odnosi się do łącznej wartości odszkodowań z programu GAREAT w wyniku jednego zdarzenia terrorystycznego.

[46] *Caisse Centrale de Réassurance*, tłum. Centralny Fundusz Reasekuracji.

[47] *France – Terrorism Risk…,* op. cit.

W Niemczech ryzyko terroryzmu można ubezpieczyć w specjalnie do tego powołanym z inicjatywy branży ubezpieczeniowej[48] towarzystwie ubezpieczeń *Extremus* AG. Jego klientami mogą stać się podmioty, które zawarły umowy ubezpieczenia mienia lub utraty zysku na sumę ubezpieczenia przekraczającą 25 mln euro. Firma działa nie tylko na rynku niemieckim, ale dzięki współpracy z syndykatami Lloyda oferuje ochronę od ryzyka terroryzmu na całym świecie. Pojemność ubezpieczeniowa *Extremus* wynosi 2,2 mld USD. Po wyczerpaniu tej puli, dalsze pokrycie zapewnia rząd federalny w postaci warstwy pokrycia o wartości 9 mld USD ponad priorytet 2,2 mld USD[49].

Brytyjski Pool Re działa na zasadzie towarzystwa reasekuracji wzajemnej, którego udziałowcami są zakłady ubezpieczeń. Powstał 1993 r. w odpowiedzi na falę zamachów bombowych w Wielkiej Brytanii organizowanych w latach 90. XX w. przez Irlandzką Armię Republikańską (IRA) jako pokłosie sporu o niezależność Irlandii Północnej. Wycofanie pokrycia dla ryzyka terroryzmu przez ubezpieczycieli i reasekuratorów, co potraktowano jako zagrożenie dla brytyjskiej gospodarki, zmusiło przedstawicieli branży ubezpieczeń i rządu do wspólnego poszukiwania nowych rozwiązań. Od początku swego istnienia Pool Re wypłacił odszkodowania z tytułu 13 ataków terrorystycznych na łączną kwotę 600 mln GBP, równocześnie nie obciążając w najmniejszym stopniu brytyjskich podatników. Finansowany z wpłacanych składek fundusz reasekuracyjny o wartości 6 mld GBP pozwala Pool Re na samodzielne pokrywanie szkód bez udziału państwa. Nawet gdyby w przypadku zdarzenia ekstremalnego konieczna była pomoc państwa w celu zapewnienia płynności poolu, w kolejnych latach zaangażowane środki publiczne powinny być zwrócone przez towarzystwa ubezpieczeń. Pool Re chroni nieruchomości komercyjne przed wszystkimi formami ryzyka terroryzmu bez względu na przyczynę, a więc działa na zasadzie „*all risks*". Niedawno doszło do rozszerzenia zakresu ochrony o cyberterroryzm[50].

Reasumując, w przypadku ryzyka terroryzmu najczęściej spotykanym rozwiązaniem są programy ubezpieczeniowe zbudowane na zasadzie poolu,

---

[48] Akcjonariuszami *Extremus* jest 15 towarzystw ubezpieczeń mających siedzibę w Niemczech.

[49] *Different forms of cooperation…,* op. cit., s. 184.

[50] *Annual Report 2018*, Pool Reinsurance Company Limited, 2019, https://www.poolre.co.uk/wp-content/uploads/2016/06/Pool-Re-Annual-Report-2018.pdf (dostęp: 15.07.2019).

tj. zrzeszające towarzystwa ubezpieczeń oferujące ubezpieczenia majątkowe z zakresem ochrony rozszerzonym o ryzyko terroryzmu. Z reguły mechanizm finansowania szkód terrorystycznych złożony jest z trzech zasadniczych warstw:

1. udział własny towarzystw ubezpieczeń[51], tj. część ryzyka niefinansowana przez program,
2. warstwa szkód finansowana przez program to zwykle reasekuracja lub retrocesja ryzyka na prywatnym rynku reasekuracyjnym dla szkód przekraczających udział własny aż do ustalonego górnego limitu odpowiedzialności[52],
3. warstwa szkód finansowana przez państwo, pełniące rolę reasekuratora ostatniej instancji.

Tabela 1. Struktura finansowania ryzyka w wybranych programach ubezpieczeń terroryzmu

Nazwa programu	Państwo	I warstwa: Udział własny ubezpieczycieli	II warstwa: Pool ubezpieczeń*	III warstwa: Państwo jako reasekurator ostatniej instancji*
Australian Reinsurance Pool	Australia	350 mln USD	2,9 mld USD	10,00 mld USD
Terrorism and Reinsurance Pool	Belgia	336 mln USD	785 mln USD	3,40 mld USD
Terrorism Insurance Pool for Non-Life Insurance	Dania	2,10 mld USD	brak	4,40 mld USD
GAREAT	Francja	560 mln USD	2,8 mld USD	bez ograniczeń
NHT	Holandia	336 mln USD	1,10 mld USD	1,12 mld USD
Extremus Versicherungs AG	Niemcy	brak	2,20 mld USD	11,20 mld USD
Terrorism Risk Insurance Program	USA	120 mln USD	brak	100 mld USD
Pool Re	Wlk. Brytania	310 mln USD	11,8 mld USD	bez ograniczeń

* górny limit odpowiedzialności

Źródło: na podstawie: *National terrorism risk…*, op. cit.

[51] Liczony indywidualnie dla poszczególnych towarzystw albo jako zagregowany udział własny całego rynku.

[52] Zazwyczaj w agregacie dla całego rynku ubezpieczeń w okresie jednego roku kalendarzowego.

W tabeli 1 przedstawiono strukturę finansowania ryzyka terroryzmu w wybranych programach ubezpieczeń. Pokazano poszczególne warstwy pokrycia ze wskazaniem górnych limitów odpowiedzialności. We wszystkich przypadkach państwo pełni rolę reasekuratora ostatniej instancji, biorąc na siebie odpowiedzialność finansową do określonej kwoty lub nieograniczoną.

Kończąc, warto odnotować, że programy australijski, brytyjski i francuski są klasycznymi poolami reasekuracyjnymi, gdzie w zamian za składkę reasekuracyjną wnoszoną *ex ante* pokrywana jest ustalona część odszkodowań. Z cedowanego ryzyka tworzy się portfel, w którym ubezpieczone szkody pokrywane są na zasadzie wzajemności. Zaletą pooli reasekuracyjnych jest stabilizacja rynku ubezpieczeń poprzez gwarancję wypłaty odszkodowań w razie wypadku ubezpieczeniowego, wsparcie poszkodowanych w odbudowie zniszczeń, minimalizacja negatywnego wpływu incydentu na gospodarkę, umożliwienie lepszego zrozumienia istoty ryzyka dzięki partnerstwu publiczno-prywatnemu, ograniczenie luki pokrycia ubezpieczeniowego, nadanie określonemu rodzajowi ryzyka odpowiedniej wagi i budowa świadomości istnienia problemu.

Przystępując do tworzenia programu ubezpieczeń katastroficznych, warto kierować się uznanymi rekomendacjami i wytycznymi, które formułowane na bazie wcześniejszych doświadczeń i dobrych praktyk pozwalają uniknąć typowych błędów. Zalecenia dla państwa pełniącego rolę reasekuratora w narodowym programie ubezpieczeń są następujące[53]:

- minimalizacja zakłóceń rynku ubezpieczeń – interwencja państwa powinna zostać podjęta po wcześniejszej analizie, czy rynek ubezpieczeń nie byłby w stanie funkcjonować prawidłowo bez udziału rządu;
- składki adekwatne do ryzyka – prawidłowo skalkulowane składki ubezpieczeniowe lub reasekuracyjne generują poprawne impulsy popytowe (ograniczenie ryzyka selekcji negatywnej), stymulują działania prewencyjne ubezpieczonych, nie podkopują pozycji konkurencyjnej podmiotów prywatnych w porównaniu z podmiotem publicznym;
- stymulacja ubezpieczeń komercyjnych – interwencja państwa powinna stymulować rozwój komercyjnego rynku ubezpieczeń i reasekuracji,

[53] V. Bruggeman, M. Faure, T. Heldt, *Insurance against catastrophe…*, op. cit., s. 422.

tak aby po ustaniu pomocy państwa był w stanie samodzielnie funkcjonować;
- dobrowolność reasekuracji – możliwość skorzystania z reasekuracji z udziałem państwa powinna być dobrowolna dla uczestników rynku ubezpieczeń;
- ograniczony horyzont czasu interwencji – interwencja państwa powinna mieć charakter tymczasowy, by nie zakłócać konkurencji.

5. Założenia autorskiej koncepcji narodowego programu ubezpieczeń terrorystycznych w Polsce

Na podstawie opisanych powyżej programów ubezpieczeń oraz uwzględniając specyfikę lokalnego rynku ubezpieczeń, proponuje się utworzenie Narodowego Programu Ubezpieczeń Terrorystycznych (NPUT) w Polsce. Idea powołania NPUT została oparta na następujących założeniach koncepcyjnych:
- Celem NPUT jest zapewnienie powszechności, pełności i realności ochrony ubezpieczeniowej w zakresie ryzyka terroryzmu i cyberterroryzmu[54] na polskim rynku ubezpieczeń, stworzenie możliwości reasekuracji ryzyka terrorystycznego, minimalizacja obciążeń budżetu państwa w razie wystąpienia aktu terroru, budowa świadomości zagrożeń i edukacja ubezpieczeniowa obywateli.
- NPUT dotyczy umów ubezpieczenia mienia, środków transportu i utraty zysku zawieranych przez podmioty gospodarcze, jednostki sektora finansów publicznych oraz osoby fizyczne, o ile przedmiot ubezpieczenia zlokalizowany jest na terytorium Polski.
- Zakres ochrony wskazanych powyżej rodzajów ubezpieczeń ma obligatoryjnie zawierać pokrycie szkód bezpośrednich spowodowanych ryzykiem terroryzmu i cyberterroryzmu[55].

[54] Dla uproszczenia, w dalszej części tekstu przyjęto, że pisząc o ryzyku terrorystycznym, autor jednocześnie ma na myśli ryzyko cyberterrorystyczne.

[55] W ramach Programu powinna być stosowane ujednolicone definicje terroryzmu i cyberterroryzmu, jak i inne definicje kluczowych pojęć dla określenia warunków ubezpieczenia.

- Tworzy się Publiczny Zakład Reasekuracji (PZR) z siedzibą w Warszawie, działający w formie towarzystwa reasekuracji wzajemnej[56], którego celem będzie oferowanie reasekuracji ryzyka terrorystycznego na zasadzie wzajemności dla zakładów ubezpieczeń będących członkami PZR. Fundusz reasekuracyjny PZR będzie finansowany ze składek jego członków, a w razie deficytu środków własnych spowodowanego wystąpieniem zdarzenia katastroficznego niedobór ten zostanie pokryty przez Skarb Państwa w formie nieoprocentowanej pożyczki (z opcją częściowego lub całkowitego umorzenia spłaty). PZR będzie zobowiązane prowadzić racjonalną gospodarkę finansową opartą na kalkulacji wysokości składek reasekuracyjnych w zgodzie z zasadami aktuariatu (składka adekwatna do poziomu ryzyka).
- Towarzystwa ubezpieczeń mogą dobrowolnie przystąpić do NPUT i skorzystać z reasekuracji ryzyka terroryzmu z gwarancjami państwa oferowanej przez PZR. Alternatywą będzie samodzielne zawarcie kontraktu reasekuracyjnego na rynku komercyjnym, jednak jest to równoznaczne z wystąpieniem towarzystwa ubezpieczeń z programu NPUT i pozbawienie dostępu do wsparcia ze strony państwa. Nie zwalnia to ubezpieczyciela z obowiązku oferowania ochrony ubezpieczeniowej dla ryzyka terroryzmu w przyjętym na mocy regulacji minimalnym zakresie.
- Struktura programu NPUT obejmuje trzy warstwy pokrycia. Warstwa pierwsza to udział własny poszczególnych ubezpieczycieli, a więc szkody pokrywane przez towarzystwa ze środków własnych, do wysokości ustalonego pułapu. Będzie on wyrażony jako łączna wartość wypłat odszkodowań z tytułu realizacji ryzyka terroryzmu w skali roku. Po przekroczeniu tego pułapu zostaje uruchomiona druga warstwa pokrycia, tj. reasekuracja nadwyżki szkód (tzw. *Excess-of-Loss reinsurance*) zapewniana przez PZR. Warstwa ta również będzie miała określony zagregowany górny limit odpowiedzialności w skali roku. W razie przekroczenia tego limitu, czyli w praktyce po wystąpieniu zamachu

[56] Towarzystwo reasekuracji wzajemnej jest dopuszczoną przez *ustawę z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2015 r. poz. 1844 ze zm.)* formą organizacyjno-prawną prowadzenia działalności reasekuracyjnej w Polsce.

o skali katastroficznej, nadwyżkę roszczeń ubezpieczeniowych pokryje państwo ze środków budżetowych. Odpowiedzialność państwa nie będzie limitowana.

6. Podsumowanie

Zaprezentowana koncepcja Narodowego Programu Ubezpieczeń Terrorystycznych ma charakter ramowy. Wiele szczegółów wymaga doprecyzowania po przeprowadzeniu konsultacji ze wszystkimi interesariuszami przyszłego programu. Pogłębionej analizy ekonomiczno-finansowej oraz aktuarialnej wymagają kwestie związane z analizą opłacalności przedsięwzięcia i jego parametryzacją, w szczególności od strony ubezpieczeniowej. Niemniej jednak celem tego opracowania było zainicjowanie debaty nad ważnym problemem finansowania negatywnych skutków terroryzmu i cyberterroryzmu, w obliczu spodziewanej eskalacji tych zagrożeń w niedalekiej przyszłości. Władze państwa polskiego, jak i sektor ubezpieczeń nie powinni przyjmować w tej sytuacji postawy biernego oczekiwania na to, co może się wydarzyć.

Na podstawie obserwacji rynku ubezpieczeń terrorystycznych można przypuszczać, iż zaangażowanie państwa powinno być ograniczone w czasie. Tuż po tragicznym ataku terrorystycznym na obiekty w USA w 2001 r. światowy rynek ubezpieczeń i reasekuracji całkowicie wycofał się z asekuracji tego ryzyka, co wymagało reakcji państw w postaci utworzenia publicznych programów ubezpieczeń terrorystycznych. Jednak po upływie blisko 20 lat widać wyraźnie, iż sytuacja na rynku ubezpieczeń zmieniła się na tyle, że kontynuacja interwencji państwa jest zbędna. Ubezpieczyciele akceptują coraz szersze *spectrum* ryzyka terroryzmu za coraz niższe stawki[57]. Należy przy tym jasno stwierdzić, iż opisana tu sytuacja nie powinna być interpretowana jako dowód na niecelowość interwencji państwa. Wręcz przeciwnie, bez zaangażowania państwa w krytycznym momencie nie byłby możliwy powrót do równowagi. W analogiczny sposób należy postrzegać motywy ewentualnej interwencji rządu na rynku ubezpieczeń cyberterroryzmu w Polsce – jako czasowy instrument stabilizacji warunków jego rozwoju.

[57] *Cyber risks and government pools. Too soon?*, Artemis, 30.03.2017, https://www.artemis.bm/news/cyber-risks-and-government-pools-too-soon/ (dostęp: 20.08.2019).

Reasumując, interwencja państwa na rynku ubezpieczeń nie powinna być kwestionowana bez rozpoznania stojących za nią uwarunkowań. Charakter wyzwań, z którymi musi się zmierzyć branża ubezpieczeniowa we współczesnym świecie, może oznaczać, iż aby im sprostać, pożądana będzie pewna forma rządowego wsparcia. Działając na zasadzie partnerstwa publiczno-prywatnego, każda ze stron wnosi takie zasoby materialne i niematerialne, w których posiada przewagę komparatywną, dzięki czemu ich wspólne przedsięwzięcie zyskuje unikalną wartość dodaną. Sektor ubezpieczeń może zwiększyć wolumen składki przypisanej oraz zapewnić asekurację trudnych i niedostatecznie rozpoznanych ryzyk, takich jak cyberterroryzm, a w dalszej perspektywie – przygotować się do samodzielnej obsługi danego segmentu rynku już bez wsparcia państwa.

Bibliografia

Annual Report 2018, Pool Reinsurance Company Limited, 2019, https://www.poolre.co.uk/wp-content/uploads/2016/06/Pool-Re-Annual-Report-2018.pdf (dostęp: 15.07.2019).

Berliner B., *Limits of Insurability of Risks*, Wyd. Prentice-Hall, Englewood Cliffs, New York 1982.

Bruggeman V., Faure M., Heldt T., *Insurance against catastrophe: Government stimulation of insurance markets for catastrophic events*, „Duke Environmental Law & Policy Forum", 2012, nr 23, s. 185–241, https://scholarship.law.duke.edu/delpf/vol23/iss1/6 (dostęp: 27.08.2019).

Cyber risk pool, Europe Economics, 21.02.2017, Londyn, http://www.europe-economics.com/publications/cyber_risk_pool.pdf (dostęp: 2.07.2019).

Cyber risks and government pools. Too soon?, Artemis, 30.03.2017, https://www.artemis.bm/news/cyber-risks-and-government-pools-too-soon/ (dostęp: 20.08.2019).

Cyberterroryzm już za dwa lata będzie głównym zagrożeniem, Business Insider Polska, 1.04.2018, https://businessinsider.com.pl/wiadomosci/cyberterroryzm-glownym-zagrozeniem-juz-w-2020-roku/p2jql6x (dostęp: 4.09.2019).

Denning D.E., *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, Washington, 23.05.2000, www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf (dostęp: 4.09.2019).

Different forms of cooperation between insurance companies and their respective impact on competition, Komisja Europejska, Bruksela 2016, http://ec.europa.

eu/competition/sectors/financial_services/KD0216918ENN.pdf (dostęp: 19.07.2019)

Eling M., Schnell W., *What do we know about cyber risk and cyber risk insurance?*, „The Journal of Risk Finance", 2016, wol. 17 (5), s. 474–491.

France – Terrorism Risk Insurance Programme, OECD, 2016, https://www.oecd.org/daf/fin/insurance/France-Terrorism-Risk-Insurance-2016.pdf (dostęp: 14.07.2019)

Global cyber terrorism incidents on the rise, Marsh & McLennan Insights, 2018, https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html (dostęp: 2.09.2019).

Grace M.F., Klein R.W., Kleindorfer P.R., *Homeowners insurance with bundled catastrophe coverage*, "Journal of Risk and Insurance", 2004, wol. 71 (3), s. 351–379.

Gray A., *Cyber risks too big to cover, says Lloyd's insurer*, Financial Times, 5.02.2015, https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de (dostęp: 20.11.2018).

Hakerski atak na elektrownie atomowe. „Poważna sytuacja", PAP, 23.12.2014, https://www.polskieradio24.pl/5/3/Artykul/1333485,Hakerski-atak-na-elektrownie-atomowe-Powazna-sytuacja (dostęp: 5.09.2019).

Jajuga K., *Koncepcja ryzyka i proces zarządzania ryzykiem – wprowadzenie*, w: *Zarządzanie ryzykiem*, red. K. Jajuga, Wyd. PWN, Warszawa 2007, s. 13–32.

Jędrzejewski M., *Analiza systemowa zjawiska infoterroryzmu*, Akademia Obrony Narodowej, Warszawa 2002.

Katastrofa rosyjskiego samolotu na Półwyspie Synaj. Nikt nie przeżył wypadku, Onet.pl, 31.10.2015 r., https://wiadomosci.onet.pl/swiat/egipt-katastrofa-rosyjskiego-samolotu-nikt-nie-przezyl-wypadku/z6zvv3 (dostęp: 4.09.2019).

Kołodziejczyk R., *Nowa odsłona terroryzmu – cyberterroryzm*, „Rocznik Bezpieczeństwa Międzynarodowego", 2017, wol. 11, nr 2, s. 149.

Kleindorfer P.R., Klein R.W., *Regulation and Markets for Catastrophe Insurance*, w: red. M.R. Sertel, S. Koray, *Advances in Economic Design*, Wyd. Springer, Berlin 2003, s. 263–279.

Kousky C., Cooke R., *Explaining the failure to insure catastrophe risks*, „The Geneva Papers on Risk and Insurance – Issues and Practice", 2012, wol. 37, s. 206–227.

Kraut G., *A fair pool sharing mechanism for illiquid catastrophe risk markets*, Munich Risk and Insurance Center Working Paper Nr 19, grudzień 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262574 (dostęp: 19.07.2019).

Lewis J., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington D.C. 2002.

Media fact sheet, Australian Reinsurance Pool Corporation (ARPC), 2018, https://arpc.gov.au/wp-content/blogs.dir/3/files/2018/07/Media-Fact-Sheet-JULY-18.pdf (dostęp: 12.07.2019).

Membership of the 2019 GAREAT Large Risk pool (LR) and GAREAT Small and Medium-sized Risk pool (SMR) for Lloyd's Insurance Company S.A. (Lloyd's

Brussels) and Lloyd's Underwriters, Lloyd's Market Bulletin Nr Y5221, 2019, https://www.lloyds.com%2F~%2Fmedia%2Ffiles%2Fthe-market%2Fcommunications%2Fmarket-bulletins%2F2018%2F12%2Fy5221.pdf (dostęp: 14.07.2019).

Muncaster P., *EU to declare cyber-attacks "Act of War"*, „Info-Security Magazine", 31.10.2017, https://www.infosecurity-magazine.com/news/eu-to-declare-cyber-attacks-act-of/ (dostęp: 2.09.2019).

Największe ataki hakerskie w historii, serwis informacyjny Orange, 8.04.2019, https://www.orange.pl/poradnik/twoj-internet/najwieksze-ataki-hakerskie-w-historii/ (dostęp: 4.09.2019).

National terrorism risk insurance programmes of OECD countries with government participation, OECD International Platform on Terrorism Risk Insurance, 2019, https://www.oecd.org/daf/fin/insurance/Terrorism-Risk-Insurance-Country-Comparison.pdf (dostęp: 16.07.2019).

Pentagon pracuje nad izolacją ISIS w cyberprzestrzeni, portal Euroislam.pl, 29.04.2016, https://euroislam.pl/pentagon-pracuje-nad-izolacja-isis-w-cyberprzestrzeni/ (dostęp: 4.09.2019).

Priest G.L., *The government, the market, and the problem of catastrophic loss*, „Journal of Risk and Uncertainty", 1996, wol. 12, s. 219–237.

Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli, Rada Europejska, (Dz. Urz. UE nr 2010/C 115 z dnia 4 maja 2010 r.).

Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009.

Terrorism threat & mitigation report 2018, Pool Re, 2018, https://trac.poolre.co.uk/tmr-2018/DataCentre (dostęp: 4.09.2019).

Terrorism risk insurance in OECD countries, „Policy Issues in Insurance" 2005, nr 9, Wyd. OECD, Paryż.

Terrorism Risk Insurance Program. Statutes, regulations and interim guidance, U.S. Department of the Treasury, 2019, https://www.treasury.gov/about/organizational-structure/offices/Domestic-Finance/Financial-Institutions/TRIP/Pages/TRIP_regulations.aspx (dostęp: 19.08.2019).

Total WannaCry losses pegged at $4 billion, Reinsurance News, 25.09.2017, https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/ (dostęp: 14.08.2019).

Ustawa z dnia 7 lipca 2005 r. o ubezpieczeniach upraw rolnych i zwierząt gospodarskich (Dz.U. 2017. poz. 2047 ze zm.).

Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. 2015 poz. 1844 ze zm.).

ROZDZIAŁ V

Internet rzeczy, sztuczna inteligencja i robotyka w transformacji przedsiębiorstw a potrzeba penalizacji nowych typów przestępstw – zakres regulacji

JOANNA TACZKOWSKA-OLSZEWSKA[1]

1. Wprowadzenie

Biorąc pod uwagę trendy w rozwoju światowej gospodarki, a w szczególności planowane w najbliższych latach kierunki działań inwestycyjnych przedsiębiorstw, konieczne wydaje się skupienie aktywności prawodawcy na zadaniach związanych z wykorzystaniem sztucznej inteligencji, robotyki i internetu rzeczy. Szacuje się, że zgodnie z rynkowymi prognozami w 2021 r. wydatki na rozwiązania bazujące na IoT (ang. *Internet of Things* – IoT) mogą wynieść 1,2 biliona USD[2]. Z badań wynika, że w perspektywie najbliższych 3 lat Internet Rzeczy (IoT) i sztuczna inteligencja (SI) będą głównymi nośnikami cyfrowych zmian w gospodarce i transformacji społecznej. Mniejsze znaczenie dla zmian w strategiach przedsiębiorstw i rozkładzie inwestycji posiada robotyka.

Z opinii przedsiębiorców prowadzących działalność gospodarczą w skali międzynarodowej wynika, że IoT będzie obszarem technologicznym, który odegra największą rolę w zmianie sposobu prowadzenia biznesu oraz

[1] Adwokat; doktor habilitowany, profesor Akademii Sztuki Wojennej w Warszawie, Kierownik Katedry Prawa Publicznego i Prywatnego w Instytucie Prawa ASzWoj. Specjalizuje się w problematyce dotyczącej ochrony i przetwarzania informacji, prawa mediów, bezpieczeństwa informacyjnego, ochrony danych osobowych, handlu elektronicznego i usług świadczonych drogą elektroniczną.

[2] *Sztuczna inteligencja i internet rzeczy głównymi nośnikami cyfrowych zmian w gospodarce*, 14.06.2018; http://www.outsourcingportal.eu/pl/sztuczna-inteligencja-i-internet-rzeczy-glownymi-nosnikami-cyfrowych-zmian-w-gospodarce

przemianie życia społecznego w ciągu następnych 3 lat[3]. Według niektórych prognoz możliwe jest, że już 2020 r. ok. 51% miejsc pracy zostanie zautomatyzowane – z wszelkimi tego konsekwencjami dla rynku pracy[4]. Z badań przeprowadzonych w 2019 r. na zlecenie Ministerstwa Cyfryzacji wynika, że ponad 50% firm z krajów G20 do 2021 r. zmodernizuje i otworzy na IoT swoje przemysłowe systemy kontroli produkcji, bez uwzględnienia obaw związanych z bezpieczeństwem IT lub bezpieczeństwem publicznym, co skłoni organy regulacyjne do stanowienia odpowiednich przepisów prawa. Kulminacyjny punkt adopcji IoT na świecie to 2020 r. Oznacza to, że Polska i krajowi przedsiębiorcy stoją przed ostatnią szansą dołączenia do wyścigu o najwyższą stawkę[5]. W Polsce słusznie zarazem podkreśla się, że IoT bez cyberbezpieczeństwa stanowi większe zagrożenie dla państwa niż rezygnacja z użycia IoT[6].

2. Istota Internetu rzeczy (IoT), sztucznej inteligencji (SI), robotyki – zakres projektowanych regulacji

Nie ma obecnie legalnej definicji żadnego ze wskazanych powyżej pojęć, a ponadto nie istnieją żadne spójne, jednolite regulacje, które normowałyby zasady rozwijania i korzystania ze sztucznej inteligencji, internetu rzeczy lub robotyki. Definicji tych pojęć nie zawierają także regulacje ponadnarodowe, w szczególności akty normatywne UE. Zarazem jednak wskazuje się,

[3] *Raport KPMG International pt. The Changing Landscape of Disruptive Technologies. Tech disruptors outpace the competition*, https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/06/pl-The-Changing-Landscape-of-Disruptive-Technologies-2018.pdf. Badanie objęło 767 członków zarządów firm działających w branży technologicznej z 15 najbardziej rozwiniętych gospodarek świata. W badaniu wzięli udział respondenci zarówno z dużych (33%), średnich (29%), jak i małych firm (28%), które dopiero rozpoczynają działalność technologiczną. Badanie zostało przeprowadzone w okresie listopad-grudzień 2017 r.

[4] *Raport MKinsey Global Institute*, cyt. za: F.M. Alexandre, *The Legal Status of Artificially Intelligent Robots*, s. 10; cyt. za: A. Chłopecki, *Sztuczna inteligencja – szkice prawnicze i futurologiczne*, Warszawa 2018; https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damrqgiydcni#tabs-metrical-info

[5] Perspektywy rozwoju branży IoT na świecie, w: *IoT w polskiej gospodarce, Raport Grupy Roboczej do spraw Internetu Rzeczy Przy Ministerstwie Cyfryzacji*, Warszawa 2019 r., s. 5.

[6] Ibid., s. 21.

że istnieje potrzeba stworzenia powszechnie akceptowanych i elastycznych definicji pojęć „robota" i „sztucznej inteligencji", tj. takich, które nie będą utrudniać innowacji[7]. Fundament tych definicji powinny stanowić prawa Asimova[8],jako prawa adresowane do projektodawców, producentów i operatorów robotów, w tym robotów z wbudowaną autonomią i możliwością samodzielnego uczenia się, ponieważ prawa te nie mogą zostać przekształcone w kod maszynowy[9].

Internet rzeczy i sztuczna inteligencja wymaga regulacji na dwóch płaszczyznach, tj. 1) wewnątrz przedsiębiorstwa (organizacji) – na płaszczyźnie ich planowania, wdrażania i stosowania w zakresie, w jakim inteligentne systemy i IoT mają służyć efektywności działania samego przedsiębiorstwa, a także 2) na płaszczyźnie oferowania tych systemów (SI, IoT) konsumentom, co stanowi *de facto* ich sprzedaż lub licencjonowanie, a uzyskane z tych czynności wynagrodzenia jest źródłem przychodu przedsiębiorstwa.

Internet rzeczy obejmuje nowe środowisko, w którym może dochodzić do wystąpienia nowych rodzajów przestępstw popełnianych przy użyciu nowych narzędzi. O ile zatem celem sprawcy, podobnie jak w przypadku wielu innych przestępstw, jest uzyskanie w szybkim czasie korzyści majątkowych albo wyrządzenie szkody, o tyle inny jest przedmiot i podmiot przestępstwa, a także inny jest jego charakter i inna będzie charakterystyka sprawcy przestępstwa.

Internet rzeczy i sztuczna inteligencja mogą być traktowane zarówno jako przedmiot i cel ataku (przestępstwa), jak również mogą zostać wykorzystane jako narzędzie służące popełnieniu przestępstwa, ale także jako instrument walki z przestępczością, a nawet narzędzie do zapobiegania popełnieniu przestępstw i wykrywania potencjalnych, tj. jeszcze nie popełnionych, a będących w fazie planowania przestępstw. W Chinach prowadzone są eksperymenty

---

[7] *Sprawozdanie zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))*, http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PL.html

[8] Robot nie może skrzywdzić człowieka ani przez zaniechanie działania dopuścić, aby człowiek doznał krzywdy. (2) Robot musi być posłuszny rozkazom człowieka, chyba że stoją one w sprzeczności z Pierwszym Prawem. (3) Robot musi chronić sam siebie, jeśli tylko nie stoi to w sprzeczności z Pierwszym lub Drugim Prawem (zob. „Zabawa w berka" (ang. Runaround), I. Asimov, 1943 r.) oraz (0) Robot nie może skrzywdzić ludzkości, lub poprzez zaniechanie działania doprowadzić do uszczerbku dla ludzkości.

[9] Zasady ogólne, ibid.

z wykorzystaniem SI do analizowania wzorów zachowań jednostek oraz całych grup ludzi w celu wykrywania anomalii, które mogą świadczyć o prawdopodobieństwie wystąpienia naruszenia prawa i uruchamiać reagowanie organów ścigania[10].

Przypuszcza się zarazem, że system SI może zostać wykorzystany do wspomagania ataków na systemy informatyczne. Zwraca się przy tym uwagę, że „obrońcy będą coraz bardziej polegać na sztucznej inteligencji, aby przeciwdziałać atakom i identyfikować podatności. Rozwijane wdrożenia i adaptacja 5G zacznie rozszerzać obszar powierzchni ataku. Wydarzenia oparte na IoT przeniosą się na nowe, bardziej niebezpieczne formy ataku. Atakujący będą coraz częściej przechwytywać dane w tranzycie. Ataki wykorzystujące łańcuch dostaw będą rosły pod względem częstotliwości i skutków"[11]. Jak na razie SI nie jest jeszcze powszechnie stosowana w przedsiębiorstwach. Jedynie 6% badanych twierdzi, że już wdrożyła na szeroką skalę rozwiązania AI w swoich organizacjach, 35% zamierza to zrobić w ciągu najbliższych 3 lat, a 23% nadal nie stworzyło konkretnych planów w tym zakresie.

Celem ataku jest, co do zasady, sfera dóbr niematerialnych obejmująca dane objęte ochroną prywatności, w tym dane osobowe, w szczególności dane o stanie majątkowych, preferencjach konsumenckich, wyznaniu, przyzwyczajeniach, nałogach, światopoglądzie oraz oczekiwaniach, a nawet planach i zamierzeniach. Dobra te stają się celem ataku, który niekiedy nie wymaga przemyślanych strategii ze strony sprawcy wykorzystującego podatności systemu.

Natura SI i IoT powoduje, że nie jest łatwe ustalenie sprawcy przestępstwa. Istotą działania tych systemów jest bowiem komunikowanie się maszyn między sobą bez udziału człowieka. Problematyczne może być zatem nie tylko wykrycie przestępstwa, ale także wskazanie podmiotu, któremu należy przypisać odpowiedzialność za jego popełnienie. O ile w żadnym z państw ustawodawca nie zdecydował się na przyznanie zdolności sądowej robotom, to jednak w niektórych państwach, jak w szczególności Belgii, Arabii

[10] M. Czapska, *Aspekty prawne związane z rozwojem sztucznej inteligencji*, w: *Przegląd Strategii Rozwoju Sztucznej Inteligencji na Świecie*, Warszawa 2018, www.digitalpoland.org

[11] M. Więckowska, *Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do UODO oraz ocena wagi naruszenie w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)*, https://uodo.gov.pl

Saudyjskiej, Chinach byty elektroniczne (roboty, maszyny) zostały obdarzone *quasi*-osobowością[12]

Jest to zatem dla ustawodawcy sytuacja nowa, kiedy to bezpośrednim sprawcą przestępstwa jest robot (maszyna), co jednak nie ułatwia określenia i wskazania podmiotu, któremu należy przypisać winę za jego popełnienie. Idealistyczne i odbiegające od realiów są zarazem twierdzenia, jakoby korzystanie z rozwiązań w pełni zautomatyzowanych nie było narażone na błędy i było w pełni bezpieczne. Dowodzi tego wypadek ze skutkiem śmiertelnym spowodowany przez pojazd autonomiczny w Arizonie w USA[13]. Samochód należał do firmy Uber Technologies, która przeprowadzała test swojego auta. W rok po wypadku stwierdzono, że nie istnieje możliwość postawienia komukolwiek z firmy Uber zarzutów karnych[14].

[12] Japonia przyznała prawo do stałego pobytu w Tokio sztucznej inteligencji o imieniu Mirai, który jest botem stworzonym na podobieństwo 7-letniego chłopca i nie ma sztucznego ciała. Sophia będąca sztuczną inteligencją otrzymała obywatelstwo Arabii Saudyjskiej. W Belgii, w urzędzie stanu cywilnego zarejestrowany został robot pod imieniem i nazwiskiem Fran Pepper (zob. M. Czapska, *Aspekty prawne…*, op. cit.).

[13] W marcu 2018 r. autonomiczny samochód należący do firmy Uber (Volvo XC90 SUV) potrącił przechodzącą ulicę kobietę, która na skutek odniesionych obrażeń zmarła w szpitalu. W momencie wypadku samochodem sterował znajdujący się na jego pokładzie komputer. Nie jest to pierwszy wypadek z udziałem autonomicznego samochodu, w którym zginął człowiek, ale pierwszy, w którym według dotychczasowych ustaleń winę ponosi autonomiczny samochód. W połowie 2017 r. w wypadku na Florydzie zginął kierowca pół-autonomicznego samochodu wyprodukowanego przez firmę Tesla. Jednak policja ustaliła wtedy ponad wszelką wątpliwość, że winę za ten wypadek ponosi kierowa samochodu. Włączył on bowiem funkcję autopilota i następnie nie wyłączył jej pomimo pojawienia się na desce rozdzielczej samochodu wielu ostrzeżeń, że w zaistniałej na drodze sytuacji należy ją wyłączyć. W efekcie samochód zderzył się z przyczepą ciężarówki i kierowca samochodu zginął (zob. J. Chustecki, *To może być pierwszy na świecie wypadek, w którym z winy autonomicznego samochodu zginął człowiek,* https://www.computerworld.pl/news/To-moze-byc-pierwszy-na-swiecie-wypadek-w-ktorym-z-winy-autonomicznego-samochodu-zginal-czlowiek,409950.html) (dostęp: 9.09.2019).

[14] W toku śledztwa okazało się, że w teorii układy samochodu miały aż 6 sekund, by zauważyć pieszą i uniknąć kolizji. Czułość systemów autonomicznych została jednak obniżona, by samochód nie reagował awaryjnym hamowaniem bez potrzeby. Nie jest jednak wykluczone, że oskarżona zostanie kobieta, która owej feralnej nocy siedziała na miejscu kierowcy autonomicznego samochodu. (Zob. T. Budzik, *Uber nie odpowie za śmiertelny wypadek. Auto jechało samo, więc nie ma kogo winić*, https://autokult.pl/33237,uber-nie-odpowie-za-smiertelny-wypadek-auto-jechalo-samo-wiec-nie-ma-kogo-winic) (dostep: 9.09.2019).

3. Odpowiedzialność prawna

Na gruncie projektowanych rozwiązań prawnych w UE wskazuje się, że odpowiedzialność prawna wynikająca ze szkodliwej działalności robota staje się kwestią centralną[15]. Prawodawca europejski – jak się wydaje – prezentuje pogląd, zgodnie z którym maszyny mogą posiadać „cechy autonomii i zdolności poznawczych, np. zdolności uczenia się poprzez doświadczenia i zdolności podejmowania quasi-niezależnych decyzji – przypominają one coraz bardziej podmioty, które wchodzą w interakcje z otoczeniem i są zdolne do zmieniania go w sposób istotny"[16]. Zastosowanie takich rozwiązań może pojawiać się w różnych płaszczyznach działania zarówno przedsiębiorstw, jak również organów administracji, a nawet na płaszczyźnie sądowniczej[17]. Roboty nowej generacji mogą być wyposażone w zdolność dostosowywania się i uczenia się, z czym wiąże się pewien stopień nieprzewidywalności ich zachowania, gdyż będą one w sposób niezależny uczyć się, opierając się na własnych, zróżnicowanych doświadczeniach i wchodzić w interakcje z otoczeniem w jedyny w swoim rodzaju i nieprzewidywalny sposób[18].

Za dopuszczalne na gruncie projektowanych w UE rozwiązań przyjmuje się także, że mogą zdarzać się sytuacje, gdy nie będzie możliwe ustalenie sprawcy czynu i przypisanie mu odpowiedzialności wówczas, gdy do zdarzenia dochodzi z udziałem maszyn[19]. Prawodawca unijny składnia się w takich wypadkach do ustanowienia zasady ponoszenia odpowiedzialności przez

---

[15] *Odpowiedzialność, Sprawozdanie zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))*, http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PL.html

[16] Ibid., s. 5.

[17] Estonia do końca tego roku planuje wdrożenie sztucznej inteligencji w pierwszej instancji sądownictwa cywilnego w sprawach, w których wartość przedmiotu sporu nie przekracza 7 tys. euro (zob. K. Żaczkiewicz-Zborska, *Sztuczna inteligencja wyręczy sędziów*, https://sip.lex.pl/#/external-news/1795580242?keyword=Sztuczna%20inteligencja%20wyr%C4%99czy%20s%C4%99dzi%C3%B3w&cm=SFIRST) (dostęp: 9.09.2019).

[18] Ibid., s. 8.

[19] Ustawodawca unijny wskazuje bowiem, że „niezbędne stają się nowe zasady i przepisy w celu zapewnienia jasności co do odpowiedzialności prawnej różnych podmiotów odnośnie do odpowiedzialności za działania i zaniechanie działania przez roboty, w przypadku gdy przyczyny nie można prześledzić i w efekcie przypisać konkretnemu podmiotowi, którym jest człowiek". Ibid., s. 7.

producentów, operatorów, właścicieli i użytkowników na zasadzie ryzyka za działanie lub zaniechanie działania przez robota[20].

W projektowanych rozwiązaniach na płaszczyźnie prawa UE przyjmuje się, że odpowiedzialność ta powinna być proporcjonalna do poziomu instrukcji, jakie wydano robotowi, i stopnia jego autonomii, a zatem im dany robot ma większą zdolność uczenia się lub większą autonomię i im dłużej trwało jego „szkolenie", tym większa odpowiedzialność powinna spoczywać na osobie prowadzącej szkolenie. Zauważa się w szczególności, że poszukując osoby, która jest rzeczywiście odpowiedzialna za szkodliwe zachowanie robota, nie należy mylić umiejętności wynikających ze „szkolenia" robota z umiejętnościami zależącymi ściśle od zdolności robota do samodzielnego uczenia się. Przyjmuje się, że przynajmniej na obecnym etapie odpowiedzialność musi spoczywać na człowieku, a nie na robocie, co jednak nie wyłącza stosowania rozwiązań przeciwnych[21].

Za dopuszczalne przyjmuje się nadanie robotom statusu osób elektronicznych, który byłby porównywalny ze statusem osób fizycznych, a w konsekwencji pozwalał na przypisanie odpowiedzialności prawnej robotowi, a nie człowiekowi. Proponuje się w szczególności stworzenie systemu ubezpieczeń obowiązkowych dla robotów; utworzenie dla nich specjalnego funduszu odszkodowawczego; umożliwienie producentowi, programiście, właścicielowi lub użytkownikowi robota korzystania z ograniczeń odpowiedzialności, jeżeli płacą oni składki na fundusz odszkodowawczy; zapewnienie widoczności powiązania pomiędzy robotem a jego funduszem, a także „nadanie robotom specjalnego statusu prawnego w perspektywie długoterminowej, aby przynajmniej najbardziej rozwiniętym robotom autonomicznym można było nadać status osób elektronicznych odpowiedzialnych za naprawianie wszelkich szkód, jakie mogłyby wyrządzić, oraz ewentualne stosowanie osobowości elektronicznej w przypadkach podejmowania przez roboty autonomicznych decyzji lub ich niezależnych interakcji z osobami trzecimi"[22].

---

[20] Ibid., s. 8.

[21] *Sprawozdanie zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))*, http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PL.html, s. 19.

[22] Ibid.

Należy zwrócić uwagę, że zaproponowana na gruncie projektowanych rozwiązań odpowiedzialność oparta na zasadzie ryzyka nie może znaleźć zastosowania na gruncie prawa karnego. Brak precyzyjnych regulacji dotyczących zasad ponoszenia odpowiedzialności za działania lub zaniechania maszyn, a przede wszystkim brak jednoznacznego określenia podmiotu, któremu należy przypisać winę, rodzi ryzyko dekryminalizacji, a nawet depenalizacji określonych kategorii czynów wówczas, gdy do popełnienia czynu dochodzi za pośrednictwem lub z udziałem maszyn (robotów).

Internet rzeczy jest w literaturze definiowany jako sieć połączonych ze sobą przedmiotów (takich jak urządzenia mobilne, artykuły gospodarstwa domowego, samochody czy gadżety elektroniczne), które wykorzystując łączność internetową, są w stanie współdziałać ze sobą i komunikować się z innymi systemami[23]. Termin sztuczna inteligencja odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie –w celu osiągnięcia konkretnych celów[24]. Rozwój SI wymaga ogromnej ilości danych. Uczenie się maszyn, które stanowi jeden z rodzajów SI, polega na identyfikacji prawidłowości istniejących w dostępnych danych, a następnie zastosowaniu tej wiedzy w odniesieniu do nowych danych[25]. Im zbiór danych jest większy, tym lepiej SI może się uczyć i znajdować w danych nawet bardzo subtelne powiązania[26].

---

[23] M. Sakowska-Baryła, *Prywatność w inteligentnym mieście*, w: G. Szpor (red.), *Internet rzeczy. Bezpieczeństwo w Smart City*, Warszawa 2015, s. 136.

[24] *Komunikat Komisji Do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów. Skoordynowany plan w sprawie sztucznej inteligencji, COM(2018) 237 i COM(2018) 795 z dnia 7.12.2018 r.*, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-795-F1-PL-MAIN-PART-1.PDF

[25] Uczenie głębokie SI stanowi punkt zwrotny, który pozwolił maszynom na rozpoznawanie obrazu lub mowy bądź tłumaczenie maszynowe. Przeszkolenie algorytmu głębokiego uczenia w celu sklasyfikowania obiektów polega na skonfrontowaniu go z dużą liczbą oznakowanych przykładów (np. obrazków) o poprawnej kategoryzacji (np. obrazki samolotów). Po przeszkoleniu algorytmy mogą poprawnie klasyfikować obiekty, których nigdy nie widziały, w niektórych przypadkach z dokładnością większą niż ludzie. Dzięki wykorzystaniu dużych zbiorów danych i niespotykanej dotąd mocy obliczeniowej dokonano znacznego postępu w tych technologiach (*Komunikat Komisji Do Parlamentu Europejskigo, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Sztuczna inteligencja dla Europy z dnia 25.04.2018r., COM(2018) 237*, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-237-F1-PL-MAIN-PART-1.PDF s. 11).

[26] *Komunikat Komisji Do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów. Skoordynowany plan w sprawie*

Priorytetowe znaczenia ma bezpieczeństwo danych osobowych w szczególności oparte na zasadach wskazanych w RODO[27]. Komisja Europejska uznaje, że rozwój gospodarczy wymaga, by w UE zostały utworzone „wspólne europejskie przestrzenie danych w szeregu obszarów, takich jak produkcja lub energia (…) Celem tych wspólnych europejskich przestrzeni danych będzie agregacja danych, zarówno dla sektora publicznego, jak i danych wymienianych między przedsiębiorstwami, w całej Europie i udostępnianie ich na użytek szkolenia sztucznej inteligencji"[28].

Internet rzeczy jest definiowany przy użyciu co najmniej trzech perspektyw, tj. 1) perspektywy technologicznej, gdzie IoT jest rozumiany jako „sieć łącząca przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym (niewymagającym zaangażowania człowieka) działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych lub wchodzenia w interakcje z otoczeniem pod wpływem tych danych"[29]; 2) perspektywy architektonicznej, gdzie IoT jest definiowany jako „koncepcja architektury informatycznej, która umożliwia współpracę (interoperacyjność) różnorodnych systemów teleinformatycznych wspierających rozmaite zastosowania dziedzinowe i jest oparta na następujących warstwach: sprzętu, oprogramowania, komunikacji i integracji"[30], a także 3) perspektywy biznesowej, gdzie pojęcie to jest definiowane jako ekosystem usług biznesowych, wykorzystujących przedmioty zdolne do zbierania i przetwarzania informacji (interakcji), połączone w sieć, zapewniające interoperacyjność i synergię zastosowań"[31].

Należy podkreślić – co posiada dużą doniosłość na gruncie stanowienia i stosowania prawa – że IoT, w rozumieniu najbardziej zbliżonym do praktyki działania przedsiębiorców i korporacji – stanowi, jak wskazano powyżej

---

sztucznej inteligencji, COM(2018) 237 i COM(2018) 795 z dnia 7.12.2018 r., https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-795-F1-PL-MAIN-PART-1.PDF, s. 5.

[27] *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.U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).*

[28] *Komunikat Komisji Do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Skoordynowany plan…*, op.cit.

[29] Definicja Internetu Rzeczy, w: *IOT w polskiej gospodarce, Raport Grupy Roboczej do spraw Internetu Rzeczy Przy Ministerstwie Cyfryzacji*, Warszawa 2019, s. 5.

[30] Ibid.

[31] Ibid.

„ekosystem usług". Struktura i działanie IoT jest bowiem oparte na wymianie usług (danych, informacji, zleceń, komend) drogą elektroniczną pomiędzy powiązanymi ze sobą urządzeniami, przy czym ścieżkę wymiany usług określa program komputerowy lub aplikacja dedykowana dla konkretnych urządzeń i ich użytkowników.

Internet rzeczy oznacza zatem sieć powiązanych ze sobą usług świadczonych w obrębie zamkniętego systemu, którego częścią są przedmioty zdolne do odbierania komunikatów i korzystania z danych przesyłanych za pośrednictwem systemu informatycznego połączonego z publiczną siecią internet. Internet rzeczy jako ekosystem usług świadczonych za pośrednictwem systemu teleinformatycznego wymaga zagwarantowania poziomu bezpieczeństwa adekwatnego do ryzyka związanego z naruszeniem ciągłości tych usług lub poufności danych. Korzystanie z IoT na skalę globalną, jak zauważono w literaturze, wiąże się z naruszeniem cyberbezpieczeństwa, a w szczególności z masowym dostępem do danych zbieranych przez urządzenia, naruszeniem bezpieczeństwa tych danych (w tym również ich kradzieżą), ryzykiem przejęcia kontroli nad przedmiotami IoT przez osoby nieuprawnione czy z tzw. DoS (ang. *denial-of-service*), czyli takim atakiem na system komputerowy lub usługę sieciową, który ma za zadanie uniemożliwić jej dalsze działanie[32].

Podmioty oferujące usługi z zakresu IoT posiadają zatem status dostawców usług cyfrowych i mogą ponosić odpowiedzialność za jakość tych usług, a także szkody powstałe w wyniku ich wadliwego wykonania. Pomimo jednak tego, że status dostawców usług cyfrowych został unormowany w art. 17 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa[33], to jednak do przedsiębiorców korzystających z IoT lub oferujących towary z wykorzytaniem tej technologii nie znajdą zastosowania przepisy tej ustawy. Trzeba bowiem mieć na uwadze, że w myśl art. 2 pkt. 15 u.s.c. wskazane w ustawie i nałożone na dostawców usług cyfrowych obowiązki dotyczą wyłącznie tych rodzajów usług cyfrowych, które zostały wskazane w załączniku nr 2 do ustawy, tj. 1) usługi internetowej platformy handlowej – usługę, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną

[32] E. Siemaszkiewicz, *Internet Rzeczy – wyzwania cyberbezpieczeństwa*, „EP", 2018, nr 1, s. 51.

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

z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową; 2) usługę przetwarzania w chmurze, która umożliwia dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników; 3) usługa wyszukiwarki internetowej, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem[34].

Należy zarazem wskazać, że przedsiębiorca będący dostawcą IoT, wówczas gdy zapewnia on usługobiorcom (klientom, konsumentom) dostęp do ekosystemu usług elektronicznych, świadczonych na odległość, opartych na rozwiązaniach zawartych w dedykowanym konkretnym urządzeniom i użytkownikom oprogramowaniu, posiada status usługodawcy w rozumieniu ustawy oświadczeniu usług drogą elektroniczną[35], a w konsekwencji może niekiedy zostać pociągnięty do odpowiedzialności prawnej na gruncie tej ustawy[36].

4. Bezpieczeństwo nowych technologii

Stosowanie rozwiązań z zakresu IoT w działalności organizacji rodzi nie tylko potrzebę normowania standardów bezpieczeństwa oraz ustalenia podstawy faktycznej i prawnej odpowiedzialności ponoszonej przez przedsiębiorców za szkody wyrządzone tą technologią, w szczególności wówczas, gdy była ona wadliwa, ale także rodzi potrzebę normowania stosunków pracy istniejących

[34] J. Taczkowska-Olszewska, *Komentarz do art. 2 pkt. 15*, w: W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, s. 75.

[35] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz.U. 2019 poz. 123 z późn. zm.)*.

[36] J. Taczkowska-Olszewska, *Komentarz do art. 2*, w: J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, s. 67–68.

pomiędzy przedsiębiorcą a personelem, któremu zostają powierzone zadania z zakresu projektowania nowych rozwiązań informatycznych.

Wykorzystanie przez przedsiębiorcę internetu rzeczy wymaga co najmniej: 1) posiadania wysoko wykwalifikowanego personelu posiadającego umiejętności w zakresie tworzenia oprogramowania i aplikacji, a także agregowania i selekcji danych (data base); 2) zarządzania prawami autorskimi, rozporządzania prawami do oprogramowania oraz udzielania na nie licencji; 3) posiadania zabezpieczeń odpowiednich do ryzyka naruszeń związanych z korzystaniem z usług.

Zważywszy, że opracowanie programu lub aplikacji wymaga wkładu twórczego w powstanie określonych rozwiązań technicznych, a ponadto mając na uwadze, że rozwiązania te już na etapie ich projektowania powinny uwzględniać wymagania dotyczące standardu ochrony prywatności użytkowników i poufności danych osobowych, na przedsiębiorcy ciąży obowiązek takiego kształtowania treści stosunków prawnych łączących go z jego kontrahentami oraz zatrudnionymi osobami, dzięki którym będzie on zdolny wykazać, że jest w stanie przewidzieć zagrożenia i przeciwdziała ich powstawaniu na wszystkich etapach produkcji, począwszy od fazy projektowej, a skończywszy na wdrożeniu i stosowaniu oferowanych konsumentom rozwiązań.

Nie jest zarazem bez znaczenia ustalenie, że przedsiębiorca oferujący dostęp do usług z dziedziny IoT posiada, co do zasady, status administratora danych osobowych w rozumieniu art. 4 pkt. 7 RODO. W myśl zawartej tam definicji administrator danych osobowych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Na administratorze ciąży obowiązek uwzględniania ochrony danych w fazie projektowania oraz obowiązek zapewniania domyślnej ochrony danych (art. 25 RODO). By móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi

tworzenia i doskonalenia zabezpieczeń. Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych (motyw 78 RODO).

Rozwiązania z zakresu IoT są wykorzystywane przede wszystkim do monitorowania i inteligentnego sterowania procesami produkcyjnymi, podczas gdy roboty wspomagają pracę człowieka w realizacji coraz większej liczby powtarzalnych czynności, zapewniając oszczędności kosztowe przy jednoczesnej poprawie wydajności i jakości wykonywanej pracy. Natomiast SI w połączeniu z analityką danych umożliwia szybkie i skuteczne rozwiązywanie bardzo złożonych problemów, wykorzystując mechanizmy uczenia, które do tej pory były wykorzystywane wyłącznie przez żywe organizmy[37]. Jak wynika z przeprowadzonych w 2018 r. badań, aż 85% prezesów firm na świecie oczekuje, że SI w ciągu pięciu lat radykalnie zmieni ich biznes, a prawie dwie trzecie uważa, że to wciąż nowe zjawisko będzie miało większy wpływ na gospodarkę niż wynalezienie internetu. Podobnego zdania są także liderzy biznesowi w regionie Europy Środkowo-Wschodniej[38].

Największy wpływ na konieczność zmiany tradycyjnych modeli biznesowych i dostosowania się do nowych reguł mają tzw. cyfrowi agregatorzy, którzy świadczą swoje usługi na masową skalę. Alibaba, Facebook, Airbnb, Amazon oraz Google są uznawane za czołowych przedstawicieli tego typu

[37] Raport KPMG International *The Changing Landscape of Disruptive Technologies. Tech disruptors outpace the competition*, https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/06/pl-The-Changing-Landscape-of-Disruptive-Technologies-2018.pdf

[38] *Coraz więcej pesymistów wśród prezesów firm na świecie*, omówienie badaniu PwC, 6.02.2019; https://www.pwc.pl/pl/media/2019/2019-01-25-pwc-22-global-ceo-survey.html (dostęp: 9.09.2019).

organizacji[39]. Firmy te specjalizują się w obsłudze cyfrowych klientów, mają przewagę technologiczną dzięki wykorzystaniu zaawansowanych technologii cyfrowych. Korzystają z chmur obliczeniowych, płatności cyfrowych, analityki danych czy SI. Dodatkowo posiadają kapitał, który mogą przeznaczyć na rozwój i inwestycje związane z wejściem w nowe obszary biznesowe[40]. Jako najbardziej dotkliwe ograniczenie wpływające na rozwój i dochodowość przedsiębiorstw wskazywano w prowadzonych w 2018 r. przez KPMG badaniach na regulacje branżowe lub chroniące konsumentów. Inne przeszkody zidentyfikowane przez respondentów badania KPMG to niewystarczająca dostępność specjalistów (22% wskazań), a także brak standardów technicznych oraz ograniczenia istniejących systemów cyfrowych (21%)[41].

Na gruncie ustawodawstwa międzynarodowego wskazuje się nie tylko na potrzebę ustanowienia i wdrożenia przepisów powszechnie obowiązującego prawa w zakresie standardów dotyczących przedsiębiorców w związku z zastosowaniem nowych technologii, ale także ustanowienie kanonu powszechnie obowiązujących zasad etycznych. Ramy etyczne pełniące rolę wytycznych powinny opierać się na zasadzie przynoszenia korzyści, nieszkodliwości, autonomii i sprawiedliwości oraz na zasadach i wartościach zapisanych w art. 2 Traktatu o Unii Europejskiej oraz w Karcie praw podstawowych Unii Europejskiej, takich jak godność ludzka, równość, sprawiedliwość i równouprawnienie, brak dyskryminacji, świadoma zgoda, ochrona życia prywatnego i rodzinnego oraz ochrona danych[42]

W komunikatach z dnia 25 kwietnia 2018 r. i z dnia 7 grudnia 2018 r. Komisja Europejska (Komisja) przedstawiła swoją wizję dotyczącą SI wspierającą „tworzenie w Europie etycznych, pewnych i najnowocześniejszych

[39] Firmy te specjalizują się w obsłudze cyfrowych klientów, mają przewagę technologiczną dzięki wykorzystaniu zaawansowanych technologii cyfrowych. Korzystają z chmur obliczeniowych, płatności cyfrowych, analityki danych czy sztucznej inteligencji (ibid.).

[40] *Sztuczna inteligencja i internet rzeczy głównymi nośnikami cyfrowych zmian w gospodarce*, 14.06.2018; http://www.outsourcingportal.eu/pl/sztuczna-inteligencja-i-internet-rzeczy-glownymi-nosnikami-cyfrowych-zmian-w-gospodarce (dostep: 9.09.2019).

[41] Ibid.

[42] *Sprawozdanie zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))*, http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PL.html

rozwiązań w zakresie SI"[43]. Przedstawiona przez Komisję wizja opiera się na trzech filarach: a) zwiększenie inwestycji publicznych i prywatnych w SI w celu jej szerszego rozpowszechnienia; b) przygotowanie się na zmiany społeczno-gospodarcze oraz c) zapewnienie odpowiednich ram etycznych i prawnych, aby wzmocnić wartości europejskie[44].

W dokumencie zatytułowanym „Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteliogencji (SI)" opublikowanym w marcu 2019 r., opracowanym przez powołaną przez Komisję grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji[45] pojęcie „godnej zaufania sztucznej inteligencji" oznacza: 1) przewodnią i nadzorczą rolę człowieka, 2) solidność techniczną i bezpieczeństwo, 3) ochronę prywatności i zarządzanie danymi, 4) przejrzystość, 5) różnorodność, niedyskryminację i sprawiedliwość, 6) dobrostan społeczny i środowiskowy oraz 7) odpowiedzialność[46]. Kodeks postępowania etycznego w dziedzinie robotyki ma stanowić podstawę identyfikacji, kontroli oraz przestrzegania podstawowych zasad etycznych, począwszy od fazy projektu, a skończywszy na fazie rozwoju.

5. Wnioski

Wobec braku legalnych definicji pojęć Internet Rzeczy, sztuczna inteligencja, robotyka, a w konsekwencji braku ich normatywnej regulacji następuje poszukiwanie w systemie prawa norm, które mogą znaleźć zastosowanie do tych rozwiązań *per analogiam*. Zalecenia dotyczące niektórych aspektów związanych z zastosowaniem tych technologii zawierają regulacje UE, jak w szczególności Ogólne Rozporządzenie o ochronie danych osobowych (RODO), jak również normy prawne rozproszone w wielu aktach prawnych,

[43] *Komunikat Komisji Do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Skoordynowany plan…,* op. cit.

[44] Ibid.

[45] Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

[46] Ibid.

w tym w ustawie o prawie autorskim i prawach pokrewnych[47], a także Kodeksie karnym[48]. Wskazuje się na „potrzebę stosowania tzw. inteligentnego prawa, czyli takiego, które zamiast arbitralnego wskazywania konkretnych technik czy działań, określa raczej cele i zasady postępowania, które mogą być stosowane mimo postępujących zmian otoczenia"[49].

Wykorzystanie przez profesjonalistów w prowadzonej przez nich działalności gospodarczej technologii polegającej na komunikowaniu się maszyn (IoT), jak również zastępowaniu człowieka w procesach decyzyjnych (SI) albo wykonywaniu innych czynności, które mogą zostać zaprogramowane i zautomatyzowane (robotyka) wymaga wdrożenia rozwiązań prawnych, które zapewnią bezpieczeństwo stosowania tych rozwiązań, przy czym **przez bezpieczeństwo należy rozmieć stan, w którym normy prawa powszechnie obowiązującego wyznaczają standardy i granice dopuszczalnego zastosowania rozwiązań technicznych oraz przewidują sankcjonowanie aktywności, które granice te przekracza**.

Istnienie norm prawnych regulujących zastosowanie nowych technologii może niewątpliwie oddziaływać prewencyjnie. **Brak regulacji, a ponadto pasywność prawodawcy w zakresie ustanawiania dopuszczalnych granic stosowania nowych technologii polegająca w szczególności na uchyleniu się od katalogowania czynów przestępczych, których popełnienie jest związane z wykorzystaniem nowych technologii jako narzędzia popełnienia przestępstwa, w oczywisty sposób zwiększa ryzyko naruszeń prawa.** Ryzyko zwiększenia naruszeń prawa, w szczególności w dziedzinie prawa karnego, ale także prawa cywilnego, w zakresie ochrony dóbr osobistych, ochrony własności intelektualnej, danych osobowych, dóbr osobistych, występuje zatem wówczas, gdy brakuje normatywnych regulacji nowych zjawisk, pomimo że zjawiska te oddziałują na stosunki społeczne i wywierają wpływ na działalność przedsiębiorstw oraz – szerzej – wywołują skutki w sferze gospodarczej.

Należy ponadto zwrócić uwagę, że nieznajomość technologii oraz brak świadomości i wiedzy po stronie konsumentów korzystających z produktów

---

[47] *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn.: Dz.U. 2019 poz. 1231 z późn. zm.).*

[48] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn.: Dz.U. z 2018 poz. 1600 z późn. zm.).*

[49] M. Zagórski, *Przedmowa*, w: *IoT w polskiej gospodarce…*, op. cit., s. 2.

wykorzystujących SI sprawia, że do nadużycia lub naruszenia prawa, w tym działań o charakterze przestępczym, może dochodzić niemal za wiedzą pokrzywdzonych, którzy z braku doświadczenia i znajomości technologii informatycznych nie tylko nie widzą potrzeby podjęcia działań ochronnych lub zapobiegnięciu popełnienia przestępstwa, ale nie dostrzegają w działaniach podjętych przez sprawcę ani zagrożenia, ani – tym bardziej – winy. Wskazuje się, że w Polsce większość użytkowników nie wie jeszcze o istnieniu IoT. Według badania IAB Polska jedynie 11% ankietowanych internautów spotkało się z tym terminem. Jednocześnie sprzęty IoT znalazły się w posiadaniu 40% korzystających z sieci Polaków. Kolejne 50% zadeklarowało chęć ich nabycia. Największy potencjał nabywczy mają technologie związane z inteligentnym domem oraz RTV i AGD[50]. Popełnienie przestępstwa, którego przedmiotem są niezabezpieczone systemy albo systemy wadliwe, zawierające luki w zabezpieczeniach może okazać się zatem możliwe także pomimo istnienia prawidłowych, tj. adekwatnych do zagrożenia, zabezpieczeń. Okolicznością sprzyjającą popełnieniu przestępstwa z wykorzystaniem systemów informatycznych jest brak świadomości lub kompetencji po stronie użytkowników internetu.

To, co jest technologicznie możliwe, nie zawsze jest bezpieczne i społecznie pożądane. **Wzrost gospodarczy, o ile jest pożądany, to jednak nie może stanowić celu o charakterze autotelicznym i zastępować realizacji innych potrzeb społecznych. Nie może w szczególności pozostawać w kolizji z prawami i wolnościami człowieka, jak prawo do ochrony prywatności, w tym bezpieczeństwa danych osobowych a także – prawo do bycia wolnym od technologii (wolność od technologicznego przymusu).** Rolą państwa jest zatem nie tylko zapewnienie wzrostu gospodarczego, ale także równoważenie wolności i praw z zakresu swobody gospodarczej (technologicznej) ze sferą wolności i praw osobistych człowieka i obywatela. Nie wszystkie zatem rozwiązania i projekcje możliwe do zrealizowania w dziedzinie nowych technologii muszą znajdować aprobatę prawodawcy. Wdrażanie IoT, SI oraz sprzedaż towarów opartych na tych technologiach wymaga dokonywania

[50] M. Albin, *Internet Rzeczy: Dlaczego komuś opłaca się włamać do twojej lodówki i szczoteczki do zębów?*, 30.06.2016, http://www.benchmark.pl/aktualnosci/internet-rzeczy-jak-wykorzystaja-go-hakerzy-i-przestepcy.html (dostęp: 9.09.2019).

w sposób ciągły, tj. adekwatny do zmieniających się rozwiązań technicznych i technologicznych, reagowania prawodawcy na te zjawiska i dokonywania oceny zgodności zastosowanych w nich rozwiązań z konstytucyjnie chronionymi wartościami.

Za nieroztropne i mało wiarygodne należy uznać prezentowane przez organy prawodawcze UE przeświadczenie polegające na upatrywaniu gwarancji bezpieczeństwa nowych technologii wdrażających SI, IoT i robotykę w zbiorach zasad etycznych powstających na użytek stosowania tych technologii. Ich słabością jest bowiem nie tylko nienormatywny charakter, a w konsekwencji brak możliwości zastosowania przymusu wobec podmiotów, które uchylają się od przestrzegania zasad etyki, ale także okoliczność, że powstają one w sposób nienaturalny, są narzucone i nie wypływają z przywiązania do tradycyjnych i ugruntowanych w danych środowiskach zwyczajów.

Podsumowując, należy stwierdzić, że skala prawdopodobnych zagrożeń związanych z nowymi technologiami (IoT, SI, robotyka) jest obecnie trudna do przewidzenia, co jednak nie zwalnia organów prawodawczych z obowiązku regulowania zasad korzystania z tych technologii. **Istnieje bowiem obawa, że brak rozwiązań prawnych będzie skłaniać do działań przestępczych, ingerujących w dobra i interesy zarówno podmiotów prywatnych, jak i publicznych. Zaniechania regulacyjne generują ryzyko pojawienia się nowych form przestępczości, których penalizacja jest konieczna ze względu na potrzebę zapewnienia bezpieczeństwa obywateli i państwa.**

Bibliografia

Albin M., *Internet Rzeczy: Dlaczego komuś opłaca się włamać do twojej lodówki i szczoteczki do zębów?*, 30.06.2016, http://www.benchmark.pl/aktualnosci/internet-rzeczy-jak-wykorzystaja-go-hakerzy-i-przestepcy.html

Budzik T., *Uber nie odpowie za śmiertelny wypadek. Auto jechało samo, więc nie ma kogo winić*, https://autokult.pl/33237,uber-nie-odpowie-za-smiertelny-wypadek-auto-jechalo-samo-wiec-nie-ma-kogo-winic

Chłopecki A., *Sztuczna inteligencja – szkice prawnicze i futurologiczne*, Warszawa 2018; https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damrqgiydcni#tabs-metrical-info

Chustecki J., *To może być pierwszy na świecie wypadek, w którym z winy autonomicznego samochodu zginął człowiek,* https://www.computerworld.pl/news/To-moze-byc-pierwszy-na-swiecie-wypadek-w-ktorym-z-winy-autonomicznego-samochodu-zginal-czlowiek,409950.html

Coraz więcej pesymistów wśród prezesów firm na świecie, omówienie badania PwC, 6.02.2019, https://www.pwc.pl/pl/media/2019/2019-01-25-pwc-22-global-ceo-survey.html

Czapska M., *Aspekty prawne związane z rozwojem sztucznej inteligencji*, w: *Przegląd Strategii Rozwoju Sztucznej Inteligencji na Świecie*, Warszawa 2018, www.digitalpoland.org

Komunikat Komisji Do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Skoordynowany plan w sprawie sztucznej inteligencji, COM(2018) 237 i COM(2018) 795 z dnia 7.12.2018 r.

Komunikat Komisji Do Parlamentu Europejskigo, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Sztuczna inteligencja dla Europy z dnia 25.04.2018r., COM(2018) 237, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-237-F1-PL-MAIN-PART-1.PDF

Perspektywy rozwoju branży IoT na świecie, w: *IoT w polskiej gospodarce, RAPORT Grupy Roboczej do spraw Internetu Rzeczy Przy Ministerstwie Cyfryzacji*, Warszawa 2019 r., s. 5.

Raport KPMG International pt. „The Changing Landscape of Disruptive Technologies. Tech disruptors outpace the competition", https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/06/pl-The-Changing-Landscape-of-Disruptive-Technologies-2018.pdf

Raport MKinsey Global Institute, cyt. za: F.M. Alexandre, The Legal Status of Artificially Intelligent Robots, s. 10.

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.U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Sakowska-Baryła M., *Prywatność w inteligentnym mieście*, w: G. Szpor (red.), *Internet rzeczy. Bezpieczeństwo w Smart City*, Warszawa 2015, s. 136.

Siemaszkiewicz E., *Internet Rzeczy – wyzwania cyberbezpieczeństwa*, „EP", 2018, nr 1, s. 51.

Sprawozdanie zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL)), http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PL.html

Sztuczna inteligencja i internet rzeczy głównymi nośnikami cyfrowych zmian w gospodarce, 14.06.2018, http://www.outsourcingportal.eu/pl/sztuczna-inteligencja-i-internet-rzeczy-glownymi-nosnikami-cyfrowych-zmian-w-gospodarce

Taczkowska-Olszewska J., *Komentarz do art. 2*, w: J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019.

Taczkowska-Olszewska J., *Komentarz do art. 2 pkt. 15*, w: W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz.U. 2019 poz. 123 z późn. zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn.: Dz.U. 2019 poz. 1231 z późn. zm.).

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

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn.: Dz.U. 2018 poz. 1600 z późn. zm.).

Więckowska A., *Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do UODO oraz ocena wagi naruszenie w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)*, https://uodo.gov.pl

Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

Zagórski M., *Przedmowa*, w: IoT w polskiej gospodarce, Raport Grupy Roboczej do spraw Internetu Rzeczy Przy Ministerstwie Cyfryzacji, Warszawa 2019.

Żaczkiewicz-Zborska K., *Sztuczna inteligencja wyręczy sędziów*, https://sip.lex.pl/#/external-news/1795580242?keyword=Sztuczna%20inteligencja%20wyr%C4%99czy%20s%C4%99dzi%C3%B3w&cm=SFIRST