Małgorzata Kutera
Wydział Zarządzania i Komunikacji Społecznej
Uniwersytet Jagielloński

Whisteblowing jako narzędzie wykrywania oszustw gospodarczych

Streszczenie
Obecnie nadużycia finansowe stanowią jedno z większych zagrożeń efektywnego funkcjonowania rynków kapitałowych. Globalizacja i związana z nią liberalizacja oraz niespotykany rozwój technologii informatycznych wyjątkowo sprzyjają oszustwom. Rośnie więc zainteresowanie różnymi narzędziami wspierającymi ich wykrywanie. Badania wskazały, że kluczową rolę w tym zakresie odgrywają zwykłe donosy pochodzące od osób związanych z danym przedsiębiorstwem. Stąd też stworzono i upowszechniono systemy wspomagające przekazywanie takich informacji, które określane są jako whisteblowing. Problem oczywiście wzbudza znaczne kontrowersje. Niektórzy uważają, iż jest to zwykłe donosicielstwo i nie ma nic wspólnego z etyczną postawą.
Niniejsze opracowanie ma na celu prezentację kluczowych zagadnień związanych z whisteblowingiem postrzeganym jako narzędzie wspomagające wykrywanie oszustw gospodarczych. W artykule poruszono głównie problemy związane z definiowaniem pojęcia, przedstawiono amerykański mechanizm whisteblowingu (uchodzący za najbardziej rozbudowany) na tle innych krajów, dokonano analizy zakresu ochrony prawnej sygnalistów i zaprezentowano podstawowe zasady tworzenia efektywnych mechanizmów zgłaszania nadużyć wewnątrz organizacji.

Słowa kluczowe: whisteblowing, sygnaliści, nadużycia, wykrywanie, etyka

1. Wprowadzenie

Nadużycia finansowe są nieodłącznym elementem gospodarki rynkowej. Wyraźnie wskazuje na to historia rozwoju ekonomicznego świata. Wszechobecna globalizacja i związana z nią liberalizacja przepływu pieniądza, dóbr i usług, siły roboczej oraz niespotykany do tej pory rozwój technologii informatycznych wyjątkowo sprzyjają oszustwom. Mechanizmy stosowane przez przestępców już dawno przekroczyły granice jednego kraju czy kontynentu. To oczywiście w znaczny sposób utrudnia walkę ze zjawiskiem. Stało się również jasne, że dalsze uszczegóławianie regulacji z zakresu prawa podatkowego, bilansowego, gospodarczego i handlowego nie przynosi pożądanych efektów. Stąd szersze zainteresowanie wszelkimi innymi narzędziami wspierającymi wykrywanie oszustw.

Badania międzynarodowych organizacji i stwierdzone przypadki nadużyć wskazały, że kluczową rolę w tym zakresie mają zwykłe donosy pochodzące od osób związanych z danym przedsiębiorstwem (najczęściej pracowników). Dlatego też w wielu krajach stworzono i upowszechniono systemy wspomagające przekazywanie takich informacji, które określane są jako *whisteblowing*[1]. Powszechnie uważa się, że najlepszy i najbardziej rozbudowany z nich funkcjonuje z Stanach Zjednoczonych. Problem oczywiście wzbudza wiele kontrowersji. Wiele osób uważa, iż jest to zwykłe donosicielstwo i nie ma nic wspólnego z etyczną postawą. Ocena w znacznym stopniu uzależniona jest od szeregu uwarunkowań historycznych, kulturowych, społecznych, które są różne w poszczególnych krajach. Stąd też występują mniej lub bardziej intensywne prace legislacyjne w tym zakresie, co przekłada się również na skuteczność całego systemu.

Niniejsze opracowanie ma na celu głównie prezentację kluczowych zagadnień związanych z whisteblowingiem, postrzeganym jako narzędzie wspomagające wykrywanie oszustw gospodarczych. Rozważania oparto na tezie głównej brzmiącej: dobrze opracowany i skutecznie wdrożony system whisteblowingu może w znacznym stopniu przyczynić się do efektywniejszego ujawniania nadużyć finansowych. Przy tworzeniu zasad i struktury jego funkcjonowania należy jednak uwzględnić czynniki historyczno-społeczne danego kraju.

Artykuł opiera się głównie na krytycznej analizie wyników badań zjawiska przeprowadzonych przez uznane organizacje międzynarodowe, stosownych aktów prawnych i literatury przedmiotu.

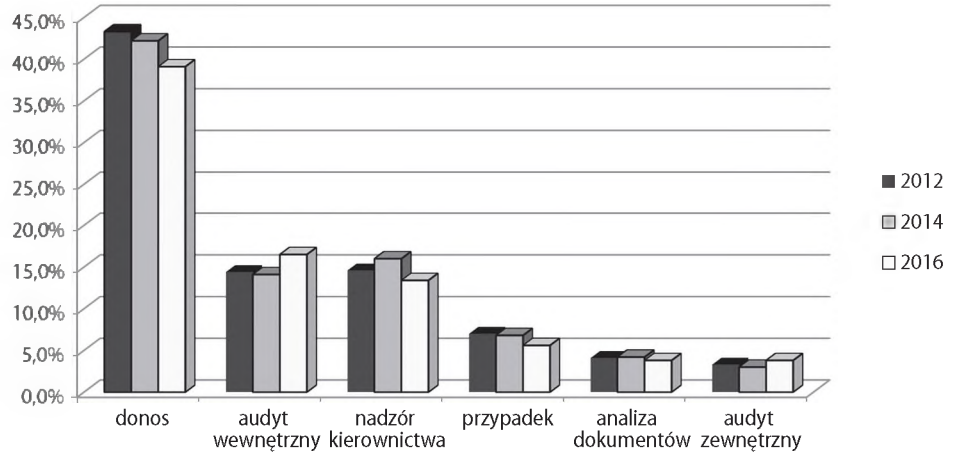
[1] Szczegółowe wyjaśnienie pojęcia zostanie przedstawione w dalszej części opracowania.

2. Donosy głównym źródłem informacji o nadużyciach finansowych

Badania prowadzone przez różne instytucje wyraźnie wskazują, że obecnie najskuteczniejszym narzędziem wykrywania oszustw jest donos. Najszersze analizy w tym zakresie prowadzone są przez amerykańskie Stowarzyszenie Biegłych ds. Nadużyć (*Association of Certified Fraud Examiners* – ACFE), które począwszy od 1996 r. prowadzi systematyczne badania dotyczące oszustw finansowych[2]. Wynika z nich jednoznacznie, że donos jest podstawą ujawnienia nadużycia w około 40% przypadków. Na drugim miejscu znajduje się audyt wewnętrzny (14,1–16,5%), a na kolejnym – nadzór ze strony kierownictwa (13,4–16,0%). Dalsza analiza wskazuje, że donosy w ponad połowie przypadków pochodzą od pracowników, a następnie od klientów i anonimowych osób[3].

Szczegółowe wyniki badań dla najważniejszych kategorii w tym zakresie w latach 2012–2016 zostały zaprezentowane na wykresach 1 i 2.

Wykres 1. Główne mechanizmy wykrywania oszustw finansowych

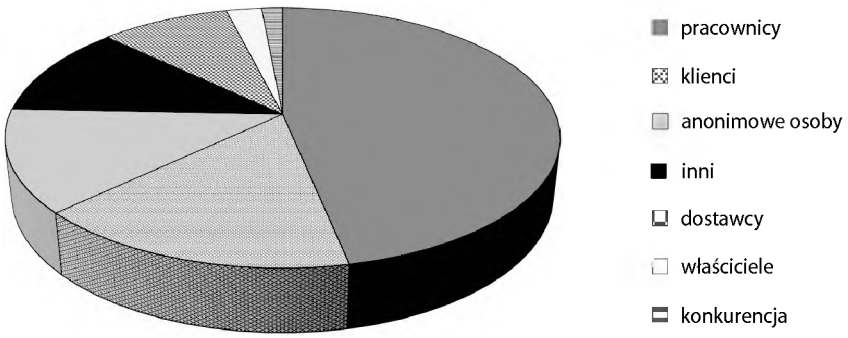


Źródło: opracowanie własne na podstawie ACFE, *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study*, s. 21.

[2] Ostatnie badanie przeprowadzone było w okresie od lipca do października 2015 r. i zawierało 81 szczegółowych pytań dotyczących stwierdzonych nadużyć. Pytania skierowane były do członków organizacji, która skupia obecnie na całym świecie ponad 41 tys. certyfikowanych biegłych zajmujących się tematem oszustw. Ankieta została wypełniona przez 7 497 osób, z czego wybrano 2 410 pełnych *case studies* jako podstawę do szacowania wyników badań.

[3] ACFE, *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study*, s. 21–26.

Wykres 2. Podstawowe grupy donosicieli w 2016 r.



Źródło: opracowanie własne na podstawie ACFE, *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study*, s. 26.

Przedstawione wyniki badań uzasadniają szersze zainteresowanie tym obszarem przez instytucje odpowiedzialne za nadzór nad rynkiem kapitałowym. Widać to głównie w Stanach Zjednoczonych, które od wielu lat prowadzą działania na rzecz maksymalnego ułatwienia zgłaszania podejrzeń popełnienia nadużyć gospodarczych.

Tworzenie sprawnie funkcjonujących gorących linii (*hot lines*) z sensownym programem ochrony sygnalistów jest szczególnie ważnym narzędziem w walce ze skomplikowanymi nadużyciami popełnianymi przez najwyższe kierownictwo spółek. Potwierdza to choćby przypadek WorldComu i osoba Cynthii Cooper's, która stała się jak dotąd najsłynniejszym whisteblowerem świata. Cynthia Cooper's była wiceszefową działu audytu wewnętrznego w WorldComie i wraz ze swoimi dwoma współpracownikami (Gene Morse i Glyn Smith) wykryła i ujawniła oszustwa popełniane przez kierownictwo tej spółki[4]. W swojej pracy wykazała się niesłychaną determinacją, gdyż na początku nikt nie chciał wierzyć w jej rewelacje, łącznie z zewnętrznym audytorem. WorldCom od lat był przecież uznawany na światowego giganta. Nie pomagała jej również postawa dyrektora finansowego Scotta Sullivana, który od początku próbował zdetronizować jej pozycję, prowadząc kuriozalną korespondencję mailową w odpowiedzi na poważne zarzuty Cynthii. Za jej wręcz heroiczną postawę w ujawnieniu skandalu magazyn „Time" ogłosił ją człowiekiem roku 2002.

[4] W przypadku Enronu podobną rolę odegrała Sherron Watkins, wiceszefowa spółki.

3. Pojęcie whisteblowingu

Do tej pory nie wypracowano jednej wspólnej definicji whisteblowingu, która byłaby powszechnie używana w przepisach prawnych. Poszczególne organizacje przyjęły w tym zakresie różne określenia. Międzynarodowa Organizacja Pracy (*International Labour Organization* – ILO) definiuje whisteblowing jako „zgłaszanie przez aktualnych lub byłych pracowników wszystkich nielegalnych, nieprawidłowych, niebezpiecznych lub nieetycznych praktyk stosowanych przez pracodawców"[5].

Rozbudowaną definicją whisteblowingu posługuje się organizacja *Transparency International*. Według niej pojęcie to odnosi się do „ujawniania lub informowania o nadużyciach, które dotyczą korupcji, działań przestępczych, niedopełniania obowiązków, decyzji podjętych bezprawnie, sytuacji zagrożenia zdrowia i bezpieczeństwa publicznego oraz środowiska naturalnego, nadużycia władzy, bezprawnego wykorzystania środków lub majątku publicznego, rażących zaniedbań w zarządzaniu, konfliktu interesów oraz wszystkich działań mających na celu ukrycie tych nieprawidłowości". Zgodnie z dalszym brzmieniem definicji sygnalistą może być każdy pracownik sektora publicznego lub prywatnego albo też inna osoba, która dysponuje informacją na temat nadużycia i jednocześnie ponosi ryzyko działań odwetowych ze strony podejrzanego. Do tych innych osób *Transparency International* zalicza m.in. konsultantów, zleceniobiorców, stażystów, wolontariuszy, praktykantów i byłych pracowników[6].

Szeroki zakres definicyjny whisteblowingu został też zawarty w prawie brytyjskim. Pojęcie to odnosi się do „każdego ujawnienia informacji, które w uzasadnionym przekonaniu osoby dokonującej zgłoszenia prowadzi do ujawnienia co najmniej jednej z poniższych sytuacji[7]:

- przestępstwa kryminalnego, które już miało miejsce, występuje aktualnie lub wystąpi w przyszłości,
- możliwe jest naruszenie zdrowia lub bezpieczeństwa ludzi,
- zagrożone jest środowisko naturalne,
- doszło do naruszenia ogólnych zasad sprawiedliwości".

[5] OECD, *G20 Anti-Corruption Action Plan. Protection of Whisteblowers. Study on Whisteblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*, s. 7.

[6] Transparency International, *Whisteblowing in Europe. Legal Protections for Whisteblowers in the EU*, 2013, s. 6.

[7] UK *Public Interest Disclosure Act (PIDA)*, Part IV A, Section 43B.

Warto podkreślić, że w kontekście tych przepisów nadużycie podlegające zgłoszeniu mogło już wystąpić w przeszłości, występuje aktualnie lub prawdopodobnie będzie miało miejsce w przyszłości. Zakres sygnalistów również jest bardzo szeroki.

Amerykańska ustawa *Whistleblower Protection Act* zawiera podobnie dość obszerną definicję prawną tego pojęcia. Zgodnie z nią whisteblowing to ujawnianie każdej informacji dotyczącej naruszenia prawa, poważnej straty, nadużycia uprawnień lub wymiernego i szczególnego zagrożenia dla zdrowia i bezpieczeństwa publicznego[8]. Informacja może być zgłaszana przez dużą grupę osób.

W języku polskim nie ma dobrego odpowiednika określenia whisteblowing. Wyrażenie to pochodzi od angielskiego zwrotu *to blow the whistle*, czyli „dmuchnąć w gwizdek", „zagwizdać". Jedna z niewielu propozycji polskiego tłumaczenia tego wyrażenia brzmi „demaskacja", „demaskacja pracownicza", „sygnalizowanie"[9]. Zwroty te nie są jednak powszechnie używane w literaturze przedmiotu. Osoby przekazujące informacje określane są mianem whisteblowers. Słowo *whiste-blower* oznacza w dosłownym tłumaczeniu „dmuchający w gwizdek". Chodzi tu o osobę, która, mając pewną wiedzę (lub tylko same podejrzenia), daje sygnał odpowiednim organom lub instytucjom o możliwym nadużyciu. Najpowszechniej przyjętym polskim odpowiednikiem stało się określenie „sygnalista", które chyba najlepiej oddaje istotę sprawy. Często osoby te dysponują tylko podejrzeniami lub niewielkimi fragmentami informacji czy też dokumentów i przekazują o tym informację komuś, kto ma kompetencje i możliwości, aby to zbadać, potwierdzić i zgromadzić dowody.

4. System whisteblowingu w Stanach Zjednoczonych

Najbardziej rozbudowane programy whisteblowingu zostały utworzone w Stanach Zjednoczonych. Obecnie funkcjonuje tam mnóstwo federalnych, stanowych i lokalnych uregulowań dotyczących tej tematyki. Do najważniejszych aktów prawnych należy zaliczyć: *The False Claims Act* (1863), *Whisteblower Protection Act* (1989) i *Whisteblower Protection Enhancement Act* (2012) – odnoszące się głównie do sektora publicznego – oraz *Sarbanes-Oxley Act* (2002) i *Dodd-Frank Act* (2010) – dotyczące sektora prywatnego[10]. Widać więc, że USA mają bogatą tradycję

[8] *Whistleblower Protection Act,* Public Law 101–12, April 10, 1989, par. 1213.

[9] W. Rogowski, *Whiste-blowing: bohaterstwo, zdrada czy interes?*, „Przegląd Corporate Governance" 2007, nr 1, s. 24.

[10] Należy dodać, że w USA istnieje jeszcze oddzielny akt prawny regulujący kwestie ochrony zdrowia i bezpieczeństwa pracowników w miejscu pracy – *Occupational Safety and Health Act* (OSHA) – który też zawiera wytyczne dotyczące sygnalistów.

w regulowaniu procedur odnoszących się do sygnalistów. Wystarczy wspomnieć, że dzięki *The False Claims Act* w latach 1987–2013 wykryto nadużycia na łączną kwotę 38,9 mld dolarów, z czego 27,2 mld dolarów (czyli 70%) dotyczyło przypadków zgłoszonych w ramach whisteblowingu[11].

Szczególnie przełomowa w tym zakresie okazała się ustawa *Sarbanes-Oxley Act* (SOX). Do tej pory bowiem szczególną uwagę zwracano na sygnalistów, którzy informowali o różnych nadużyciach dotyczących sfery zdrowia publicznego, bezpieczeństwa państwa i finansów publicznych. Nie istniały żadne regulacje dotyczące whisteblowingu w sektorze prywatnym. Tymczasem skandale finansowe, które miały miejsce na początku XXI w. wyraźnie wskazały, że kluczową rolę w ich wykryciu mogą mieć pracownicy przedsiębiorstw.

Ustawa SOX nakazała wszystkim komitetom audytu opracowanie i wdrożenie w spółkach odpowiednich programów whisteblowingu. Każdy komitet jest odpowiedzialny za przyjęcie efektywnych procedur w zakresie przyjmowania, przechowywania i reagowania na skargi dotyczące spraw kontroli wewnętrznej, księgowości, sprawozdawczości i audytingu, składane zarówno przez osoby z zewnątrz, jak i wewnątrz podmiotu[12]. Zgodnie z wymogami spółka publiczna powinna więc wdrożyć program whisteblowingu dla pracowników i dla zewnętrznych podmiotów, m.in. klientów, dostawców, inwestorów, kredytodawców. Należy zwrócić uwagę na dość dużą swobodę, jaką przyznaje się sygnalistom. Nie muszą oni w żaden sposób wykazywać, że podejrzenia są prawdziwe. Ustawa wymaga tylko, aby pracownik kierował się uzasadnionym przekonaniem co do popełnienia oszustwa. Może on ponadto wybrać różne sposoby przekazania informacji, tzn. sygnał może być przekazany do zwierzchnika, jakiegokolwiek organu wchodzącego w zakres ładu korporacyjnego, organu państwowego czy wreszcie do mediów. SOX zabrania jednocześnie jakichkolwiek działań restrykcyjnych względem sygnalistów, którzy uzyskują specjalną ochronę[13]. W tym zakresie przewidziano zarówno zwiększoną odpowiedzialność cywilną, jak i karną. Przepisy przewidują wysokie grzywny i karę więzienia nawet do 10 lat.

Kolejnym przełomowym działaniem było uchwalenie w 2010 r. ustawy Dodda-Franka (*Dodd-Frank Act*), na mocy której amerykańska komisja papierów wartościowych i giełdy wprowadziła swój dodatkowy program whisteblowingu. SEC oparła program na trzech filarach: nagrody pieniężne, ochrona sygnalistów przez działaniami odwetowymi i zagwarantowanie poufności. Niezmiernie skuteczny

[11] US Department of Justice, *Fraud Statistics – Overview*, October 1, 1987 – September 30, 2013.

[12] SOX, Section 301 *Public Company Audit Committees*.

[13] SOX, Section 806 *Protection for Employees of Publicly Traded Companies Who Provide Evidence of Fraud*, Section 1107 *Retaliation Against Informants*.

okazał się fakt, że ustawa Dodda-Franka nie tylko wzmocniła ochronę sygnalistów, lecz także przyznała im prawo do wynagrodzenia za informacje, które będą skutkowały podjęciem przez SEC rzeczywistych działań. Zgodnie z przepisami sygnalista, który dostarczy tego typu informacje, może liczyć na wypłatę od 10 do 30% wysokości kary opiewającej na milion dolarów lub więcej, nałożonej na firmę, która dokonała przestępstwa finansowego. Szczegółowe warunki przyznawania nagród pieniężnych zostały przestawione na rysunku 1.

Rysunek 1. Warunki przyznawania nagród pieniężnych w amerykańskim systemie whisteblowingu

Sygnalista otrzymuje nagrodę w wysokości 10–30% kary nałożonej przez SEC po łącznym spełnieniu następujących warunków:

- informacja musi być oryginalna – ma dotyczyć niezależnych faktów lub analiz, co do których SEC nie ma jeszcze żadnych zgłoszeń; nie może to być również informacja ujawniona w publicznych źródłach,
- w wyniku pozyskania informacji SEC przeprowadzi skuteczne postepowanie egzekucyjne; zawiadomienie powinno być więc przekazane w odpowiednim momencie, aby możliwe było efektywne zastosowanie procedur,
- kary nałożone przez SEC w danym przypadku wynoszą co najmniej 1 mln dolarów.

Sygnalista nie otrzymuje nagrody, gdy:

- na podstawie obowiązujących go przepisów prawa był zobligowany do wcześniejszego przekazania tej informacji SEC,
- jest prawnikiem usiłującym wykorzystać informacje pozyskane od klienta,
- zdobył informacje w sposób nielegalny,
- jest specjalistą zaangażowanym w prace SEC,
- pozyskał informacje od innego pracownika,
- ma kryminalne powiązania z osobą lub sytuacją, w zakresie której przekazuje informacje.

Źródło: opracowanie własne na podstawie https://www.workplacefairness.org/corporate-whisteblowers-Sarbanes-Oxley (dostęp: 10.04.2016).

Powyższe uregulowanie wywołało wiele dyskusji, ale niewątpliwie okazało się bardzo skutecznym narzędziem[14]. Potwierdzają to dane na temat działania programu

[14] Zarzuty dotyczą głównie etycznych aspektów programu. Wielu specjalistów uważa, że whisteblowing jest zwykłym donosicielstwem (sygnalistów określają mianem konfidentów czy wręcz zdrajców). Przyznawanie za to nagród pieniężnych jeszcze bardziej wzmocniło te poglądy.

raportowane do Kongresu USA przez SEC. Ich analiza wyraźnie wskazuje, że z roku na rok wzrasta liczba zgłoszeń przyjmowanych w tym systemie i wielkość nagród pieniężnych. Dotychczas SEC wypłaciła łącznie ponad 57 mln dolarów 26 sygnalistom[15]. Rekord wysokości przyznanej nagrody dla jednego sygnalisty został ustanowiony we wrześniu 2014 r. – SEC przyznało premię w wysokości ponad 30 mln dolarów! Budżet całego programu na koniec 2015 r. wynosił ponad 400 mln dolarów[16]. Od początku programu systematycznie wzrasta liczba przekazywanych donosów. W 2015 roku była najwyższa i wyniosła 3 923. Oznacza to ponad 30% wzrost w porównaniu z 2012 rokiem, który był pierwszym pełnym okresem funkcjonowania programu. Prawie połowa osób zgłaszających nadużycia dotyczy byłych lub aktualnych pracowników. Liczba przyjętych zgłoszeń od wdrożenia ustawy została przedstawiona w tabeli nr 1.

Tabela 1. Liczba zgłoszeń o podejrzanych transakcjach zarejestrowana w ramach *Dodd-Frank Whisteblower Program* w USA w latach 2011–2015

2011	2012	2013	2014	2015
334[17]	3 001	3 238	3 620	3 923

Źródło: SEC, *2015 Annual Report to Congress on the Dodd-Frank Whisteblower Program*, s. 21.

Warto dodać, że SEC uwzględnia też donosy pochodzące z innych krajów. Od początku funkcjonowania programu informacje zostały przekazane z 95 krajów. W ciągu 2015 r. najwięcej donosów spoza USA dotyczyło Wielkiej Brytanii, Kanady, Chin, Australii.

5. Ochrona prawna sygnalistów w USA na tle innych krajów

Kluczowym elementem powodzenia systemu *whisteblowingu* w USA, oprócz nagród pieniężnych dla sygnalistów, jest również silna ochrona prawna tych osób. Jak wspomniano wyżej, wszelkie działania odwetowe podejmowane przez podejrzanych mogą zakończyć się 10-letnią karą więzienia i wysokimi grzywnami. Zapewnienie skutecznej ochrony sygnalistów jest właściwie podstawą systemu.

[15] http://www.sec.gov/news/pressrelease/2016-41.html (dostęp: 26.03.2016).

[16] SEC, *2015 Annual Report to Congress on the Dodd-Frank Whisteblower Program*, s. 27.

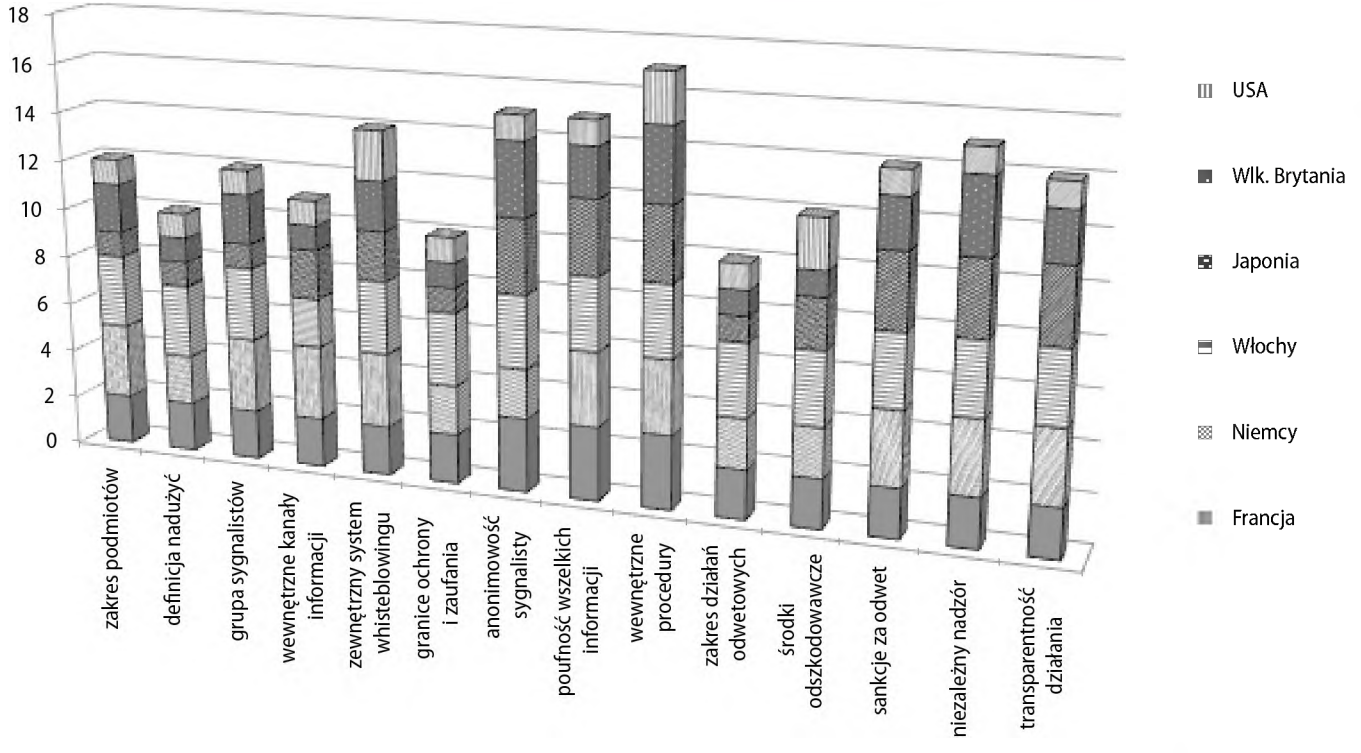
[17] Ze względu na faktyczne wejście w życie zapisów w 2011 r., dane za ten rok odnoszą się tylko do okresu 7 ostatnich tygodni.

Ciekawe badania w tym zakresie zostały przeprowadzone wśród krajów grupy G-20. Szczegółowej analizie poddano przepisy prawne tych państw dotyczące ochrony osób zgłaszających potencjalne nadużycia. Na podstawie badań stworzono ranking najskuteczniejszych systemów prawnych i zestaw najlepszych kryteriów przyjętych w tym obszarze. Do najistotniejszych zaliczono następujące uregulowania[18]:

- obszerny zakres podmiotów prawnych, których dotyczą przepisy, tzn. pochodzących zarówno z sektora prywatnego, jak i publicznego,
- szeroka definicja nadużyć podlegających zgłoszeniu (m.in. korupcja, fałszowanie sprawozdań, nieetyczne zachowania w różnych aspektach),
- zróżnicowany profil potencjalnych sygnalistów, zgłoszenia są przyjmowane od pracowników, dostawców, odbiorców, wolontariuszy itd.,
- wiele wewnętrznych kanałów informacyjnych umożliwiających przekazanie donosu,
- istnieją również zewnętrzne systemy whisteblowingu, tzn. informacja może być przekazana do instytucji zewnętrznej (publicznej), a niekoniecznie do spółki,
- odpowiednio ustawione granice ochrony i zaufania – przyjmuje się domniemanie, że sygnaliści działają w interesie publicznym i nie chcą celowo nikogo skrzywdzić,
- zapewnienie pełnej anonimowości sygnalisty – system umożliwia złożenie anonimowego doniesienia, a w późniejszym okresie (jeśli konieczne będzie ujawnienie pewnych danych) gwarantuje pełną ochronę,
- zachowanie poufności wszelkich informacji – maksymalna w czasie ochrona wszystkich informacji związanych z doniesieniem i przebiegiem postępowania,
- szeroki i ujednolicony zestaw wewnętrznych procedur stosowanych we wszystkich etapach programu,
- uwzględnienie wielu możliwych działań odwetowych ze strony podejrzanych np. zmiana warunków zatrudnienia, zwolnienie z pracy, bezpośrednie naciski, nękanie,
- odpowiednie środki odszkodowawcze dla sygnalistów w przypadku pojawienia się krzywdzących działań podejrzanego,
- wysokie sankcje za działania odwetowe na sygnalistach zarówno w sferze prawa cywilnego, jak i karnego,
- niezależny nadzór nad systemem,
- transparentność i odpowiedzialność w stosowaniu przepisów prawa oraz podejmowanych działaniach.

[18] OECD, *G20 Anti-Corruption Action Plan. Protection of Whisteblowers. Study on Whisteblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*, s. 30–33.

Wykres 3. Regulacje prawne dotyczące whisteblowingu w wybranych krajach



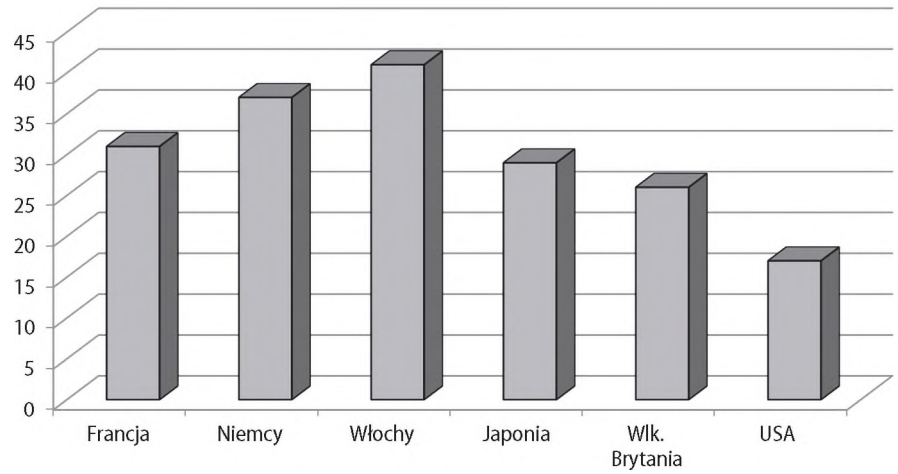
Źródło: opracowanie własne na podstawie S. Wolfe, M. Worth, S. Dreyfus, A.J. Brown, *Whisteblower Protection Laws in G20 Countries. Priorities for Action*, The University of Melbourne, Griffith Univeristy, Transparenty International Australia, September 2014, s. 22–65.

Podsumowanie wyników badań dla wybranych krajów grupy G-20 według powyższych kryteriów zostało przestawione na wykresie 3. Prezentowane dane dotyczą wyłącznie systemów whisteblowingu odnoszących się do sektora prywatnego[19].

Analiza wykresu wskazuje, że ogólnie najsłabszymi elementami tych systemów jest stosowanie jednolitych procedur wewnętrznych odnoszących się do zbierania i analizowania informacji pozyskiwanych od sygnalistów. Za wyjątkiem USA kraje mają też problemy z pełnym zachowaniem anonimowości i poufności danych oraz niezależnym nadzorem.

Sumaryczne wyniki dla analizowanych krajów zostały zaprezentowane na wykresie 4. Wynika z nich jednoznacznie, że największy stopień dopasowania istniejących przepisów prawnych do kryteriów ogólnie zalecanych jest w Stanach Zjednoczonych. USA stały się niejako wzorcem w tym zakresie. Stosunkowo słabo w tym ujęciu wypadają Włochy i Niemcy.

Wykres 4. Ogólna ocena przyjętego systemu whisteblowingu w wybranych krajach



Źródło: opracowanie własne na podstawie S. Wolfe, M. Worth, S. Dreyfus, A.J. Brown, *Whisteblower Protection Laws in G20 Countries. Priorities for Action*, The University of Melbourne, Griffith Univeristy, Transparenty International Australia, September 2014, s. 22–65.

Analitycy podkreślają, że przykładowo we Włoszech duży wpływ na funkcjonowanie whisteblowingu mają czynniki kulturowe. Niezbyt popularne jest donoszenie

[19] Skala ocen przyjęta w badaniu była następująca: pełna zgodność z kryterium – 1 pkt, średni poziom zgodności – 2 pkt, brak uregulowań lub mało precyzyjne w danym obszarze – 3 pkt; najlepiej w ocenie wypada system, który ma najmniejszą liczbę punktów.

na działania podejmowane przez inne osoby. Toczyła się tam ostra debata na ten temat, która zaowocowała przyjęciem standardów, ale tylko w zakresie instytucji finansów publicznych i skierowanych głównie na walkę z łapownictwem. Nie ma natomiast specjalnych uregulowań na poziomie krajowym z zakresu ochrony prawnej dla pracowników sektora prywatnego. Podobna sytuacja występuje w Niemczech. Pełną ochroną objęci są tam tylko pracownicy finansów publicznych, którzy zgłoszą przypadki łapówek[20]. Jeśli chodzi o przedstawicieli spółek prywatnych najważniejszym aktem prawnym jest zwykły Kodeks pracy i wszystkie postępowania w tym zakresie są rozpatrywane przez sądy pracy. Stosowne systemy whisteblowingu są więc tworzone wewnętrznie w przedsiębiorstwach, bez wsparcia ze strony instytucji centralnych[21]. Podobnie sytuacja wygląda również w Polsce. W naszym kraju nie ma szeroko rozwiniętych systemów whisteblowingu. Wynika to głównie z braku odpowiednich regulacji prawnych. Niektóre podmioty wprowadzają jednak dobrowolnie podobne programy, biorąc pod uwagę głównie ich skuteczność. W przypadku spółek z większościowym kapitałem zagranicznym mogą one być również narzucone przez spółki dominujące.

Nieco inaczej sytuacja wygląda w krajach anglosaskich. W Wielkiej Brytanii funkcjonują trzy podstawowe akty prawne w tym zakresie: *Public Interest Disclosure Act* (PIDA) z 1998 r., *Enterprise and Regulatory Reform Act* (2013), *Employment Rights Act* (1996). Głównym źródłem przepisów dotyczących ochrony sygnalistów jest PIDA, mocno znowelizowany w 2013 r. Dotyczy on zarówno pracowników sektora prywatnego, jak i publicznego. Nie obejmuje jednak wolontariuszy, praktykantów czy też osób ubiegających się o pracę. W Wielkiej Brytanii zdefiniowano w szeroki sposób zestaw możliwych działań odwetowych podejmowanych przez osoby podejrzane o nadużycia i określono sposoby ich rekompensaty. Najbardziej rozwinięty system whisteblowingu występuje jednak w Stanach Zjednoczonych, co zostało już wcześniej wspomniane.

Na koniec tej części rozważań warto jeszcze przytoczyć ogólne wyniki badań z zakresu ochrony prawnej sygnalistów przeprowadzone przez *Transparency International*. Ich podsumowanie zawiera tabela 2.

Jak wynika z zestawienia, stosunkowo mało krajów Unii Europejskiej ma silnie rozbudowane systemy informowania o nieprawidłowościach, zapewniające skuteczną ochronę sygnalistom. Miejsce Wielkiej Brytanii jako kraju o anglosaskiej kulturze jest tu oczywiste i pokrywa się z wynikami poprzedniego badania. Zaskakująca jest bardzo dobra ocena Rumunii i Słowenii. Jako nowi członkowie UE kraje

[20] *Criminal Code of Germany*, Chapter 30, Sections 331–337.

[21] *Corporate Crime. The Age of Whisteblower*, „The Economist", December 5th 2015.

te zaimplementowały od początku wysokie standardy, bazując na dobrych wzorcach. Najwięcej krajów mieści się w środkowej grupie (w tym również Polska). Należy jednak wspomnieć, że kilka państw europejskich w ostatnim czasie wprowadziło zmiany prawne wzmacniające ochronę sygnalistów: Austria, Belgia, Dania, Francja, Węgry, Włochy, Malta. Pozostałe pracują nad takimi przepisami, aczkolwiek czynniki polityczne, socjalne i historyczne w dużym stopniu blokują te działania. Oceniając europejskie uregulowania, trzeba stwierdzić, że najstarszym i najlepszym z nich jest brytyjski *Public Interest Disclosure Act* (PIDA) z 1998 r.

Tabela 2. Stopień ochrony prawnej sygnalistów w krajach UE

Wysoki	Średni	Niski lub brak
Luksemburg	Austria	Bułgaria
Rumunia	Belgia	Finlandia
Słowenia	Cypr	Grecja
Wielka Brytania	Czechy	Litwa
	Dania	Portugalia
	Estonia	Słowacja
	Francja	Hiszpania
	Niemcy	
	Węgry	
	Irlandia	
	Włochy	
	Łotwa	
	Malta	
	Holandia	
	Polska	
	Szwecja	

Źródło: Transparency International, *Whisteblowing in Europe. Legal Protections for Whisteblowers in the EU*, 2013, s. 8.

6. Zasady tworzenia efektywnych systemów whisteblowingu

W procesie przyjmowania i rozpatrywania informacji przekazywanych w ramach wewnętrznego systemu whisteblowingu można wyróżnić kilka podstawowych etapów, na które należy zwrócić szczególną uwagę. Dla każdego z nich trzeba opracować i zaimplementować stosowne procedury, wzmacniające skuteczność całego systemu. Ma to zasadnicze znaczenie dla komitetów audytu, które ponoszą pełną odpowiedzialność za wdrożenie tych procedur. Kluczowe etapy programu whisteblowingu zostały przedstawione na rysunku 2.

Rysunek 2. Podstawowe etapy programu whisteblowingu

Źródło: opracowanie własne.

Procedury przyjmowania informacji od sygnalistów wymagają ściśle określonych i zdyscyplinowanych metod dokumentowania i weryfikacji donosów. Każda informacja przekazywana ustnie lub pisemnie powinna być zarejestrowana. Następnie zaleca się ich wstępną segregację pod względem znaczenia i istotności. Mogą tego dokonywać zarówno członkowie komitetów audytu, jak również wyspecjalizowani konsultanci mający dostęp do kierownictwa firmy i jej pracowników. Wstępna weryfikacja powinna dotyczyć dwóch aspektów:

- rzetelności – czy informacja jest wiarygodna, aktualna i uzasadniona,
- treści merytorycznej – jakich obszarów i procesów dotyczy: rachunkowości, kontroli wewnętrznej, audytu, zakupów, sprzedaży?

Na tym etapie niezwykle ważny jest sposób kontaktu z sygnalistą[22]. Konieczna jest przy tym możliwość zapewnienia pełnej i rzeczywistej anonimowości informatorów, jeśli tego żądają. W każdym przypadku jako minimum wymaga się zachowania poufności danych dotyczących osoby zgłaszającej problem (czyli można przekazać te dane wyłącznie wąskiej grupie ludzi, gdy jest to konieczne). Inne aspekty decydujące o efektywności rejestrowania donosów, które należy wziąć pod uwagę to:

[22] Badania przeprowadzone przez ACFE w 2015 r. wyraźnie wskazują, że najpopularniejszym środkiem przekazywania informacji jest linia telefoniczna (39,5%), następnie e-mail (34,1%) i strona internetowa (23,5%). *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study*, s. 28.

- gorąca linia powinna być czynna 24 godziny przez 7 dni w tygodniu,
- przeszkoleni i umiejętni wywiadowcy,
- możliwość komunikowania się w różnych podstawowych językach, gdyż zgłoszenie może pochodzić z innego kraju,
- uwzględnienie, że sygnaliści mogą mieć różny system wartości, nierzadko zupełnie inny niż kierownictwo spółki,
- system zakodowanej identyfikacji sygnalistów, np. nadawanie im niepowtarzalnych numerów, którymi będą mogli się posługiwać w przyszłości, podając szczegóły lub też nowe informacje,
- rejestrowanie wszystkich zgłoszonych przypadków niepoprawnych zachowań,
- odpowiednia i niezwłoczna odpowiedź na zgłoszenie,
- system nagród dla sygnalistów,
- szerokie propagowanie informacji o istniejącej *hot line* wśród pracowników, akcjonariuszy, dostawców, odbiorców itd.

Niezwykle ważną kwestią w tym zakresie jest odpowiednio przeszkolony i doświadczony personel obsługujący *hot lines*. Niejednokrotnie zachowanie i reakcja wywiadowcy przesądza o dalszym powodzeniu sprawy. Stąd na szkoleniach zwraca się szczególną uwagę na podstawowe zasady, jakie powinny być zachowane podczas takiego wywiadu, i kluczowe informacje, które należy pozyskać. Oto najważniejsze z nich[23]:

- na początku poucz rozmówcę, że rozmowa jest w pełni poufna i nie jest rejestrowana; zapewnij go o anonimowości, chyba że sam chce ujawnić pewne dane osobiste,
- zanotuj datę i godzinę rozmowy,
- jeśli to możliwe, zanotuj operatora, numer telefonu i/lub lokalizację rozmówcy,
- nadaj rozmówcy niepowtarzalny zakodowany numer identyfikacyjny, którym będziecie się posługiwać w przyszłości w razie ewentualnych kolejnych kontaktów,
- czy rozmówca jest pracownikiem, dostawcą, odbiorcą, do jakiej grupy należy,
- o jakie naruszenie chodzi, czego dotyczy,
- w jaki sposób rozmówca zorientował się, że dochodzi do naruszenia; w jaki sposób uzyskał informację,
- kto bierze udział w nadużyciu – w tym zakresie wywiadowca powinien uzyskać możliwie najwięcej szczegółowych informacji,
- kiedy, gdzie i z jaką częstotliwością dochodziło na naruszenia,
- jak długo trwało nadużycie i czy nadal ono trwa,

[23] M.T. Biegelman, J.T. Bartow, *Executive Roadmap to Fraud Prevention and Internal Control. Creating a Culture of Compliance,* John Wiley& Sons, New Jersey 2012, s. 274.

- czy rozmówca dysponuje jakimikolwiek dokumentami związanymi z oszustwem,
- czy rozmówca zgłaszał już wcześniej podobne zdarzenie.

Po otrzymaniu wstępnie rozpoznanych informacji członkowie komitetu audytu powinni przeprowadzić pogłębioną analizę sytuacji przy wsparciu prawników. Jej celem jest zidentyfikowanie wszystkich istotnych faktów i informacji oraz określenie kierunków dalszego działania. W tym zakresie komitet audytu musi kierować się pewnymi zestandaryzowanymi procedurami, co zapewnia obiektywizm w każdym analizowanym przypadku. Pogłębiona weryfikacja powinna obejmować głównie dwa aspekty:

- merytoryczny wpływ stwierdzonych zdarzeń i okoliczności na sytuację podmiotu – jakich obszarów działalności dotyczy nadużycie, kto ponosi odpowiedzialność za ten proces i w jakim zakresie doszło do naruszenia prawa,
- istotność – próba określenia finansowego wpływu zdarzenia na sytuację spółki i podmiotów z nią związanych.

Po określeniu merytorycznego związku oszustwa z działalnością przedsiębiorstwa i jego potencjalnych skutków finansowych podejmowana jest decyzja o dalszej weryfikacji problemu. Jeśli problem nie jest znaczący, komitet audytu może zlecić wyjaśnienie tej sytuacji organom wewnętrznym przedsiębiorstwa lub wybranym jego pracownikom. Należy jednak w tym zakresie zwrócić uwagę, czy nie zachodzi konflikt interesów. Jako minimum przyjmuje się, że nadzór nad takim postepowaniem powinien mieć zewnętrzny specjalista. W przypadku poważniejszych nadużyć zalecane jest prowadzenie prac dochodzeniowych w pełni przez podmioty zewnętrzne, np. w ramach audytu śledczego.

Po etapie pełnego ustalenia stanu faktycznego i jego zakresu finansowego dochodzi do podjęcia decyzji o dalszym postępowaniu. Powinna ona dotyczyć dwóch obszarów: skierowanie sprawy na drogę prawną w celu wyciągnięcia odpowiedzialności wobec konkretnych osób i działania korygujące, które mają wzmocnić kontrolę w danym obszarze objętym nadużyciem. Należy przy tym pamiętać o sprawnym i rzetelnym podejmowaniu decyzji. Po ujawnieniu nadużycia wszystkie strony będą oczekiwały szybkich i konkretnych działań. Sygnaliści są zainteresowani bieżącym raportowaniem o postępie prac, niewinni podejrzani chcą natychmiastowego uwolnienia od nieprawdziwych zarzutów a faktyczni sprawcy nadużyć powinni być jak najszybciej osądzeni. Szczególną ostrożność należy przy tym zachować podczas komunikowania się z różnymi stronami i raportowania. Z jednej strony trzeba dbać o zachowanie poufności niektórych danych, a z drugiej informowanie musi być rzetelne, żeby postępowanie mogło być prowadzone sprawnie.

Dokumentacja związana z każdym rozpatrywanym oszustwem podlega stosownej archiwizacji. Powinna ona obejmować i identyfikować wszystkie etapy procesu

rozpatrywania donosu, począwszy od jego zgłoszenia. Dokumenty objęte są pełną tajemnicą ochrony informacji również po zakończeniu postępowania.

7. Podsumowanie

W związku z rosnącą skalą nadużyć finansowych szczególnego znaczenia nabiera poszukiwanie skutecznych sposobów walki z tym zjawiskiem. Ważne są przede wszystkim efektywne mechanizmy wykrywania oszustw. Badania dowodzą, że standardowe procedury związane z nadzorem korporacyjnym są w tym zakresie niewystarczające. Jak pokazuje historia narzędzia stosowane przez kontrolę wewnętrzną, audytorów, radę nadzorczą, komitety audytu często nie przynosiły pożądanych efektów. Okazuje się, że oszustwa bardzo często wykrywane są dzięki donosom osób związanych z danym przedsiębiorstwem. Stąd też rosnące zainteresowanie zjawiskiem whisteblowingu zarówno wśród teoretyków, jak i praktyków. Doprowadziło ono w wielu krajach do uchwalenia szczegółowych przepisów prawnych regulujących zasady informowania o ryzyku nadużyć. Najlepiej ten mechanizm funkcjonuje w Stanach Zjednoczonych. Inne kraje o anglosaskim systemie gospodarczym również z powodzeniem wdrażają zmiany. W mocno rozwiniętych społeczeństwach obywatelskich whisteblowing pełni ważną funkcję w ochronie szeroko rozumianego interesu społecznego. Analiza regulacji prawnych jednoznacznie ujawniła jednak duże różnice w zasadach składania donosów i zakresie ochrony prawnej sygnalistów. Do kluczowych kwestii można tu również zaliczyć definicję prawną whisteblowingu, kanały przekazywania informacji i zakres osób, które mogą tego dokonywać. Przy tworzeniu regulacji prawnych z pewnością należy uwzględnić aspekty historyczne, kulturowe i społeczne poszczególnych państw. W przeciwnym razie może się okazać, że system *whisteblowingu* będzie miał opracowane szczegółowe zasady, ale w praktyce nie będzie funkcjonował skutecznie.

Bibiografia

1. ACFE, *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study*.
2. Biegelman M. T, Bartow J.T., *Executive Roadmap to Fraud Prevention and Internal Control. Creating a Culture of Compliance*, John Wiley & Sons, New Jersey 2012.
3. Bowers J., Fodder M., Lewis J., Mitchell J., *Whisteblowing: Law and Practice*, Oxford University Press, Oxford 2012.

4. Calland R., *Whisteblowing Around the World: Law, Culture and Practice*, IDASA Publishers, 2005.
5. *Corporate Crime. The Age of Whisteblower*, „The Economist", December 5th 2015.
6. OECD, *G20 Anti-Corruption Action Plan. Protection of Whisteblowers. Study on Whisteblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation.*
7. Rogowski W., *Whiste-blowing: bohaterstwo, zdrada czy interes?*, „Przegląd Corporate Governance" 2007, nr 1.
8. SEC, *2015 Annual Report to Congress on the Dodd-Frank Whisteblower Program.*
9. Thüsing G., Forst G., *Whisteblowing – A Comparative Study*, Springer International Publishing, Switzerland 2016.
10. Transparency International, *Whisteblowing in Europe. Legal Protections for Whisteblowers in the EU,* 2013.
11. UK, *Public Interest Disclosure Act* (PIDA).
12. US Department of Justice, *Fraud Statistics – Overview*, October 1, 1987 – September 30, 2013.
13. *Whistleblower Protection Act*, Public Law 101–12, April 10, 1989.
14. Wolfe S., Worth M., Dreyfus S., Brown A.J., *Whisteblower Protection Laws in G20 Countries. Priorities for Action*, The University of Melbourne, Griffith Univeristy, Transparenty International Australia, September 2014.

Źródła internetowe

1. https://www.workplacefairness.org/corporate-whisteblowers-Sarbanes-Oxley.
2. http://www.sec.gov/news/pressrelease/2016–41.html.

Whistleblowing as a Business Fraud Detecting Instrument

Summary

At present financial abuse is a major threat to an effective operation of capital markets. Globalisation and the related liberalization as well as an unprecedented development of information technologies exceptionally favour frauds. Thus, the interest in all kinds of tools supporting their detection is on the rise. The research indicates that the key role in this area is played by the information provided by the stakeholders. Hence, systems supporting the provision of this information called whistleblowing have been created and made popular. The problem naturally arouses controversy. The present study aims primarily at the presentation of key issues connected with whistleblowing considered to be a tool to support detection business fraud. The article presents mainly the problems connected with the definition of the issue, the American model of whistleblowing (thought to be well developed) compared to other countries, analyses the scope of legal protection of whistleblowers and discusses the principles of creation of effective mechanisms of abuse in-house reporting.

Keywords: whistleblowing, whistleblower, abuse, detection, ethics