Dariusz Pauch

System anonimowego informowania o nadużyciach w przedsiębiorstwie : "whistleblowing"

Ekonomiczne Problemy Usług nr 80, 71-78

2011

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 695 EKONOMICZNE PROBLEMY USŁUG NR 80 2011

DARIUSZ PAUCH
Uniwersytet Szczeciński

SYSTEM ANONIMOWEGO INFORMOWANIA O NADUŻYCIACH W PRZEDSIĘBIORSTWIE – *WHISTLEBLOWING*

Wprowadzenie

Jednym z celów właściciela lub zarządu spółki jest zapewnienie właściwego poziomu bezpieczeństwa. Dla większości osób bezpieczeństwo jednoznacznie kojarzy się z bezpieczeństwem fizycznym – ochroniarzami, kontrolą dostępu czy monitoringiem. Jednak samo bezpieczeństwo jest terminem dużo szerszym i obejmuje – obok bezpieczeństwa fizycznego – także takie aspekty, jak zapewnienie ochrony przed nadużyciami dokonywanymi przez pracowników. Tutaj bardzo cenne okazuje się uczestnictwo pracowników w działaniach kontrolnych, które łączą z rolą obserwatora, demaskatora, który informuje o bezprawnych lub niemoralnych praktykach w organizacji.

Celem artykułu jest przedstawienie systemu anonimowego informowania o nadużyciach jako instrumentu umożliwiającego uzyskanie informacji o nadużyciach w przedsiębiorstwie.

1. Definicja pojęcia *whistleblowing*

Pojęcie *whistleblowing*, choć znane od średniowiecza, dopiero od 40 lat jest łączone z ujawnianiem przestępczości w organizacjach. Stało sie również terminem prawniczym[1] i podobnie jak *corporate governance* wieloznacznym zwrotem języka globalnego. Znaczenie *whistleblowing* w krajach anglosaskich rośnie od lat, a wraz z uchwaleniem w 2002 roku ustawy Sarbanes-Oxley Act (SOX) awansował on do klasy głównych instrumentów mających chronić ład korporacyjny.

Trudno znaleźć w języku polskim odpowiednik, który miałby naturalne brzmienie i jednocześnie nie przywoływałby negatywnych skojarzeń. Słowo *whistleblower* to w dosłownym tłumaczeniu *dmuchający w gwizdek*. Nawiązuje do angielskich policjantów, którzy na widok przestępstwa posługiwali się gwizdkami, aby zaalarmować kolegów i sprowadzić pomoc. Jedna z nielicznych propozycji to *sygnaliści*, a więc osoby sygnalizujące właści-

[1] M. Dodge, *Whistleblowers*, w: *Encyclopedia of white-collar and corporate crime*, red. L.M. Salinger, SAGE Publications, Thousand Oaks 2005, Vol. 1 & 2, s. 860.

wym organom lub opinii publicznej pewne nieprawidłowości. Określenie *sygnaliści* jest o tyle trafne, że z góry definiuje rolę osoby informującej o nieprawidłowościach. W większości przypadków osoby te dysponują jedynie podejrzeniami, fragmentami informacji budzącymi niepokój, pojedynczymi cząstkami całej układanki, a więc pewnymi *sygnałami* o nieprawidłowościach. Określenie *sygnalista* wskazywałoby zatem, że jego rola to przede wszystkim *zasygnalizowanie* swoich podejrzeń komuś, kto będzie miał kompetencje i możliwości, aby je zweryfikować i ewentualnie zgromadzić dowody na ich potwierdzenie[2].

Whistleblower – czyli osoba, która sygnalizuje zachowania nieetyczne. W języku polskim można się również spotkać z takimi określeniami, jak: *informator w dobrej wierze*, *donosiciel*, *kapuś* czy *tajny współpracownik*. Dlatego alternatywnie proponuje się, aby *whistleblower* został *demaskatorem*[3].

Wśród definicji określających system anonimowego informowania można wybrać następujące:

1. *Whistleblowing* – demaskowanie, demaskacja pracownicza, sygnalizowanie/ nagłaśnianie zachowań nieetycznych, ujawnianie w dobrej wierze, informowanie przełożonych, wołanie na trwogę, „dać na trwogę", „bić w bębny (tarabany) na trwogę", „hue and cry" – okrzyki niezadowolenia na wieść o zbrodni, „łapać złodzieja!", wczesne ostrzeganie o nieprawidłowościach[4].
2. *Whistleblower* – demaskator, demaskator pracowniczy, informator w dobrej wierze, „ten, kto dmie w gwizdek, aby ujawnić nieprawidłowości", donosiciel w dobrej wierze, donosiciel w interesie publicznym, „pracownik, który publicznie ujawnia nielegalne operacje firmy[5].

M. Miceli i J.P. Near określają *whistleblowing* jako ujawnienie przez członka organizacji (byłego lub obecnego) nielegalnych, niemoralnych lub bezprawnych praktyk dokonywanych za wiedzą pracodawcy, dokonane poprzez poinformowanie osób lub organizacji, które są zdolne do podjęcia skutecznych działań (w celu powstrzymania tych praktyk)[6].

R. Nader stwierdza, że *whistleblower* to osoba, która zgłasza w dobrej wierze i na racjonalnych podstawach właściwemu organowi wszelkie zdarzenia związane z przestępstwami[7].

Zdaniem G.R. Watchmanaka, w*histleblower* to aktywny obywatel, który będąc świadkiem bezprawnego działania, zabiega o jego wyeliminowanie. Takie osoby odgrywają żywotną rolę w społeczeństwie otwartym, społeczeństwie demokratycznym. Zmuszają

---

[2] A. Wojciechowska-Nowak, *Jak zdemaskować szwindel? Czyli krótki przewodnik po whistleblowingu*, Fundacja im. Stefana Batorego, Warszawa 2008, s. 9.

[3] Szerzej: W. Rogowski, *Whistleblowing: bohaterstwo, zdrada czy interes?*, „Przegląd Corporate Governance" 2007, nr 1 (9).

[4] *Ibidem*, s. 24.

[5] *Ibidem*.

[6] J.P. Near, M.P. Miceli, *Organizational Dessidence: The Case of Whistle-blowing*, „Journal of Business Ethics" 1985, No. 4, s. 4.

[7] D. Banisar, *Whistleblowing Internal Standards and Developments*, Instituto de Investigaciones Sociales, Unam 2006, s. 5.

bowiem nasze instytucje publiczne do odpowiedzialności wobec ludzi, którym z założenia mają one służyć. Zbyt często jednak okazuje się, że osoby te są raczej karane niż nagradzane za swoje zasługi, które prowadzą do wyciągnięcia na światło dzienne zachowań łamiących prawo, zagrożeń dla zdrowia publicznego, oszustw, nadużyć władzy lub błędów stwarzających ryzyko dla bezpieczeństwa narodowego[8].

Amerykańska ustawa o ochronie osób udzielających informacji o nadużyciach w organizacji (*Whistleblower Protection Act*) zawiera definicję prawną procesu demaskowania, precyzując, że „jest to ujawnianie informacji, która w pojęciu pracownika jest udokumentowana ewidencją działań nielegalnych, poważnej straty, znacznego nadużycia zarządczego, nadużycia władzy lub wymiernego i szczególnego zagrożenia dla zdrowia i bezpieczeństwa publicznego”[9].

W ujęciu teoretycznym nieprawidłowością prowadzącą do strat jest każde odchylenie od stanu optymalnego w realizacji strategii. W praktyce może to być np. zakup surowców po zawyżonej cenie, wynagradzanie pracownika nieadekwatne do świadczonej pracy, przeszacowana ocena potencjału intelektualnego przyjmowanego pracownika, nieprawidłowe księgowanie czy podpisany przez prezesa zarządu kontrakt zawierający niekorzystne dla spółki rozstrzygnięcia. Ze względu na stochastyczną w pewnym zakresie naturę przedsiębiorczości w każdym działaniu biznesowym jest margines błędu i ryzyko jego wystąpienia[10].

Próbując bliżej opisać ideę *whistleblowingu*, należy skoncentrować się na czterech istotnych punktach (elementach składowych)[11]:

- **sensacyjne odkrycie** – ujawnia niemożliwe do zaakceptowania niebezpieczeństwa, ryzyko i nieprawidłowości (np. naruszanie zapisów umów, korupcji), które stanowią zagrożenie dla współżycia społecznego lub środowiska,
- **szlachetne pobudki** – nie działa dla własnej korzyści, ale z troski o dobro bliźnich oraz stan środowiska,
- **wszczęcie alarmu** – zgłasza nieprawidłowości w miejscu pracy; dopiero przy braku reakcji ze strony kompetentnych osób lub jeśli reakcja ta jest nieadekwatna, informuje opinię publiczną,
- **zagrożenie własnej egzystencji** – naraża się na duże niebezpieczeństwo, ryzykuje swoją karierę zawodową albo nawet swoją egzystencję.

---

[8] A. Wojciechowska-Nowak, *Jak zdemaskować szwindel?...*, s. 5.

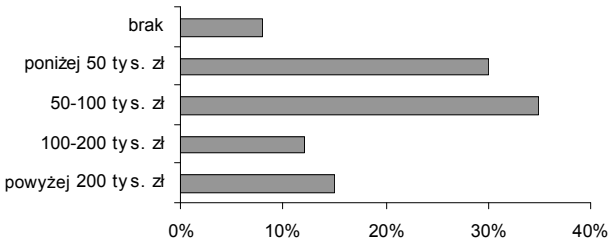
[9] *Encyclopedia of white-collar and corporate crime...*, Vol. 2, s. 860.

[10] S. Kasiewicz, W. Rogowski, *Ryzyko a wzrost wartości przedsiębiorstwa*, „Kwartalnik Nauk o Przedsiębiorstwie” 2006, nr 1, s. 34.

[11] *Sport bez korupcji. Podręcznik dobrych praktyk*, red. H.M. Arndt, D. Miebach, MSWiA, Apla – Oficyna Poligraficzna, Kielce 2006, s. 214.

2. Ryzyko nadużyć a skłonność przedsiębiorców do korzystania z systemu anonimowego informowania

Podejmując próbę oceny zjawiska przestępczości gospodarczej w Polsce, warto posłużyć się danymi przygotowanymi i opublikowanymi pod koniec 2009 roku przez Euler Hermes. Jak wynika z raportu, do strat z tytułu nieuczciwych pracowników przyznaje się aż 92% ankietowanych przedsiębiorców. Tymczasem w podobnych badaniach przeprowadzonych w 2008 roku poszkodowani to zaledwie połowa firm. Szybko rośnie nie tylko liczba, ale także wartość tego typu przestępstw (rys. 1). Już 15% przedsiębiorstw w Polsce notuje z tego powodu straty przekraczające 200 tys. zł. A odsetek przedsiębiorstw, które przez nieuczciwych pracowników straciły od 50 tys. do 100 tys. zł, zwiększył się z 15% (2008 r.) do 35% (2009 r.).



Rysunek 1. Wartość strat wywołanych przez pracowników na szkodę pracodawcy w 2009 roku

Źródło: TU Euler Hermes SA.

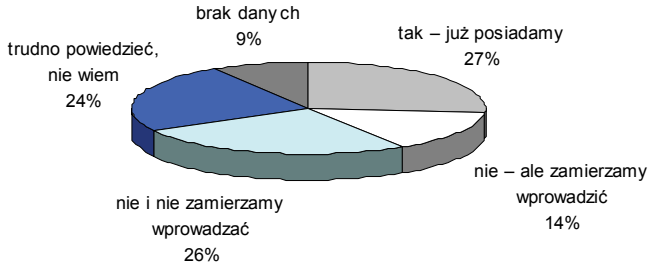
Najczęstszym sposobem ujawnienia nadużyć w polskich firmach była informacja anonimowa lub pochodząca od pracowników (łącznie 66%), następnie rutynowe działania kontrolne, audyt wewnętrzny, system zarządzania ryzykiem i na końcu – zaangażowanie państwowych organów ścigania[12]. Wyniki te są zbliżone do uzyskanych w USA: w 2004 roku 43% malwersacji i przestępstw korporacyjnych zostało ujawnionych w wyniku informacji uzyskanych od pracowników, kontrahentów lub klientów spółki, w której doszło do przestępstwa, czyli w wyniku działań demaskatorskich (*whistleblowing*). Formalne systemy kontroli – audyt wewnętrzny oraz zewnętrzny – były mniej skuteczne, ich działanie ujawniło odpowiednio 24% i 11% przestępstw korporacyjnych[13].

---

[12] M. Rzepnikowska, *Nadużycia gospodarcze w polskich firmach*, prezentacja z konferencji Corporate Governance XXX *Przestępczość korporacyjna. Zapobieganie i wykrywanie*, 7 czerwca 2006 r., Warszawa, Deloitte, s. 8. Badaniami objęto kadrę zarządzająca 1000 największych firm i instytucji publicznych. Przyczyną niższego udziału pracowników mogą być nieodkryte w śledztwie powiązania sprawców przestępstw z pracownikami działającymi w zmowie.

[13] J. Tackett, F. Wolf, G.A. Claypool, *Anonymous reporting mechanism: Hotlines versus Questionaires*, „Internal Auditing" 2005, Nov/Dec 20, 6, s. 32.

Na rysunku 2 przedstawiono nastawienie przedsiębiorców do korzystania z systemu umożliwiającego anonimowe informowanie w organizacji.



Rysunek 2. Czy w firmie działa lub zamierza się wprowadzić system umożliwiający pracownikom anonimowe przekazywanie informacji o zaistniałych nadużyciach gospodarczych[14]

Źródło: Deloitte, *Nadużycia – niewidzialny wróg przedsiębiorstw 2008*, s. 17.

Jak wynika z powyższych badań, tylko 27% przedsiębiorstw posiada system umożliwiającym anonimowe przekazywanie informacji o nadużyciach gospodarczych. Natomiast połowa badanych nie posiada i nie zamierza go wprowadzać lub nie jest w stanie stwierdzić, czy wprowadzi taki system do organizacji.

3. System anonimowego informowania w praktyce

Aby system anonimowego informowania spełniał swoje zadanie, muszą zostać spełnione następujące warunki[15]:

- **dostępność** – kanały informowania, niezależnie od formy, powinny być dostępne poza godzinami pracy firmy, umożliwiając w ten sposób pracownikom przekazanie informacji w warunkach komfortowych i gwarantujących zachowanie prywatności (np. z domu) – optymalnie 24 godziny przez 7 dni w tygodniu,
- **anonimowość** – umożliwienie zachowania anonimowości będzie istotne dla części informatorów, pozostała część zgłoszeń będzie pochodziła od osób, które nie tylko „się przedstawią", ale też będą niekiedy oczekiwać informacji zwrotnej o postępach dochodzenia,
- **podejście –** nie należy podchodzić do informatorów z podejrzliwością, ale raczej z chłodnym i obiektywnym profesjonalizmem; głównym celem powinno być po-

[14] „Nadużycia – niewidzialny wróg przedsiębiorstw" to czwarta edycja badań poświęconych problemowi nadużyć gospodarczych w firmach. Bezpośrednim celem badań było zapoznanie się z opiniami prezesów największych polskich firm na temat zjawiska nadużyć gospodarczych, zebranie informacji o przypadkach nieprawidłowości, z którymi się zetknęli oraz funkcjonujących i planowanych w ich firmach mechanizmach kontroli wewnętrznej, ograniczających ryzyko występowania nadużyć.

[15] www.expolink.co.uk/WhistleblowingHotline/BestPractice.aspx z dnia 23.10.2011 r.

zyskanie istotnych i użytecznych informacji, a nie potwierdzanie czy kwestionowanie zasadności zgłoszenia,
- **koszty** – przekazywanie informacji nie powinno wymagać poniesienia jakichkolwiek kosztów (np. połączeń międzynarodowych) przez informatora; jest to wyraźny sygnał, że firma aktywnie (również finansowo) wspiera przekazywanie informacji przez *whistleblowerów*,
- **bezpieczeństwo** – informatorzy powinni mieć pewność, że przekazane przez nich informacje trafią tylko do wyznaczonych osób w firmie; ochrona danych powinna obowiązywać zarówno w trakcie dochodzenia, jak i po jego zakończeniu,
- **wielojęzyczność** – ma szczególne znaczenie, jeśli np. linia etyczna ma obsługiwać pracowników z różnych krajów; bariera językowa nie powinna zniechęcać pracowników do dzielenia się swoimi wątpliwościami czy informacjami.

Dodatkowo przy wprowadzaniu systemu należy wziąć pod uwagę to, że[16]:
- utworzenie infolinii pozwoli zredukować nadużycia o połowę,
- anonimowe informacje są jedną z głównych metod wykrywania nadużyć w przedsiębiorstwie,
- promowanie systemu anonimowego informowania może stać się elementem środowiska etycznego w przedsiębiorstwie,
- rozszerzenie systemu o osoby z zewnątrz organizacji (dostawców, klientów) pozwoli na lepsze zarządzanie ryzykiem nadużyć,
- skarga/informacja na temat pracownika kadry zarządzającej powinna przejść bezpośrednio do działu audytu.

4. Czy warto zostać *whistleblowerem*?

Według raportu przygotowanego przez Fundację Batorego, osoba, która dostarczyła informacji w dobrej wierze, zarówno instytucji z zewnątrz organizacji, jak i kierownictwu własnego przedsiębiorstwa, bardzo często staje się ofiarą swojego etycznego postępowania. Wśród problemów, z którymi się spotyka, wymienia się najczęściej[17]:
- odsuwanie na „boczny tor"; przesuwanie pracownika na niższe stanowisko, co wiąże się z odcięciem dostępu pracownika do dokumentów i informacji stanowiących źródło niepokojących sygnałów,
- alienowanie od reszty pracowników, marginalizując jego rolę w instytucji i w zespole,
- szykanowanie pracownika, określanego jako „czarna owca",
- odmawianie premii uznaniowej lub pozbawianie prawa do mieszkania służbowego,
- pozwy wobec *whistleblowera* o naruszenie dóbr osobistych,

[16] T.L. Coenen, *Essential of Corporate Fraud*, John Wiley & Sons, New Jersey 2008, s. 151–152.
[17] A. Wojciechowska-Nowak, *Jak zdemaskować szwindel?...*, s. 12–13.

– wypowiedzenie umowy o pracę; najczęstszymi przyczynami wypowiedzenia jest: likwidacja stanowiska pracy, utrata zaufania do pracownika lub jego konfliktowy charakter.

Rolę *whistleblowingu* osłabia brak dostatecznej ochrony prawnej na gruncie prawa pracy, ale również przepisy procedury karnej. Demaskator nie mieście się w wąskiej definicji pokrzywdzonego. Sąd Najwyższy stwierdza bowiem, że „pokrzywdzonym może być w procesie karnym jedynie ten, kogo przestępstwo dotyka bezpośrednio, naruszając lub zagrażając w taki sposób jego dobru prywatnemu, chronionemu przez naruszony przez sprawę przepis"[18]. W świetle tej interpretacji pokrzywdzonym jest pracodawca i jedynie on sam może złożyć zażalenie.

Wyniki raportu *Alternative to silence*[19] (alternatywa dla milczenia) opracowanego przez *Transparency International* wskazują, że w większości przypadków *whistleblowerzy*, znani też pod nazwą demaskatorów, za swoje działania, mające na celu ochronę dobra publicznego, ponoszą wysokie ryzyko osobiste. W 10 przebadanych krajach termin *whistleblower* kojarzony jest z kapusiem, osobą, która dostarcza informacji dotyczących sąsiadów, współpracowników i członków rodziny.

Dodatkowo raport prezentuje następujące rekomendacje[20]:

– szerzenie wiedzy o kluczowej roli demaskatorów w ujawnianiu nieprawidłowości,
– stworzenie jednolitych i zrozumiałych ram prawnych dla ochrony *whistleblowerów*, odnoszących się zarówno do sektora prywatnego, jak i publicznego, z jasnymi procedurami raportowania, procedurami pozwalającymi na niezależną ocenę i umożliwiającymi odwołanie oraz odpowiednim zadośćuczynieniem w przypadku negatywnych skutków, jakie ponosi *whistleblower*,
– odpowiednia kadra kierownicza, która zapewni powołanie właściwych kanałów raportowania,
– niezależny podmiot państwowy, odpowiedzialny za zbieranie informacji na temat ilości spraw w tym zakresie, co pozwoliłoby na skuteczny, bazujący na dowodach monitoring i ocenę *whistleblowingu* w każdym kraju Unii Europejskiej,
– wprowadzenie uregulowań zawartych w Konwencji Narodów Zjednoczonych Przeciw Korupcji i Prawnokarnej Konwencji o Korupcji.

Podsumowanie

Ryzyko nadużyć dotyczy zarówno małych, jak i dużych przedsiębiorstw, niezależnie od rodzaju i miejsca prowadzonej działalności gospodarczej. Jest to problem, z którym spotyka się coraz więcej przedsiębiorstw. Brak odpowiedniego systemu informowania

[18] Postanowienie Sądu Najwyższego z 17.11.2005 r., II KK 108/05, OSN w SK 2005/1/2094.
[19] Badania przeprowadzone w 10 europejskich krajach: Bułgaria, Czechy, Estonia, Węgry, Irlandia, Włochy, Łotwa, Litwa, Rumunia i Słowacja.
[20] *Alternative to Silence. Whistleblower Protection in 10 European Countries*, Transparency International, 2009, s. 44–46.

o nadużyciach może przyczynić się do zwiększenia strat w przedsiębiorstwie. Jednak bez skutecznej ochrony prawnej demaskatora każda decyzja osoby będącej świadkiem nadużyć będzie wiązała się z dużym ryzykiem. Decyzja o zawiadomieniu właściwego organu lub przełożonych podejmowana będzie ze świadomością nie tylko ryzyka narażenia się na ostracyzm, ale przede wszystkim na utratę pracy. Dopóki rozwiązania systemowe nie pozwolą na ochronę demaskatora, dopóty wprowadzenie najlepszych rozwiązań w zakresie *whistleblowingu* nie przyniesie wymiernych skutków.

ANONYMOUS SYSTEM REPORT ON CORPORATE FRAUD IN ENTERPRISE – WHISTLEBLOWING

Summary

The article attempts characteristic of anonymous system report on corporate fraud. The author definied the concept of whistlebowing. Then presents the level of fraud in Polish enterprises, in order to indicate the tendency of enterprises to enter anonymous system report in business.

The author presented the rules for implementation of whistleblowing in the organization. At the end of an attempt to identify the risk posed by the decision of becoming a whistleblower.

Translated by Dariusz Pauch