Z zagadnień bezpieczeństwa biznesu

Prace studentów
Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego

Z zagadnień bezpieczeństwa biznesu

pod redakcją
Jerzego Koniecznego

Kraków 2008

Rada Wydawnicza:
Klemens Budzowski, Zbigniew Maciąg, Jacek M. Majchrowski

Recenzja:
prof. dr hab. Maciej Szostak

Projekt okładki:
Joanna Sroka

Redaktor prowadzący:
Halina Baszak Jaroń

ISBN: 978-83-89823-73-1

Na zlecenie:
Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego
www.ksw.edu.pl

Wydawca:
Krakowskie Towarzystwo Edukacyjne sp. z o.o.
Oficyna Wydawnicza AFM, Kraków 2008

Łamanie:
Joanna Sroka

Druk i oprawa:
Eikon Plus

Spis treści

Przedmowa
Dzieci spokojnej rewolucji

Prywatyzacja bezpieczeństwa – w zakresie akceptowanym przez państwo, ale też przez zainteresowane kręgi społeczne – dokonała się w Polsce szybko i sprawnie, patrząc zaś z kilkunastoletniego już dystansu, można powiedzieć, że bardzo sprawnie. Powodów owej sprawności było (i jest) kilka, głównym jednak wydaje się dążenie do racjonalizacji wydatków: demokratyczne państwo rezygnuje z monopolu sprawowania funkcji bezpieczeństwa (w imię przesłanek ideowych i ekonomicznych), zaś wolni obywatele i ich organizacje (lepiej niż biurokracja znający swoje potrzeby) inwestują, w miarę możliwości, sami w swoje bezpieczeństwo. Proces ten, w cywilizowanych krajach, nastąpił w drugiej połowie XX wieku (a w naszej części Europy w jego ostatniej dekadzie) i już dość dawno określony został mianem „spokojnej rewolucji"[1].

Spokojna rewolucja objęła wszystkie dziedziny życia społecznego, ale najsilniejsze piętno odcisnęła na szerokiej sferze zapewnienia bezpieczeństwa w działalności gospodarczej. To biznes, akceptujący w granicach zdrowego rozsądku zasadę, iż bezpieczeństwo jest ważniejsze niż zysk, nie tylko wygenerował powstanie ogromnego rynku produktów

[1] Po raz pierwszy termin „spokojna rewolucja" na określenie prywatyzacji bezpieczeństwa został użyty w pracy: P. Stenning, C. Shearing, *The Quiet Revolution: The Nature, Development and General Legal Implications of Private Security in Canada*, „Criminal Law Quarterly" 1979–80, Vol. 22, s. 240–48 (por. także obszerne omówienie kontekstu w: R. Sarre, *Researching Private Policing: Challenges and Agendas for Researchers*, „Security Journal" 2005, 18 (3), s. 57–70; J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, Warszawa 2004).

i usług, rynku – dodajmy – utrzymującego globalnie stałą i wysoką dynamikę wzrostu, ale też dał impuls do powstania nowej, rozległej dziedziny wiedzy, jaką jest bezpieczeństwo biznesu.

Zarządzanie bezpieczeństwem staje się w Polsce coraz częściej uruchomianym, bo chętnie wybieranym przez młodzież, kierunkiem studiów. Ale bezpieczeństwo biznesu budzi zainteresowanie także studentów innych specjalności, wśród nich, co naturalne, prawników, słusznie widzących w owej, relatywnie – przynajmniej w naszym kraju – nowej dziedzinie pole do popisu w przyszłych karierach zawodowych.

Prace prezentowane w tym tomie powstały w toku działania sekcji bezpieczeństwa Studenckiego Koła Naukowego Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego, w roku akademickim 2005/06. Ich autorami są studenci prawa. Generacyjnie są więc dziećmi wspomnianej spokojnej rewolucji. Z mocną wiarą, że nie grozi im pożarcie ani przez tę, ani przez żadną inną, zachęcam do lektury.

Jerzy Konieczny

Zagadnienia ogólne

Agnieszka Bąk, Andrzej Tokarz

Prewencja kryminalna wobec zagrożeń bezpieczeństwa biznesu

Omówienie tematu prewencji kryminalnej w biznesie należy rozpocząć od określenia grupy społecznej, której zagadnienie to dotyczy. Przedsiębiorcy zajmują się produkcją, handlem, usługami, tworzą nowe miejsca pracy, wytwarzają nowej jakości usługi i produkty rozumiane nie tylko jako wytwory materialne oraz uzyskują z tego tytułu określone zyski. Tym samym społeczność ta narażona jest na różnego rodzaju zagrożenia. Poświęcając uwagę zagrożeniom szeroko pojętego biznesu, należałoby najpierw zastanowić się, czy specjalne traktowanie pewnej grupy społecznej jest celowe i w pewnym sensie etyczne. Przecież zwykły człowiek nieobracający wielomilionowym kapitałem nie może liczyć na to, że na przykład policja będzie organizowała dla niego specjalne, cykliczne szkolenie, jak uniknąć obrabowania na ulicy.

Oczywiście biznesmeni i wysoka kadra menedżerska są bardziej narażeni na pewnego rodzaju przestępstwa z racji swojej zamożności i tego, że nierzadko są osobami publicznymi. Przedsiębiorcy determinują rozwój gospodarczy, tworzą szeroką warstwę społeczną zwaną klasą średnią, która stanowi o stabilności państwa i jego potencjale. Można by powiedzieć, że ta grupa społeczna posiada środki, dzięki którym sama może zwiększyć swoje bezpieczeństwo, wykorzystując do tego na przykład firmy ochrony osób i mienia. Jednakże z tego powodu nie wolno przedsiębiorców wystawiać poza nawias, a wręcz przeciwnie. Z ekonomicznego punktu widzenia to oni decydują o bogactwie kraju i jego obywateli. Dzięki nim państwo może się rozwijać, powstają nowe miejsca pracy, a co za tym idzie jest mniej niepokojów społecznych. Ważnym elementem każdego narodu jest silna i liczna klasa średnia, która zapewnia państwu stabilność. Klasa ta nie głosuje na populistów

i nie wyciąga ręki po pieniądze z budżetu. Tworzą ją zaś głównie przedsiębiorcy i ludzie przez nich zatrudniani.

Biznesmen, który boi się o swoją rodzinę, firmę czy mienie może się zastanawiać, czy nadal inwestować w Polsce, czy przenieść swoją działalność gdzie indziej. Dzięki globalizacji przeniesienie działalności (zwłaszcza produkcyjnej) do innego kraju nie jest takim problemem jak dawniej. A trzeba pamiętać, że zgodnie z zasadami marketingu niezadowolony klient, w tym wypadku „klient" państwa, swoją opinią podzieli się ze znajomymi, a oni przekażą ją własnym znajomym. Napływ kapitału inwestycyjnego, dużych pieniędzy lokowanych w Polsce uzależniony jest właśnie od obszaru, na jakim dana firma ma działać, a dokładnie od tego, jak obszar ten został oczyszczony i przygotowany dla inwestora. Wydaje się, że idealnym polem przyciągającym biznes jest ten obszar, gdzie przestępczość pospolita jest niewielka lub nie ma jej prawie wcale. Oczywiste jest, że zagrożenia te muszą być wkalkulowane w ryzyko inwestowania. Jednakże to, gdzie inwestor zdecyduje się ulokować swoją inwestycję, będzie uzależnione w dużej mierze od stopnia przestępczości w zakresie włamań, kradzieży czy porwań osób dla okupu na danym obszarze. Właśnie dlatego tak ważne jest dbanie w szczególności o przedsiębiorców inwestujących w Polsce oraz tych, którzy się do tego dopiero przymierzają. Dlatego aby nasz kraj rozwijał się w szybkim tempie, potrzebne są nie tylko nowe drogi, przejrzysty system podatkowy, ale także właśnie instytucjonalne działania na rzecz bezpieczeństwa biznesu. Niestety przez całe lata ten problem nie doczekał się instytucjonalnych rozwiązań czy programów. Polscy politycy albo boją się współpracować oficjalnie z biznesem i przeznaczać środki na tego typu działania, albo po prostu nie są tym zainteresowani. Można zrozumieć strach przed specjalnym traktowaniem bogatych, ludzie zamożni nigdy nie byli w Polsce pozytywnie postrzegani i próby pójścia im na rękę mogłyby być źle odebrane przez wyborców. Dzieje się to jednak kosztem finansów państwa, utraty inwestycji zagranicznych, a nawet dobrego wizerunku Polski w Europie i na świecie. Bojaźliwość polityków doprowadza do tego, że przestępczość gospodarcza oraz skierowana bezpośrednio przeciwko biznesmenom (na przykład porwania)

rozwija się bez specjalnych przeszkód. Im dłużej to trwa, tym trudniej będzie w przyszłości zwalczyć te zjawiska.

Rozważając kwestie zagrożeń bezpieczeństwa w biznesie, po ustaleniu grupy społecznej, która jest najbardziej predestynowana do wiktymizacji, możemy zacząć mówić o zagrożeniach kryminalnych, które, jak wiemy, są nieodłącznym elementem każdej działalności biznesowej.

Nie sposób oczywiście poruszyć tutaj wszystkich niebezpieczeństw czyhających na biznesmenów i ich działalność, ale możemy spróbować podzielić je na pewne kategorie, tak aby można było podjąć odpowiednie działania prewencyjne na nie nakierowane.

Spróbuję teraz dokonać pokrótce podziału zagrożeń biznesu. Niniejszy podział związany jest z poziomą płaszczyzną działania przedsiębiorstw, nie odnosi się on do sfery tworzenia prawa i wpływu czynników na jego tworzenie.

Ogólnie zagrożenia, jakie mogą spotkać szeroko pojęty biznes (nie tylko ludzi, ale i środki, jakimi oni dysponują), można podzielić w sposób bardzo uproszczony na trzy typy kategorii, które nie są jednak zbiorami rozdzielnymi, a tylko podziałem typologicznym:

I. zagrożenia zewnętrzne i wewnętrzne,
II. zagrożenia materialne i niematerialne,
III. zagrożenia bezpośrednie i pośrednie.

Ad I. Do zagrożeń zewnętrznych można zaliczyć każdą umyślną działalność człowieka (niezwiązanego jednak bezpośrednio z firmą) na szkodę przedsiębiorstwa bądź przedsiębiorcy, prowadzącą do ograniczenia możliwości działania biznesu, spowolnienia lub całkowitego zaprzestania działalności. W takim szerokim rozumieniu zagrożenia zewnętrznego będziemy rozumieć wszystkie działania o charakterze kryminalnym *sensu stricto* skierowane bezpośrednio na przedsiębiorcę lub bezpośrednio na jego mienie mające charakter zachowania gwałtownego:

- porwanie dla okupu,
- kradzież majątku prywatnego przedsiębiorcy,
- zniszczenie mienia,

- zabójstwo,
- pomówienie firmy,
- pomówienie produktu,
- sabotaż zlecony pracownikowi.

W szerszym ujęciu można by też do zagrożeń zewnętrznych zakwalifikować przestępstwa dokonane na partnerach biznesowych, urzędnikach i innych osobach mających wpływ na działalność przedsiębiorstwa:

- szantaż w stosunku do osoby bliskiej,
- szantaż w stosunku do osoby zajmującej istotne z punktu widzenia strategicznego firmy miejsce,
- pomówienia, w których zostaje zachwiana wiarygodność i pozycja firmy na rynku,
- pomówienia, w których zostaje zachwiana wiarygodność danego produktu na rynku,
- działanie na szkodę firmy (będące w istocie swoistą formą sabotażu), na przykład poprzez wprowadzenie do firmy osoby, która obdarzona szczególnym zaufaniem (na przykład księgowy) doprowadza do ograniczenia jej działalności lub upadku.

Do zagrożeń wewnętrznych zaliczymy natomiast każde zachowanie pracowników firmy, umyślnie działających na jej szkodę z chęci zysku bądź zemsty.

Owe zachowanie mogą polegać na przykład na:

- kradzieży,
- sabotowaniu działań firmy,
- fałszowaniu produktów,
- niszczeniu mienia,
- sprzedawaniu informacji konkurencji.

Podział ten nakłada się w pewien sposób na siebie, lecz jego istotą jest kwestia podejścia do biznesu lub przedsiębiorstwa jako pewnego obszaru działania zespołu ludzkiego. W takim rozumieniu możliwe jest, że cele działalności człowieka pokrywają się mimo różnych motywów.

Omawianie problemu nielojalnych bądź po prostu nieuczciwych pracowników należy zacząć od stwierdzenia, że nadal żyjemy w kra-

ju postkomunistycznym, a co za tym idzie większość pracowników „etosu pracy" nauczyło się jeszcze za czasów państwa pseudokomunistycznego.

W tamtym okresie wyniesienie z pracy worka cementu czy nawet odkurzacza było raczej powodem do dumy niż wstydu. U wielu ludzi takie postawy nadal nie budzą oburzenia. Niedawno media donosiły, że w firmie jednego z największych producentów okien ogromną część produkcji (wartej wiele milionów złotych) pracownicy sprzedawali na boku. Nie byłoby to tak wyjątkowe, gdyby nie to, że w procederze uczestniczyli wszyscy: od szeregowych pracowników po najwyższą kadrę menedżerską. Dodatkowo wielkim problemem wielu polskich firm jest to, że rozwijały się one zbyt szybko i większość nie zdołała przystosować swojego systemu zarządzania do wielkości przedsiębiorstwa. Stąd na przykład oszustwa w magazynach firmowych są wykrywane zbyt późno, a czasem nie da się postawić pracownikowi żadnych zarzutów, ponieważ nie ma dowodów jego nieuczciwości – brak bowiem odpowiednich systemów zabezpieczeń i kontroli. Niczym wyjątkowym nie jest firma, w której dwaj kierowcy w ciągu paru miesięcy dorabiają się własnych sklepów, mając przez pół roku towar za darmo, który „wzięli" sobie z magazynu, a nikt nie zwrócił na to uwagi. Producent mimo to nie wprowadził żadnych systemów bezpieczeństwa, bo straty przy gwałtownym rozwoju firmy nie były aż tak znaczne. Prawdopodobnie w krajach starej Unii Europejskiej przy dużej konkurencji nie mógłby sobie pozwolić na taką rozrzutność.

W obrębie wspomnianych zagrożeń w sensie *largo* nie wspomniano o innych, a więc takich, co do których charakter działania nie musi nosić znamion umyślności i wynika z szeregu nakładających się elementów: z obowiązującego i wprowadzonego prawodawstwa, specyfiki i charakteru danego rynku oraz grup nacisku zwanych lobby.

Podstawowym uwarunkowaniem kształtującym rozwój przedsiębiorczości jest trwałość, stabilność i niezmienność obowiązującego prawa (w konsekwencji można przejść do wyższego poziomu zagrożeń, tj. sfery tworzenia prawa, będącego w istocie poza opinią publiczną a zatem miejscem, w którym grupy nacisku – formalne lub nieformalne

– realizują swoje dalekosiężne plany związane ze strategią firmy, przedsiębiorstwa lub korporacji poprzez naciski na podmioty tworzące prawo).

W takim ujęciu zagrożenia kryminalne można rozszerzyć na elementy nieuprawnionego i pozaprawnego działania zewnętrznego skierowanego na jednego przedsiębiorcę lub grupę biznesmenów, którego zamiarem jest wyróżnienie firmy, przedsiębiorstwa, korporacji w celu zdominowania danego rynku. W takim postrzeganiu przestrzennym zagrożenia zewnętrzne i wewnętrzne są wynikiem nacisku pewnych grup, których celem nie jest wyrządzenie krzywdy danej osobie (a poprzez to osłabienie jej kondycji), lecz zmarginalizowanie działania biznesu w pewnym określonym obszarze rynkowym, eliminacja bądź uzyskanie informacji o możliwych zmianach, które – biorąc pod uwagę szybkość dostępu do informacji, implikują możliwość dostępu i wpływu na dany rynek – stwarzają warunki do eliminacji konkurencji (kto ma informację, ten ma władzę). Kwestia dotyczy tych fragmentów działalności biznesowej, która odcięta lub pozbawiona bieżącej, szybkiej i pewnej informacji – ulega deprecjacji i rugowaniu z rynku. Szybkość uzyskania informacji jest elementem decydującym o funkcjonowaniu firmy/przedsiębiorcy/biznesmena na danym rynku, a zatem powszechność i jednakowa dostępność ważnych informacji jest kluczowa dla możliwości działania jej w danym obszarze. Gdyby spojrzeć na tę przestrzeń w latach 70., 80. i początku lat 90. XX wieku, to nie miałaby ona racji bytu. Jednakże ze względu na wzrost technologiczny oraz elementy globalizacji od połowy lat 90. szybkość w dostępie do informacji ma ogromny wpływ na usadowienie i pozycję przedsiębiorcy, biznesmana, firmy na danym rynku. Ponadnarodowe korporacje działające od wielu lat na obszarze całego globu stworzyły system, w którym niestabilność w jednym rejonie kompensowana jest zyskami w drugim, tym samym eliminując możliwość wyrugowania z rynku. Warunkiem koniecznym jest jednak dostęp do informacji w danym regionie lub obszarze działania. Odbiór społeczny pewnych zachowań nie odzwierciedla prawdziwych motywów działania sprawcy, gdy mamy do czynienia z porwaniem i zabójstwem. Wówczas w oczach społeczeństwa kreuje się element zbrodni zabójstwa. Tymczasem motywem mogą być elemen-

ty biznesowe: tym samym w konfrontacji zabójstwo – motyw ucieka element prawdziwego celu działania sprawcy. Oczywiście wpływ na te determinanty zachowań ludzkich ma:

- stopień zamożności społeczeństwa,
- możliwości prawne w powstawaniu nowych konkurencyjnych firm,
- stabilna polityka fiskalna państwa,
- stabilność i przewidywalność w celach krótkoterminowych i średnioterminowych zmian o charakterze polityczno-gospodarczym,

Kwestie te w sposób oczywisty mają wpływ na sfery:

- wpływów zmian podatkowych na strukturę przestępstw,
- wpływu możliwości zatrudniania i bezrobocia na motywy zachowania potencjalnych sprawców przestępstw,
- możliwości przenoszenia działalności gospodarczej poza obszar danego państwa.

Mówiąc o zagrożeniach, należy wspomnieć o takich działaniach, które nie są związane bezpośrednio z przestępczością pospolitą. Tym niemniej obserwując polską scenę gospodarczą z kilkunastu lat w Polsce, można zauważyć trendy, z których wnioskować można o potencjalnych kierunkach zagrożeń niebędących jeszcze *stricte* kryminalnymi, ale w przyszłości mogącymi takimi się stać. Chodzi tutaj o masowość tworzonego prawa gospodarczego, nowelizację przepisów, wprowadzanie zmian i dodatków (zarówno w obrębie działalności gospodarczej, jak i sferze podatkowej). Szybkość dostępu do tej informacji określonej grupy osób (biznesmenów) i jego pozaprawnego wykorzystania. Typowym przykładem może być sprawa tzw. oscylatora bankowego. Zagrożenia te płyną z zewnątrz niezależnie od woli właściciela i prowadzą wprost do zagrożeń o charakterze kryminalnym.

Ad II. W drugiej kategorii zagrożeń, tj. materialnych i niematerialnych, uwaga została skupiona na celu działania sprawcy.

W przypadku celowego działania osoby lub grupy osób przedmiotem zamachu mogą być rzeczy materialne oraz pieniądze. Głównym celem działania sprawcy jest uzyskanie korzyści kosztem danego bi-

znesmena. Do takich przestępstw można zaliczyć kradzieże, włamania, przywłaszczenia. Jeżeli celem działania sprawcy jest inna wartość chroniona prawem (nie tylko karnym oczywiście), na przykład intelektualna, autorska, informacja, tajemnica oraz zdrowie i życie, możemy mówić o zagrożeniach niematerialnych.

Dla tego podziału z punktu widzenia strat nie jest istotne, czy zagrożenia płyną z zewnątrz przedsiębiorstwa, czy z jego wnętrza poprzez pracowników tam zatrudnionych, niemniej jednak z punktu widzenia działań prewencyjnych rozróżnienie to jest bardzo istotne.

Ad III. Trzeci podział zagrożeń bezpośrednich i pośrednich obejmować może właściciela, jego firmę bez pośrednictwa osób trzecich albo mechanizmy, za pomocą których może powstać zagrożenie dla działania firmy.

W pierwszym przypadku obejmować one będą (w rozumieniu kryminalnym) na przykład porwania dla okupu, zabójstwa, włamania, kradzieże, pobicia, wymuszenia, niszczenie mienia. W drugim przypadku zagrożenia pośrednie mogą być wywołane przez tzw. czynnik ludzki (wprowadzenie do firmy osoby z konkurencji, której celem będzie przekazywanie informacji na temat strategii, lub też działalność prowadzącą do jej upadku, na przykład podstawiony księgowy) lub też poprzez urządzenie, przepis pozwalający sprawcy na ingerencje w zastrzeżony obszar działalności firmy na przykład poprzez użycie podsłuchu, nieuprawnione włączenie się do sieci teleinformatycznej, zablokowanie lub wykorzystanie dostępu do informacji, która we współczesnym świecie jest rzeczą najcenniejszą, o dużym popycie i najbardziej narażoną na przestępstwo.

W dobie funkcjonowania poczty elektronicznej i powszechnego korzystania z usług sieci teleinformatycznej z perspektywy biznesu największe zagrożenie dla przedsiębiorstw niosą systemy elektroniczne. Zatem minimalizacja zagrożeń związanych z ciągłym działaniem systemów informatycznych jest priorytetem każdej firmy, która może stać się obiektem działania hakerów. Nieistotne jest, czy zagrożenie włamaniem do sieci wypływa z zabawy indywidualnej osoby czy też

jest planowanym, celowym zabiegiem mającym na celu pozyskanie informacji dla siebie lub innego przedsiębiorstwa. Istotą rzeczy jest prewencja związana z prawidłowym zabezpieczeniem przetwarzania i gromadzenia danych, jakimi się dysponuje. Trzeba wspomnieć, że teleinformatyczne systemy zabezpieczeń są coraz doskonalsze, ale w ślad za ich doskonałością idzie odpowiednia cena, a pomysły hakerów są wręcz nieograniczone. Polska pod względem zabezpieczeń gromadzonych danych jest niestety krajem zacofanym. Pewnymi pozytywnymi krokami w tym względzie są wprowadzone w życie ustawy o ochronie danych osobowych i ochronie informacji niejawnych, które określają stopień jawności informacji. Jednakże w ślad za tym ze względu na braki finansowe nie idzie budowa baz danych, systemów zabezpieczeń i specjalnie chronionych pomieszczeń. Koszty budowy takich pomieszczeń są zbyt wysokie, co niewątpliwie wpływa na zagrożenie kryminalne biznesu.

Czy w Polsce możemy mówić o prewencji kryminalnej w biznesie? Zdania na ten temat są podzielone. Tak – jeśli dotyczy to sfery prywatnej, w której przedsiębiorca sam podejmuje działania w kierunku zabezpieczenia swoich interesów: zatrudnia agencje ochrony osób i mienia, buduje swoje wewnętrzne struktury odpowiedzialne za bezpieczeństwo w jego firmie, inwestuje w technikę itd. Jednak kiedy przypatrzymy się prewencji kryminalnej Policji skierowanej na działalność biznesową, to na powyższe pytanie nie da się odpowiedzieć twierdząco.

Przy opracowywaniu niniejszego referatu sięgnięto do informacji zawartych w *Kryminalistyce* prof. Brunona Hołysta. Interesujące dane dotyczą ilości funkcjonariuszy policji państwowej w porównaniu z liczbą funkcjonariuszy służb ochrony w danym kraju. Celem porównania wybrano kilka państw o podobnej lub zbliżonej powierzchni oraz liczbie ludności i tak w Niemczech na około 263 tys. policjantów przypada 168 tys. funkcjonariuszy prywatnych służb ochrony, we Włoszech na około 278 tys. policjantów tylko 25 tys. funkcjonariuszy prywatnych służb ochrony, w Hiszpanii na około 179 tys. policjantów przypada 71,5 tys. pracowników ochrony, a w Wielkiej Brytanii na około 185 tys. policjantów przypada 200 tys. pracowników służb ochrony. W Polsce proporcje te wynoszą odpowiednio około 105 tys. policjan-

tów na 200 tys. pracowników ochrony, natomiast w Turcji 175 tys. policjantów i 82 tys. pracowników ochrony. Wskazane liczby pokazują, że kraje zamożne, bogate, o ustalonym typie demokracji (na przykład Niemcy, Włochy, Hiszpania) posiadają ponaddwukrotnie większą lub prawie dwukrotnie większą liczbą policjantów w stosunku do liczby prywatnych służb ochrony, jedynym wyjątkiem w tej grupie jest Polska (państwa mniejsze takie jak Czechy lub Węgry nie zostały porównane z Polską). Charakterystyczne jest to, że transformacja ustrojowa w Polsce zezwoliła na niekontrolowany wypływ i rejestrację służb pomocniczych. Z analizy przedstawionej w cytowanej pozycji wynika, że kraje zachodnioeuropejskie w pierwszym rzędzie inwestują w bezpieczeństwo publiczne, tj. Policję, dając jej odpowiednie środki i narzędzia techniczne, a dopiero dalej w inne służby pomocnicze uzupełniające powstałe na rynku nisze. Nawet Turcja, której PKB jest niższy niż PKB Polski przy nieco większym potencjale ludzkim (około 58 mln. osób), ma dużo większą liczbę policjantów i znacznie mniej rozbudowane prywatne służby pomocniczej ochrony. Jeżeli weźmiemy pod uwagę zaawansowanie techniczne i technologiczne tych krajów, specjalizacje komórek, stabilność legislacyjną, poziom szkolenia dotyczący bezpieczeństwa publicznego, to Polska jawi się jako kraj upośledzony. Odziedziczyła ona w roku 1990 przestarzałą strukturę administracyjną, nadmiernie rozbudowany system administracyjno-logistyczny, słabą bazę szkoleniową. Cechuje ją zapaść technologiczna i techniczna, brak możliwości bezpośredniego i szybkiego wpływania na zmiany o charakterze legislacyjnym adekwatne do aktualnych potrzeb i zmiennych realiów rynku.

Zauważalna jest dysproporcja w liczbie przypadających policjantów na 100 tys. mieszkańców w każdym z wymienionych krajów, jasno określone reguły i procedury postępowania w sprawach zagrożeń biznesu oraz precyzyjny podział zadań dla poszczególnych pionów (segmentów) policji kryminalnej. Polska po wejściu do Unii Europejskiej ma niezwykle trudne zadanie, by nadążyć za już utrwalonymi standardami europejskimi. Poza niewłaściwą strukturą organizacyjną, brakiem systemu motywacyjnego ostrej krytyce poddawany był cały system szkolenia policji świadczący o jej słabej mobilności i sprawności działania,

brak odpowiedniej kadry otwartej na nowe sposoby i metody szkolenia, brak środków technicznych do realizacji tych zadań, a w konsekwencji brak osób, których poziom wiedzy, doświadczenie, umiejętności i kompetencje pozwalałyby na wyławianie najzdolniejszych pracowników Policji. W tzw. sekcjach przestępczości gospodarczej często są zatrudniani ludzie przypadkowi z ograniczoną wiedzą, bez chęci samokształcenia, a także są nieodpowiednio motywowani. Zwrócić jednakże należy uwagę, że nie jest wystarczające podjęcie takich kroków, które zakładają przyjęcie do pracy w danym pionie policji osoby tylko ze względu na profil szkoły, jaką ukończyła. Często praca policyjna w zakresie zapobiegania przestępczości biznesowej wymaga umiejętności łączenia posiadanej wiedzy ze specyfiką pracy policji, pomysłowości w realizowaniu zadań. Tymczasem policja z wyżej wymienionych względów nie jest w stanie racjonalnie zajmować się zagrożeniami, tym bardziej że nie jest w stanie nadążyć za stale zmieniającymi się realiami i ewolucją współczesnego świata. Jej działania mają być uzupełniane przez szeroko rozumiany rynek ochrony pojęciowo obejmujący zarówno kwestie detektywistyczne, jak i ochrony osób i obiektów. Wydaje się, że Polska popełniła poważny błąd, zezwalając po roku 1990 na powstanie nie do końca kontrolowanego rynku usług detektywistycznych, z którego w pierwszej kolejności zaczęły korzystać osoby będące w przeszłości funkcjonariuszami służb policyjnych). Z perspektywy lat wydaje się, że nie do końca sprecyzowane przepisy dotyczące tego rynku spowodowały, że podejmując działalność prewencyjną, agencje ochrony skupiały się przede wszystkim na zagarnięciu jak największej części rynku, nie zaś na jakości świadczonych usług i ich profesjonalizmie. Jednocześnie powszechne stało się ze względów ekonomicznych zatrudnianie do tzw. ochrony obiektów emerytów bądź rencistów, którzy zazwyczaj nie mają wysokiej sprawności fizycznej. Również niektóre stosowane obecnie techniczne metody ochrony obiektów nie do końca mogą zostać praktycznie wykorzystane do wykrycia ewentualnego przestępstwa – monitoring w bankach czy na stacjach benzynowych montowany jest często w nieodpowiednich miejscach, jakość obrazu jest tak słaba, że nie pozwala nawet w przybliżeniu na identyfikację ewentualnego sprawcy

przestępstwa. W odróżnieniu od Polski wszystkie kraje poza państwami Europy Środkowowschodniej nie zezwoliły na rozbudowanie służb prywatnych w sposób niekontrolowany i taki, który powodowałby, iż liczba pracowników tych służb byłaby większa od liczby funkcjonariuszy policji. Zaletą takiego podejścia jest to, że służby mundurowe jako reprezentujące państwo w sferze bezpieczeństwa w pierwszej kolejności dbają o spokój społeczny między innymi poprzez profesjonalne przygotowanie i zaplanowane działania. Żadne z tych państw nie oddało tego bezpieczeństwa tak łatwo jak Polska w ręce prywatne. Istotą myśli było to, że to państwo ma gwarantować bezpieczeństwo obywatelom i przedsiębiorcom, a służby prywatne mogą być jedynie dla nich uzupełnieniem. Ponadto zachowują one kontrolę, która w sposób bardziej rygorystyczny i jednoznaczny przydziela i odbiera koncesje na prowadzenie takiej działalności (której istotą jest również dostęp do informacji). W Polsce zamiast wzmacniać w pierwszej kolejności Policję, w latach 90. źle oceniono zagrożenia płynące z przestępczości i oddano rynek w sposób mało kontrolowany w ręce prywatne, uznając, że wolny rynek dopuszcza sytuacje, w których i ten obszar, tj. bezpieczeństwo publiczne, może być przedmiotem obrotu, za usługi bowiem się płaci. Tymczasem Policja, która w głównym nurcie powinna stać się realizatorem programu profilaktyki bezpieczeństwa, od kilkunastu lat posiada niezmienną (z małymi wahaniami) liczbę funkcjonariuszy, którzy z roku na rok muszą się zajmować coraz większą liczbą zdarzeń o charakterze kryminalnym, w tym godzących w bezpieczeństwo w biznesie. Ponadto policjanci oraz funkcjonariusze prywatnych służb ochrony zamiast współpracować, nierzadko konkurują ze sobą, co ma bezpośrednie przełożenie na poziom bezpieczeństwa biznesu.

Z uwagi na ciągły wzrost przestępczości przeciwko szeroko pojętemu biznesowi odnotowanej w ostatnich latach, w 2000 postanowiono kompleksowo zająć się tematyką prewencji kryminalnej w biznesie. Zadania tego podjęło się Biuro Służby Prewencyjnej Komendy Głównej Policji w Warszawie, które nawiązało współpracę z Brytyjsko-Polską Izbą Handlową (British Polish Chamber of Commerce – BPCC) w celu wdrożenia pilotażowego programu „Bezpieczeństwo w biznesie".

Program został opracowany w 2000 roku i realizowany do roku 2003.

Przyczyny wdrożenia programu „Bezpieczeństwo w biznesie":

- wzrost liczby zdarzeń kryminalnych skierowanych przeciwko podmiotom gospodarczym,
- wzrost liczby zdarzeń kryminalnych skierowanych przeciwko przedstawicielom biznesu i ich rodzinom,
- straty bezpośrednio związane z popełnionymi przestępstwami, jakie ponoszą firmy i osoby w nich zatrudnione,
- straty pośrednie:
  - zmniejszenie wpływów podatków do budżetu państwa,
  - zawieszanie lub ograniczanie działalności gospodarczej,
  - przenoszenie działalności gospodarczej poza terytorium Polski,
  - wzrastające bezrobocie,
  - ograniczenie rozwoju gospodarczego kraju, zmniejszenie zamówień dla kooperantów krajowych działających na rzecz zakładów tworzących produkt finalny,
  - straty z zakresu *public relations* – negatywne postrzeganie Polski jako kraju lokowania inwestycji zagranicznych i prowadzenia działalności gospodarczej.

W ramach programu realizowane były specjalistyczne seminaria z zakresu bezpieczeństwa w biznesie z zaangażowaniem ekspertów Policji oraz osób reprezentujących firmy zrzeszone w BPCC. Odbywały się cykliczne dyżury, tzw. Safe Business Clinics, podczas których można było uzyskać merytoryczną wiedzę i porady z zakresu zapobiegania przestępczości i unikania zagrożeń podczas prowadzenia działalności gospodarczej.

Dzięki temu programowi, spotkaniom i wymianom poglądów z biznesmenami policja miała szansę dowiedzieć się, jakie są ich główne problemy, a także zdobyć zaufanie i współpracowników do dalszych działań.

Przykładowymi tematami spotkań było:

- unikanie zagrożeń w prowadzeniu działalności biznesowej,
- zabezpieczenia firmy,

- profilaktyka unikania zagrożeń,
- bezpieczeństwo osobiste *etc*.

Mimo przygotowania i zorganizowania kilkunastu specjalistycznych seminariów szkoleniowych z zakresu:
- bezpieczeństwa firmy,
- bezpieczeństwa na drodze,
- ochrony informacji niejawnych,
- windykacji należności,
- nadużyć gospodarczych w firmie,
- przestępstw w obrocie gospodarczym i wyłudzeń podatku VAT,
- prania pieniędzy i przestępczości zorganizowanej,
- wysokiej oceny wykładowców w zakresie ich profesjonalizmu,

realizacja takich seminariów jest w istocie bardzo wątłym elementem prewencji kryminalnej w biznesie. Pomijając skromną obsadę, brak jest zaplecza, które kompleksowo zajmowałoby się tą sferą. Nie ma w KGP przygotowanej żadnej strategii działania, która w sposób kompleksowy obejmowałaby podział zagrożeń (przeciwko życiu, mieniu, gospodarczych) w odniesieniu do struktury prowadzonych przedsiębiorstw i działalności gospodarczej, liczby zatrudnionych osób, czasu działania na rynku oraz wypracowanych programów pomocowych, które zwrócone byłyby w kierunku obecnie istniejących i przewidywanych zagrożeń. Ten brak strategii działania obejmujący elementy krótkofalowe, czyli do załatwiania od zaraz, średniofalowe w perspektywie 5–10 lat i długofalowe – powyżej lat 10, zastąpiony został przez szczytne co prawda działania, takie jak działalność Polsko-Brytyjskiej Izby Handlowej, ale oderwane od jakichkolwiek punktów odniesienia stanowiących oparcie dla wypracowania jednolitego planu działania w zakresie prewencji. Zorganizowanie nawet stu konferencji albo seminariów dla wąskiej grupy przedsiębiorców nigdy nie będzie elementem wystarczającym dla metodyki rozwiązywania problemów bezpieczeństwa w biznesie.

Jakkolwiek sam program z punktu widzenia zawartych w nim elementów jest godny naśladowania, to biorąc pod uwagę mizerne środki, jakimi dysponuje Polska, by program ten dotarł do wszyst-

kich osób prowadzących działalność gospodarczą, należy uznać go za co najmniej niewystarczający, a na pewno za program zawieszony w próżni i pozbawiony oparcia. Zwrócić należy uwagę też na to, że wyróżnienie przedsiębiorców, którzy ze względu na swoją pozycję są jedynie administratorami i strategami firmy najczęściej rozumianej jako przedsiębiorstwo duże lub średnie zatrudniające co najmniej kilkaset osób, jest w realiach polskich nietrafne, gdyż struktura powstających firm wskazuje, że ponad 93% z nich to firmy jedno- lub kilkuosobowe, często rodzinne. Firmy te, podobnie jak i te duże, działając w tych samych realiach gospodarczych, obracając jednak dużo mniejszymi pieniędzmi, narażone są na takie same zagrożenia jak firmy średnie, duże i ich właściciele. Dlatego programy takie jak Program Polsko-Brytyjskiej Izby Handlowej nie docierają do nich, a jeżeli nawet, to sposób przekazywania wiedzy na temat zagrożeń często odbiega od możliwości jej przyswojenia.

Na bazie rozwiązań wypracowanych przez program „Bezpieczeństwo w biznesie" planuje się wdrożenie przez Wydział Profilaktyki Społecznej Biura Służby Prewencyjnej KGP ogólnopolskiego programu zapobiegania przestępczości w biznesie. Taki program miałby na celu inspirowanie współpracy policji, izb biznesu, samorządów i przedstawicieli biznesu na rzecz ograniczania przestępczości w tym obszarze.

Współpraca w celu działalności prewencyjnej tych partnerów miałaby polegać między innymi na:

- organizowaniu specjalistycznych seminariów szkoleniowych,
- dyżurach ekspertów policyjnych,
- konsultacjach, doradztwie z zakresu bezpieczeństwa biznesu,
- przygotowywaniu artykułów na ten temat.

Pomimo takich planów program, który objąłby swoim zakresem cały kraj, i kompleks działań przeciwko zagrożeniom biznesu jednak nie powstaje. Nie wiemy, dlaczego tak się dzieje; czy utknął on w Komendzie Głównej Policji, w jej biurokratycznych zakamarkach, czy też po prostu nie dostał politycznego zielonego światła? Szkoda, bo jego powstanie byłoby dobrą wiadomością nie tylko dla przedsiębiorców, ale i dla każdego zainteresowanego rozwojem kraju.

Z punktu widzenia prewencji kryminalnej na poziomie funkcjonowania przedsiębiorstwa na danym rynku podstawą zapewnienia firmie optimum bezpieczeństwa powinien być:

– staranny dobór kadr i pracowników polegający na zatrudnieniu psychologa lub innej osoby, która w trakcie rozmów kwalifikacyjnych, przeprowadzenia testów, będzie w stanie ujawnić prawdziwe i ukryte cele danej osoby chcącej zatrudnić się w przedsiębiorstwie. Bez względu na to, czy będzie to przyszły pracownik fizyczny, umysłowy czy przedstawiciel kierownictwa,

– należy również rozważyć możliwość użycia poligrafu jako jednego ze środków prewencji,

– istotne jest również sprawdzanie opinii danej osoby w poprzednich miejscach pracy,

– zalecić należy prowadzenie szkoleń mających na celu uświadomienie zarówno pracowników, jak i kadrę kierowniczą przed ewentualnymi zagrożeniami,

– powinien istnieć szczegółowy regulamin służący temu, aby pracownicy dokładnie wiedzieli, do czego są zobowiązani na poszczególnych stanowiskach, a jeśli zachodzi taka potrzeba – by podpisali klauzulę tajności,

– w każdej firmie powinien zostać powołany do życia kodeks etycznego postępowania jej pracowników,

– kolejnym ważnym krokiem winno być każdorazowe sprawdzanie partnerów biznesowych, by uchronić się przed nieuczciwymi, a zwłaszcza przed firmami-wydmuszkami,

– powinna powstać baza jawnych informacji na temat firm działających na rynku, dzięki którym można by sprawdzić ich wiarygodność na przykład przed powzięciem decyzji o współpracy. Rolę administratora, dysponenta takiej bazy odgrywałby ustawowo powołany organ. Baza taka miałaby na celu ujawnienie danych na temat działających w danym obszarze firm, jej przedstawicieli, osób, które będąc same właścicielami firm, wielokrotnie omijały prawo lub je łamały. Baza powinna zawierać informacje ustalające wiarygodność finansową firmy, jej dokonania, historię, wszelkie zmiany kierownictwa z odpowiednimi zastrzeżeniami,

a także być zintegrowana centralnie z urzędami skarbowymi, ZUS-em, bankami. Każdy z tych podmiotów mógłby uzyskać informacje w wybranym i dozwolonym zakresie.

Zastrzeżenia dotyczące czasu funkcjonowania firmy, jej kontrahentów, wiarygodności i inne dają możliwość oceny ryzyka przy ewentualnych transakcjach, minimalizując błąd, że dane przedsiębiorstwo ma na celu działania przestępne (oszustwa), a w przypadkach urzędu skarbowego, ZUS-u szybkość działania celem egzekwowania należności bankom dałaby dane ograniczające do minimum ryzyko udzielanych pożyczek. Co prawda, od pewnego czasu funkcjonuje w Polsce Krajowy Rejestr Sądowy, jednakże nie obejmuje on wszystkich firm działających na rynku, działa zbyt krótko, a zakres informacji tam zawartych i udostępnianych publicznie jest zbyt wąski i niewystarczający.

Bardzo istotne jest również zabezpieczenie fizyczne, zwłaszcza ważnych dokumentów, serwerów i miejsc pracy pracowników, których praca ma szczególne znaczenie dla firmy (działy badawcze itp.). Ochrona fizyczna powinna rozpocząć się od wydzielenia obszarów bezpiecznych. Należy stworzyć bariery fizyczne otaczające pomieszczenia firmy. Kolejne bariery tworzyć mają obwody zabezpieczające, na przykład:

- ogrodzenie dookoła budynku,
- ściana, drzwi, zamki w drzwiach,
- brama wejściowa otwierana za pomocą karty,
- recepcja obsługiwana przez człowieka,
- oświetlenie chronionego obszaru,
- kamery telewizji przemysłowej (CCTV),
- systemy alarmowe,
- pracownicy ochrony.

Wiele dużych firm zatrudnia obecnie byłych pracowników służb specjalnych, aby zapewnić sobie kontrwywiadowczą ochronę przed działaniami konkurencji, a także by w razie potrzeby nie musieć zgłaszać się do policji po pomoc, a co za tym idzie nagłaśniać sprawy w mediach, kiedy trzeba przeprowadzić wewnętrzne śledztwo. Zauważyć tu należy, że policja powinna dążyć do jak najlepszego zabezpieczenia się

przed „wyciekami" informacji, aby firmy nie bały się prosić ją o pomoc ze strachu przed ujawnieniem ich tajemnic.

W tym miejscu omówimy rolę mediów w kształtowaniu świadomości zagrożeń w biznesie. Analiza niektórych cykli artykułów prasowych lub programów publicystycznych w telewizji prowadzi do wniosku, że nawet tzw. dziennikarze śledczy nie umieją w sposób interesujący, ale też fachowy pisać o niebezpieczeństwach. Media publiczne powinny kłaść nacisk na edukację społeczeństwa również w zakresie biznesu w różnych aspektach, tymczasem słownictwo, jakim się posługują osoby reprezentujące dane stanowisko, w tym często funkcjonariusze policji (na przykład rzecznicy prasowi policji), może wprowadzać w błąd. Fakt, że we współczesnym świecie informacja ma docierać do odbiorcy w sposób błyskawiczny, zwięzły i agresywny, nie usprawiedliwia braków podstawowej wiedzy prawnej przekazywanej do ogółu społeczeństwa. W telewizji i prasie brakuje takich programów, które w sposób jasny i precyzyjny informowałyby społeczeństwo o możliwościach najbardziej powszechnych zagrożeń oraz o trybie i sposobie reagowania, prawach i możliwościach żądania działania ze strony uprawnionych służb. Nie ma szerokiego dostępu do informacji o tym, co robić, by unikać zagrożeń, oraz co robić, gdy zagrożenie takie występuje. Ponadto informacje prezentowane w mediach są niedopracowane, podawane w taki sposób, jakby całe społeczeństwo składało się z wyjątkowo inteligentnych ludzi. Tymczasem konieczne jest opracowanie takich informacji, które byłyby łatwo przyswajalne również dla mniej wykształconej części społeczeństwa. Oprócz tego brak jest edukacji dotyczącej podstawowej wiedzy na temat bezpieczeństwa. W tym zakresie media publiczne nie realizują elementu prewencji bezpieczeństwa w biznesie.

Nawet w nielicznych programach traktujących o przestępstwach i pracy policji osoby prezentujące przestępstwa posługują się bardzo często językiem potocznym, który nie wyraża ani zakresu podmiotowego, ani przedmiotowego podejmowanych działań lub też oczekiwań. Jednak pomimo dość dużego obiektywizmu programu oderwanego od modelu sensacyjnego nie przekazuje on treści o charakterze zapobiegania przestępstwom.

Wszystkie te założenia dotyczą szeroko pojętego bezpieczeństwa. Oczywiście w zależności od samych firm, ich bezpośredniego otoczenia zewnętrznego i wewnętrznego, wielkości, charakteru prowadzonej działalności skala użytych środków będzie różna.

Trudno wyobrazić sobie, by przedsiębiorca posiadający dwa kioski warzywne próbował wpłynąć jednoosobowo na kształt ustawy lub by stosował zabezpieczenia techniczne z ekonomicznego punktu widzenia zupełnie niepotrzebne, na przykład bramki elektroniczne. Zakres stosowanych środków i metod prewencji powinien być adekwatny przede wszystkim do skali zagrożeń funkcjonujących w danej firmie, w następnej kolejności adekwatny do rachunku ekonomicznego.

Przy omówieniu prewencji kryminalnej w biznesie konieczne jest rozszerzenie tematu o pewne specyficzne dla charakteru polskiej przedsiębiorczości elementy, tj. pewne formy klientelizmu połączonej z płatną protekcją i wręczaniem korzyści majątkowej, nowymi formami działalności, jakimi są giełdy, technologie *high-tech*, a także sposobami zabezpieczeń informacji różnego rodzaju i o różnym charakterze.

Rynek giełdowy jest stosunkowo młodym rynkiem w Polsce. Skupia dużą liczbę firm będących jednocześnie graczami giełdowymi godzących się przy tym na upublicznienie części informacji o sobie, tj. strategii, planowanych działań i przedsięwzięć, osiąganych zysków (generalnie bilansu finansowego). Giełda jako rynek papierów wartościowych skupia uwagę zarówno firm, jak i osób indywidualnych, które będąc graczami, pozostają anonimowe. Działają przez bukmacherów giełdowych, na których również spoczywa szczególna odpowiedzialność ze względu na posiadaną wiedzę oraz szybkość dostępu do informacji. Mimo że giełda w 97% stanowi nadal własność Skarbu Państwa i jest jak na razie tworem dość bezpiecznym, to jednak i tutaj widać potencjalne zagrożenia. Pierwsze wypływają z faktu upublicznienia danych o danej firmie notowanej na giełdzie. Dane te mogą być wykorzystywane przez konkurencję również w sposób kryminalny do osiągania określonych zysków dla siebie lub innej osoby, na przykład kwestia kontroli ruchów akcji lub wykorzystanie informacji o osiąganych zyskach w celach kryminalnych.

Nie sposób opisać wszystkich metod zabezpieczania się przedsiębiorstw przed przestępczą działalnością, gdyż ich ilość jest ogromna. Najważniejsze wydaje się jednak zadbanie o to, by pracownikami firmy zostawały tylko osoby godne zaufania, ponieważ powszechnie wiadomo, że największe niebezpieczeństwo dla każdej firmy stanowi jej pracownik.

Niestety niewiele firm na razie nie zdaje sobie sprawy z tego, że czasem nawet ich fizyczne istnienie nie zależy tylko od dobrych wyników sprzedaży, ale także na przykład od tego, czy zabezpieczają się one przed sfrustrowanym zwolnionym ze stanowiska informatykiem, który wprowadza do bazy danych wirusa bądź kasuje dane i przekazuje je konkurencji.

Reasumując, warunkiem koniecznym do zabezpieczenia się przed tego i innego rodzaju atakami na firmę i jej właścicieli (menedżerów) są przede wszystkim daleko posunięta OSTROŻNOŚĆ przedsiębiorców oraz współpraca z policją, a także zadbanie przez zarządzających firmą o stworzenie takich warunków, w których dokonanie przestępstwa będzie utrudnione lub wręcz niemożliwe. Im więcej działań prewencyjnych zostanie przez nas podjętych, tym bardziej potencjalny napastnik będzie zniechęcony do przestępstwa – bądź ze względu na możliwość szybkiego i skutecznego wykrycia, bądź ze względu na niewspółmiernie wysokie sankcje.

Paweł Pomorski

Bezpieczeństwo biznesu w opiniach przedsiębiorców

Cel badania

Badanie bezpieczeństwa biznesu ujęto w szerokim kontekście, aby ukazać ogół problemów, z jakimi muszą zmagać się przedsiębiorcy, w tym przypadku w województwie małopolskim. Małopolska, choć nie w całej swej rozciągłości geograficznej, jest regionem silnie rozwiniętym gospodarczo. Jednym z największych problemów małopolskich przedsiębiorców (a także przedsiębiorców z pozostałych polskich województw) jest bezpieczeństwo. Zarówno bezpieczeństwo w obliczu zewnętrznych przestępstw kryminalnych, jak i – a może przede wszystkim – bezpieczeństwo wewnątrz firm. Omawiane tu badanie przedstawia obawy pracodawców, ich sposoby uchronienia się przed niebezpieczeństwami, tymi spoza firmy oraz wewnątrz niej. Porusza także kwestie współpracy ze specjalistami, jak i współpracy z państwem w zakresie bezpieczeństwa.

Badanie miało również na celu wykazanie zależności pomiędzy różnymi czynnikami wynikającymi z pytań dotyczących bezpieczeństwa, a także pomiędzy nimi a oględnymi danymi na temat ankietowanych przedsiębiorstw.

Czym jest bezpieczeństwo biznesu?

Co rozumieć przez termin „bezpieczeństwo biznesu"? W języku polskim słowo bezpieczeństwo oznacza „stan niezagrożenia, pewności tudzież spokoju". Biznes to z kolei interes, przedsięwzięcie przynoszące zysk; potocznie mianem biznesu określa się również firmę realizującą takie przedsięwzięcie. W niniejszym tekście sformułowanie „bezpieczeństwo biznesu" będzie oznaczać „stan niebędący zagrożeniem (a także metody do takiego stanu prowadzące) dla działań człowieka podejmowanych w celu osiągnięcia korzyści majątkowej".

1. Metoda badania

Badanie przeprowadzono na grupie przedsiębiorców z sześciu miast Małopolski według klucza liczby mieszkańców w pięciu przedziałach (I: do 10 000 mieszkańców; II: 10 000–50 0000 mieszkańców; III: 50 000–100 000 mieszkańców; IV: 100 000–250 000 mieszkańców; V: powyżej 250 000 mieszkańców). Miasta te zostały wybrane również ze względów geograficznych, albowiem reprezentują różne regiony województwa małopolskiego.

Pierwsza część ankiety składała się z pięciu pytań określających, na ile to możliwe, zarys firmy. W odpowiedzi na pytanie dotyczące rodzaju firmy (pytanie nr 1) w razie wielokrotnego zakreślenia oznaczano jako rodzaj firmy odpowiedź „mieszana". Druga część składała się z czternastu pytań z dwoma odpowiedziami na zasadzie „TAK albo NIE" (pytania 1–13, 16) oraz dwóch z trzema możliwymi odpowiedziami na zasadzie „PIERWSZE albo DRUGIE, albo TRZECIE" (pytania 13 i 14). Wszelkie odpowiedzi z więcej niż jednym zakreśleniem w pytaniach nr 14 oraz nr 15 zatratowano jako nieważne. Uznanie całej ankiety za nieważną sprowadzało się do anulowania tego formularza, w którym nie udzielono poprawnej odpowiedzi na trzy lub więcej pytań oraz takiego, który wrócił niewypełniony.

Następnie sprawdzono zależności pomiędzy odpowiedziami na pytania i usytuowano je w tabelach czteropolowych. Hipotezy testowane były za pomocą testu na χ^2 przy poziomie istotności α=0,05, gdzie próg zależności wynosił 3,841. Pytania, gdzie było trzy lub więcej odpowiedzi, dostosowywano do modelu kwadratu 2x2, łącząc niektóre odpowiedzi w sposób dający najmniejszą możliwość podważenia takiego wyboru (np. podział miejscowości na te do 50 000 mieszkańców i powyżej 50 000 mieszkańców).

2. Jak traktować ankietę?

Ankieta nie jest i nie może być w pełni istotna dla badania zagadnienia, choćby z racji nieobjęcia nią wszystkich pożądanych dla przeprowadzenia badań przedsiębiorców. Ponadto domniemywać należy, że nie wszystkie odpowiedzi zaznaczone przez respondentów były zgodne

z prawdą. Wynikać to mogło zarówno z niezrozumienia pytania, jak i z celowego działania.

Należy zwrócić uwagę, iż za każdym razem, gdy w niniejszym opracowaniu ankiety padną słowa „każdy", „żaden" itp., oznaczać to będzie odniesienie tylko i wyłącznie do ogółu przedsiębiorstw biorących udział w ankiecie.

Poniżej zamieszczono treść ankiety.

ANKIETA

CZĘŚĆ I. Przedsiębiorstwo

1. Jakiego rodzaju przedsiębiorstwem Pan/Pani zarządza?
□ Usługowe □ Handlowe □ Produkcyjne □ Mieszane

2. Ilu pracowników zatrudnia przedsiębiorstwo, którym Pan/Pani zarządza?
□ Do 50 pracowników □ 51–250 pracowników □ Powyżej 250 pracowników

3. Kto jest właścicielem przedsiębiorstwa przez Pana/Panią zarządzanego?
□ Kapitał polski □ Kapitał zagraniczny □ Kapitał mieszany

4. W jak dużej miejscowości znajduje się przedsiębiorstwo przez Pana/Panią zarządzane?
□ Do 10 000 mieszkańców □ 10 000–50 000 mieszkańców
□ 50 000–100 000 mieszkańców □ 100 000–250 000 mieszkańców
□ Powyżej 250 tysięcy mieszkańców

5. Czy przedsiębiorstwo przez Pana/Panią zarządzane prowadzi wymianę handlową zagraniczną (w rozumieniu „Polska–świat")?
□ Tak □ Nie

CZĘŚĆ II. Bezpieczeństwo w przedsiębiorstwie

1. Czy zagadnienie szeroko rozumianego zapobiegania przestępczości jest priorytetem w zarządzanym przez Pana/Panią przedsiębiorstwie („Czy bezpieczeństwo jest ważniejsze niż zysk")?
□ Tak □ Nie

2. Czy dla ochrony własnego przedsiębiorstwa korzysta Pan/Pani z usług zewnętrznej firmy ochrony usług i mienia?
□ Tak □ Nie

3. Czy ogólnie rzecz biorąc, ufa Pan/Pani swoim pracownikom?
□ Tak □ Nie

4. Czy w zarządzanym przez Pana/Panią przedsiębiorstwie zatrudnieni są specjaliści selekcjonujący kandydatów na pracowników?
□ Tak □ Nie

5. Czy w zarządzanym przez Pana/Panią przedsiębiorstwie prowadzone są specjalistyczne szkolenia pracowników w zakresie profilaktyki antyprzestępczej?
□ Tak □ Nie

6. Czy w przedsiębiorstwie przez Pana/Panią zarządzanym po zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę przedsiębiorstwa zmieniane są każdorazowo kody dostępu, zamki itp.,
z którymi pracowała zwolniona osoba?
□ Tak □ Nie

7. Czy w przedsiębiorstwie przez Pana/Panią zarządzanym prowadzony jest poufny wywiad środowiskowy wśród pracowników dotyczący zjawisk patologicznych (np. kradzieży pracowniczych)?
□ Tak □ Nie

8. Czy w zarządzanym przez Pana/Panią przedsiębiorstwie prowadzona jest kontrola i ewidencja dostępu pracowników i gości (identyfikacja osób, ruch osobowy poza godzinami pracy itp.)?
□ Tak □ Nie

9. Czy przedsiębiorstwo przez Pana/Panią zarządzane znajduje się w okolicy o dużym natężeniu przestępczości kryminalnej (włamania, rozboje itp.)?
□ Tak □ Nie

10. Czy w przedsiębiorstwie przez Pana/Panią zarządzanym dokonywana jest archiwizacja kopii bezpieczeństwa danych?
□ Tak □ Nie

11. Czy w zarządzanym przez Pana/Panią przedsiębiorstwie niszczone są zbędne dokumenty w sposób niedopuszczający do ich ponownego odtworzenia?
□ Tak □ Nie

12. Czy w przedsiębiorstwie przez Pana/Panią zarządzanym zakres tajemnicy przedsiębiorstwa określany jest w odrębnym, specjalnym dokumencie?
□ Tak □ Nie

13. Czy w sprawach bezpieczeństwa firmy korzysta Pan/Pani z kontaktów ze specjalistami spoza Pana/Pani firmy?
□ Tak □ Nie

14. Czy informuje Pan/Pani organy ścigania o wszystkich przestępstwach popełnionych przez Pana/Pani pracowników?
□ Nie □ Tylko wówczas, gdy działania na własną rękę okażą się nieskuteczne lub niewystarczające
□ Niezwłocznie w każdym przypadku

15. Czy dotychczasowa praktyka zarządzania przedsiębiorstwem przekonała Pana/Panią, iż największym zagrożeniem dla bezpiecznej działalności firmy jest:
□ Brak lojalności pracowników □ Przestępcze zagrożenie zewnętrzne
□ Zmowa pracowników z osobami spoza firmy

16. Czy ogólnie rzecz biorąc, uważa Pan/Pani, iż organy państwa w należytym stopniu zapewniają warunki do wspierania biznesu?
□ Tak □ Nie

Ogólne omówienie wyników

Z wysłanych 300 ankiet wróciło 65 uznanych za ważne (według wcześniej omówionego schematu), czyli 21,7% całości, co daje efekt zadowalający, albowiem średnia zwracalność ankiet oscyluje wokół 13,0%. Ankiety najczęściej wypełniali przedsiębiorcy z tzw. branży mieszanej (36,9%) oraz usługowej (35,4%), rzadziej handlowej (15,4%) oraz produkcyjnej (12,3%). Aż w 81,5% są to firmy zatrudniające do 50 osób, tylko 4,6% zaś to przedsiębiorstwa zatrudniające ponad 251 osób, pozostałe 13,8%

stanowią firmy zatrudniające więcej niż 51, a mniej niż 250 pracowników. 93,8% z ogółu przedsiębiorstw ma polski wkład kapitałowy, natomiast wkład kapitałowy zarówno zagraniczny, jak i mieszany wynosi po 3,1%. Najwięcej ankiet nadeszło z miasta o liczbie ludności pomiędzy 10 000––50 000 mieszkańców (32,3%), najmniej z miasta, którego liczba mieszkańców mieści się w przedziale 50 000–100 000 mieszkańców (9,2%), duży odsetek stanowią firmy z miasta, w którym mieszka 10 000–250 000 mieszkańców (21,5%) oraz z miast, które mają nie więcej niż 10 000 mieszkańców (20,0%); z największego miasta – powyżej 250 tysięcy osób przybyło 16,9% ankiet. 81,5% ankietowanych nie prowadzi wymiany handlowej zagranicznej w rozumieniu „Polska–świat"[1].

64,6% ogółu ankietowanych uznaje priorytet bezpieczeństwa nad zyskiem. Różnica pomiędzy firmami korzystającymi z usług agencji ochrony i mienia a niekorzystającymi z takich usług wynosi ledwie 1,6%. Tylko 9,8% właścicieli firm, ogólnie ujmując, nie ufa swoim pracownikom. Tylko 13,8% respondentów zatrudnia specjalistów selekcjonujących kandydatów na pracowników, a niewiele mniej (9,2%) nie przeprowadza szkoleń. 44,6% badanych zmienia zamki po każdorazowym zwolnieniu pracownika. 69,2% pracodawców nie prowadzi poufnego wywiadu wśród pracowników dotyczącego kwestii patologicznych. Niewiele mniej ankietowanych (64,6%) nie prowadzi kontroli i ewidencji dostępu, a przedsiębiorstwa, których właściciele odpowiadali na pytania w ankiecie, zazwyczaj (84,6%) nie prowadzą swoich firm w okolicy o dużym natężeniu przestępczości kryminalnej.

Ponad trzy czwarte (75,4%) respondentów archiwizuje dane za pomocą kopii bezpieczeństwa, a już 83,1% niszczy nieodwracalnie zbędne dokumenty. Tylko jeden na czterech przedsiębiorców (24,6%) sporządza dokument określający zakres tajemnicy firmowej. 63,1% firm korzysta z kontaktów ze specjalistami z zewnątrz w sprawach bezpieczeństwa przedsiębiorstwa.

59,0% respondentów w razie popełnienia przestępstwa przez swojego podwładnego informuje organy ścigania tylko wówczas, gdy działania na własną rękę okażą się nieskuteczne lub niewystarczające. 23,0%

[1] A nie w rozumieniu UE–świat.

nie informuje policji ani prokuratury w ogóle w takich przypadkach, a 18,0% czyni to niezwłocznie w każdym przypadku bez wyjątku.

Aż 66,5% badanych na podstawie własnego doświadczenia za największe zagrożenie dla bezpiecznej działalności firmy uznało brak lojalności pracowników, mimo iż większość z nich ufa swoim pracownikom. 24,1% uważa, że największym zagrożeniem dla działalności przedsiębiorstwa jest przestępcze zagrożenie zewnętrzne, a 10,3% pracodawców za najistotniejszą na tej płaszczyźnie uznało zmowę pracowników z osobami spoza firmy.

Aż 93,8% pytanych właścicieli firm wskazało, iż państwo nie zapewnia w należytym stopniu warunków do wspierania biznesu. Ciekawostką jest to, iż kilka odpowiedzi na „NIE" zaakcentowanych było wykrzyknikami lub podkreśleniami.

Hipotezy zerowe

Na podstawie badań sformułowano 41 następujących hipotez zerowych:

$\mathbf{H_0^{01}}$ – Nie ma związku między prowadzeniem kontroli i ewidencji dostępu pracowników i gości a zasadą priorytetu bezpieczeństwa nad zyskiem.

$\mathbf{H_0^{02}}$ – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy.

$\mathbf{H_0^{03}}$ – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a położeniem firmy w okolicy o dużym natężeniu przestępczości kryminalnej.

$\mathbf{H_0^{04}}$ – Nie ma związku między korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

$\mathbf{H_0^{05}}$ – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

$\mathbf{H_0^{06}}$ – Nie ma związku między zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0^{07}}$ – Nie ma związku między korzystaniem z usług firmy ochrony usług i mienia a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0^{08}}$ – Nie ma związku między prowadzeniem kontroli i ewidencji dostępu pracowników i gości a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0^{09}}$ – Nie ma związku między zasadą priorytetu bezpieczeństwa nad zyskiem a korzystaniem z usług firmy ochrony usług i mienia a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0^{10}}$ – Nie ma związku między zasadą priorytetu bezpieczeństwa nad zyskiem a zmienianiem zamków, kodów dostępu itp. po każdorazowym zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy.

$\mathbf{H_0^{11}}$ – Nie ma związku między zasadą priorytetu bezpieczeństwa nad zyskiem a położeniem firmy w okolicy o dużym natężeniu przestępczości kryminalnej.

$\mathbf{H_0^{12}}$ – Nie ma związku między przeprowadzaniem poufnego wywiadu środowiskowego wśród pracowników, dotyczącego zjawisk patologicznych a korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy.

$\mathbf{H_0^{13}}$ – Nie ma związku między zasadą priorytetu bezpieczeństwa nad zyskiem a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

$\mathbf{H_0^{14}}$ – Nie ma związku między niszczeniem zbędnych dokumentów w sposób niedopuszczający do ich ponownego odtworzenia a przeprowadzaniem poufnego wywiadu środowiskowego wśród pracowników dotyczącego zjawisk patologicznych.

$\mathbf{H_0^{15}}$ – Nie ma związku między dokonywaniem archiwizacji kopii bezpieczeństwa danych a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0^{16}}$ – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a niszczeniem zbędnych dokumentów w sposób niedopuszczający do ich ponownego odtworzenia.

$\mathbf{H_0^{17}}$ – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a opinią

pracodawców o zapewnianiu warunków do wspierania biznesu ze strony państwa.

$\mathbf{H_0^{18}}$ – Nie ma związku między ogólnym zaufaniem wobec swoich pracowników a zmienianiem zamków, kodów dostępu itp. po każdorazowym zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy.

$\mathbf{H_0^{19}}$ – Nie ma związku między położeniem firmy w okolicy o dużym natężeniu przestępczości kryminalnej a opinią pracodawców o zapewnianiu warunków do wspierania biznesu ze strony państwa.

$\mathbf{H_0^{20}}$ – Nie ma związku między korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy a określeniem zakresu tajemnicy firmy w odrębnym, specjalnym dokumencie.

$\mathbf{H_0^{21}}$ – Nie ma związku między zmienianiem zamków, kodów dostępu itp. po każdorazowym zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy a dokonywaniem archiwizacji kopii bezpieczeństwa danych.

$\mathbf{H_0^{22}}$ – Nie ma związku między ogólnym zaufaniem wobec swoich pracowników a informowaniem organów ścigania o przestępstwach popełnionych przez pracowników.

$\mathbf{H_0^{23}}$ – Nie ma związku między liczbą zatrudnionych w przedsiębiorstwie pracowników a korzystaniem z usług firmy ochrony usług i mienia.

$\mathbf{H_0^{24}}$ – Nie ma związku między pochodzeniem kapitału a przeprowadzaniem poufnego wywiadu środowiskowego wśród pracowników, dotyczącego zjawisk patologicznych.

$\mathbf{H_0^{25}}$ – Nie ma związku między liczbą zatrudnionych w przedsiębiorstwie pracowników a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0^{26}}$ – Nie ma związku między informowaniem organów ścigania o przestępstwach popełnionych przez pracowników a zmienianiem zamków, kodów dostępu itp. po każdorazowym zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy.

$\mathbf{H_0^{27}}$ – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a zmienianiem zamków, kodów dostępu itp. po każdorazowym zwolnieniu

pracownika mającego dostęp do informacji stanowiących tajemnicę firmy.

$\mathbf{H_0}^{28}$ – Nie ma związku między informowaniem organów ścigania o przestępstwach popełnionych przez pracowników a zasadą priorytetu bezpieczeństwa nad zyskiem.

$\mathbf{H_0}^{29}$ – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a przeprowadzaniem poufnego wywiadu środowiskowego wśród pracowników dotyczącego zjawisk patologicznych.

$\mathbf{H_0}^{30}$ – Nie ma związku między liczbą zatrudnionych pracowników a przeprowadzaniem poufnego wywiadu środowiskowego wśród pracowników, dotyczącego zjawisk patologicznych.

$\mathbf{H_0}^{31}$ – Nie ma związku między liczbą zatrudnionych pracowników a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

$\mathbf{H_0}^{32}$ – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

$\mathbf{H_0}^{33}$ – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a ogólnym zaufaniem wobec swoich pracowników.

$\mathbf{H_0}^{34}$ – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a prowadzeniem kontroli i ewidencji dostępu pracowników i gości.

$\mathbf{H_0}^{35}$ – Nie ma związku między liczbą zatrudnionych pracowników a prowadzeniem kontroli i ewidencji dostępu pracowników i gości.

$\mathbf{H_0}^{36}$ – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a niszczeniem zbędnych dokumentów w sposób niedopuszczający do ich ponownego odtworzenia.

$\mathbf{H_0}^{37}$ – Nie ma związku między liczbą zatrudnionych pracowników a określeniem zakresu tajemnicy firmy w odrębnym, specjalnym dokumencie.

H_0^{38} – Nie ma związku między liczbą zatrudnionych pracowników a korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy.

H_0^{39} – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy.

H_0^{40} – Nie ma związku między wielkością ośrodka miejskiego a zasadą priorytetu bezpieczeństwa nad zyskiem.

H_0^{41} – Nie ma związku między wielkością ośrodka miejskiego a ogólnym zaufaniem wobec swoich pracowników.

Hipotezy, gdzie stwierdzono brak podstaw do odrzucenia

Hipotezy badano testem χ^2 na poziomie istotności α=0,05, gdzie próg zależności wynosi 3,841. Stwierdzono brak podstaw do odrzucenia wyników jedenastu testowanych hipotez zerowych (H_0^2, H_0^5, H_0^{20}, H_0^{23}, H_0^{25}, H_0^{27}, H_0^{31}, H_0^{36}, H_0^{37}, H_0^{38}, H_0^{41}), a tym samym wykazano zależności pomiędzy zmiennymi następujących hipotez:

H_0^2 – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy.

2	Są specjalistyczne szkolenia		Nie ma specjalistycznych szkoleń		Σ		Φ = -0,417
Są kontakty ze specjalistami spoza firmy		6 25,0%	30,5%	18 75,0%	24	36,9%	X^2 = 11,292
Nie ma kontaktów ze specjalistami spoza firmy	0,0%	0 0,0%	69,5%	41 100,0%	41	63,1%	X = 0,417
Σ	6		59		65		WYSTĘPUJE ZWIĄZEK
	9,2%		90,8%				

Źródło: opracowanie własne.

W grupie ankietowanych przedsiębiorców aż 100,0% firm, które prowadzą szkolenia wewnątrzfirmowe w zakresie profilaktyki antyprzestępczej, korzysta również z porad specjalistów spoza firmy. Odsetek nieutrzymujących kontaktów ze specjalistami spoza firmy i nieprowadzących szkoleń wynosi także 100,0%, podczas gdy pracodawców owe szkolenia prowadzących, ale nieutrzymujących kontaktu ze specjalistami wynosi 0,0%. Tylko 25,0% utrzymujących wspomniane kontakty prowadzi zarazem szkolenia. Tylko 30,5% nieprowadzących szkoleń zarazem korzysta z porad specjalistów. 36,9% respondentów utrzymuje kontakty ze specjalistami spoza firmy w sprawach bezpieczeństwa tychże.

H_0^5 – Nie ma związku między prowadzeniem specjalistycznych szkoleń pracowników w zakresie profilaktyki antyprzestępczej a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

5	Są prowadzone szkolenia		Nie ma prowadzonych szkoleń		Σ		Φ = -0,488
Są specjaliści od selekcji	66,7%	4 44,4%	8,5%	5 55,6%	9	13,8%	X^2 = 15,460
Nie ma spec. od selekcji	33,3%	2 3,6%	91,5%	54 96,4%	56	86,2%	X = 0,488
Σ	6		59		65		WYSTĘPUJE ZWIĄZEK
	9,2%		90,8%				

Wśród ankietowanych tylko 13,8% badanych zatrudnia specjalistów od selekcji kandydatów na pracowników. Aż 91,5% respondentów jednocześnie nie prowadzi szkoleń i nie zatrudnia specjalistów od selekcji, a 44,4% pracodawców zatrudniających specjalistów od selekcji prowadzi zarazem szkolenia. Tylko 8,5% przedsiębiorców nieprowadzących specjalistycznych szkoleń pracowników z zakresu profilaktyki antyprzestępczej zatrudnia specjalistów od selekcjonowania osób ubiegających się o pracę w badanych firmach. 96,4% pracodawców niezatrudniających specjalistów od selekcji nie prowadzi również szkoleń.

H_0^{20} – Nie ma związku między korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy a określeniem zakresu tajemnicy firmy w odrębnym, specjalnym dokumencie.

20	Są kontakty ze specjalistami spoza firmy		Nie ma kontaktów ze specjalistami spoza firmy		Σ		Φ = -0,548
Jest określony zakres tajemnicy firmy	56,5%	13 81,2%	7,1%	3 18,8%	16	24,6%	X^2 = 19,528
Nie ma określonego zakresu tajemnicy firmy	43,5%	10 20,4%	92,9%	39 79,6%	49	75,4%	X = 0,548
Σ	23		42		65		WYSTĘPUJE ZWIĄZEK
	35,4%		64,6%				

56,5% badanych pracodawców, którzy korzystają z porad specjalistów spoza firmy, określa w specjalnym dokumencie zakres tajemnicy własnego przedsiębiorstwa, a ogólnie taki dokument formułuje tylko 24,6% przedsiębiorców. Tylko 18,8% przedsiębiorców posiadających ów dokument nie czerpie porad od specjalistów spoza firmy. Zgoła odwrotnie te proporcje przedstawiają się u firm, które nie posiadają wspomnianego już dokumentu – aż 79,6% z nich nie korzysta z usług specjalistów spoza firmy w zakresie bezpieczeństwa. 92,9% nieutrzymujących merytorycznych kontaktów ze specjalistami w zakresie bezpieczeństwa firmy jednocześnie nie formułuje dokumentu określającego zakres tajemnicy firmy.

H_0^{23} – Nie ma związku między liczbą zatrudnionych w przedsiębiorstwie pracowników a korzystaniem z usług firmy ochrony usług i mienia.

23	Do 50 pracowników		Powyżej 51 pracowników		Σ		Φ = 0,325
Jest firma ochrony mienia	41,5%	22	83,3%	10 31,2%	32	49,2%	X^2 = 6,848
Nie ma firmy ochrony mienia	58,5%	31	16,7%	2 6,1%	33	50,8%	X = 0,325
Σ	53		12		65		WYSTĘPUJE ZWIĄZEK
	81,5%		18,5%				

W 83,3% firm zatrudniających powyżej 51 pracowników zawarto umowę z firmą ochrony usług i mienia. 58,5% pracodawców dających zatrudnienie najwięcej 50 pracownikom nie ma zawartej umowy z firmą ochroniarską. Aż 93,9% przedsiębiorstw niezatrudniających firmy ochraniającej mienie nie ma w swoich szeregach więcej niż 50 pracowników, wśród zatrudniających agencje ochrony, a jednocześnie małych firm jest to odsetek rzędu 68,8%. W ankietowanych firmach średnich i dużych agencję ochrony usług i mienia zatrudnia 83,3% z nich. 50,8% ankietowanych firm nie korzysta z usług firmy ochrony usług i mienia.

H_0^{25} – Nie ma związku między liczbą zatrudnionych w przedsiębiorstwie pracowników a ogólnym zaufaniem wobec swoich pracowników.

25	Do 50 pracowników		Powyżej 51 pracowników		Σ		Φ = -0,259
Ufa pracownikom	94,3%	50 84,7%	75,0%	9 15,3%	59	90,8%	X^2 = 4,368
Nie ufa pracownikom	5,7%	3 50,0%	25,0%	3 50,0%	6	9,2%	X = 0,259
Σ	53		12		65		WYSTĘPUJE ZWIĄZEK
	81,5%		18,5%				

90,8% pracodawców ufa swoim podwładnym. Aż 94,3% pracodawców zatrudniających nie więcej niż pięćdziesięciu pracowników ufa tymże. 84,7% mających zaufanie do podwładnych to przedsiębiorcy prowadzący małe firmy. Trzech na czterech superiorów firm średnich i dużych łącznie ufa swoim podwładnym (75,0%). Odsetek pracodawców niemających zaufania do zatrudnionych przez siebie ludzi dzieli się po równe 50,0% zarówno dla firm małych, jak i dla firm średnich i dużych.

H_0[27] – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a zmienianiem zamków, kodów dostępu itp. po każdorazowym zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy.

27	Przest. zagr. zewn.		Brak lojalności/ Zmowa		Σ		Φ = 0,265
Zmiana zamków	21,4%	3 11,5%	52,3%	23 88,5%	26	44,8%	X^2 = 4,085
Brak zmiany zamków	78,6%	11 34,4%	47,7%	21 65,6%	32	55,2%	X = 0,265
Σ	14		44		58		WYSTĘPUJE ZWIĄZEK
	24,1%		75,9%				

52,2% właścicieli firm nie zmienia zamków i kodów dostępu za każdym razem, gdy zwolni pracownika mającego dostęp do informacji będących istotą tajemnicy firmy. Ledwo ponad połowa ankietowanych (52,3%), według których największe zagrożenie dla ich firm płynie od pracowników, zmienia zamki i kody dostępu każdorazowo po zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy. Wśród dopatrujących się niebezpieczeństwa z przestępczego zagrożenia zewnętrznego tylko 21,4% przedsiębiorców zmienia zamki i kody dostępu w sytuacji zwolnienia pracownika mającego dostęp do informacji stanowiących tajemnicę firmy. 65,6% niezmieniających zamków i kodów dostępu w takich sytuacjach najbardziej obawia się podwładnych. Wśród zmieniających każdorazowo zamki i kody dostępu w sytuacji zwolnienia pracownika mającego dostęp do informacji stanowiących tajemnicę firmy aż 88,5% respondentów obawia się najbardziej nielojalności swych podwładnych oraz ich zmowy z osobami spoza firmy łącznie.

H_0^{31} – Nie ma związku między liczbą zatrudnionych pracowników a zatrudnieniem specjalistów selekcjonujących kandydatów na pracowników.

31	Do 50 pracowników		Powyżej 51 pracowników		Σ		Φ = 0,498
Są specjaliści od selekcji	5,7%	3 33,3%	50,0%	6 66,7%	9	13,8%	X^2 = 16,126
Nie ma specjalistów od selekcji	94,3%	50 89,3%	50,0%	6 10,7%	56	86,2%	X = 0,498
Σ	53		12		65		WYSTĘPUJE ZWIĄZEK
	81,5%		18,5%				

Przeszło 86,2% przedsiębiorców nie korzysta z usług specjalistów od selekcji kandydatów na pracowników. Aż 94,3% pracodawców z małych firm nie zatrudnia specjalistów od selekcji, w firmach średnich i dużych łącznie proporcje dzielą się już po połowie. 89,3% niezatrudniających specjalistów od selekcji firm nie zatrudnia więcej niż pięćdziesięciu pracowników. Tam, gdzie specjaliści są zatrudnieni, odsetek firm małych wynosi już tylko 33,3%. Wśród firm średnich i dużych odsetek tych, które zatrudniają specjalistów od selekcji, wynosi równe 50,0%.

H_0^{36} – Nie ma związku między wskazaniem największego wynikającego z praktyki zagrożenia dla bezpiecznej działalności firmy a niszczeniem zbędnych dokumentów w sposób niedopuszczający do ich ponownego odtworzenia.

36	Przest. zagr. zewn.		Brak lojalności/ Zmowa		Σ		Φ = 0,383
Niszczy zbędne dokumenty	57,1%	8 16,7%	90,9%	40 83,3%	48	82,8%	X^2 = 8,487
Nie niszczy zbędnych dokumentów	42,9%	6 60,0%	9,1%	4 40,0%	10	17,2%	X = 0,383
Σ	14		44		58		WYSTĘPUJE ZWIĄZEK
	24,1%		75,9%				

82,8% respondentów niszczy zbędne dokumenty w sposób niedopuszczający do ich ponownego odtworzenia. 90,9% pracodawców wskazujących, iż największe zagrożenie pochodzi od pracowników, niszczy zbędne dokumenty, atoli wśród ankietowanych najbardziej obawiających się przestępczego zagrożenia zewnętrznego dokumenty usuwa w sposób nieodwracalny już tylko 57,1%. Wśród niszczących zbędne dokumenty tylko 16,7% badanych uważa za największe zagrożenie dla działalności przedsiębiorstwa brak lojalności pracowników i zmowę tychże z osobami spoza firmy łącznie, podczas gdy wśród nieniszczących zbędnych dokumentów jest ich już tylko 40,0%.

H_0[37] – Nie ma związku między liczbą zatrudnionych pracowników a określeniem zakresu tajemnicy firmy w odrębnym, specjalnym dokumencie.

37	Do 50 pracowników		Powyżej 51 pracowników		Σ		Φ = 0,280
Jest określony zakres tajemnicy	18,9%	10 62,5%	50,0%	6 37,5%	16	24,6%	X^2 = 5,111
Nie ma określonego zakresu tajemnicy	81,1%	43 87,8%	50,0%	6 12,2%	49	75,4%	X = 0,280
Σ	53		12		65		WYSTĘPUJE ZWIĄZEK
	81,5%		18,5%				

Aż 81,1% małych firm nie ma dokumentu, w którym określa zakres tajemnicy swoich przedsiębiorstw, a wśród przedsiębiorstw średnich i małych odsetek niemających tego dokumentu przedsiębiorców wynosi 50,0%. Odsetek przedsiębiorstw, które określają zakres tajemnicy firmy w specjalnym dokumencie, a jednocześnie zatrudniają nie więcej niż 50 pracowników, wynosi 62,5%. Wśród przedsiębiorstw nieujmujących zakresu bezpieczeństwa firmy w odrębnym dokumencie 87,8% to firmy małe.

H_0[38] – Nie ma związku między liczbą zatrudnionych pracowników a korzystaniem z kontaktów w sprawach bezpieczeństwa ze specjalistami spoza firmy.

38	Do 50 pracowników		Powyżej 51 pracowników		Σ		Φ = 0,357
Są kontakty ze specjalistami spoza firmy	30,2%	16 64,0%	75,0%	9 36,0%	25	38,5%	X^2 = 8,301
Nie ma kontaktów ze specjalistami spoza firmy	69,8%	37 92,5%	25,0%	3 7,5%	40	61,5%	X = 0,357
Σ	53		12		65		WYSTĘPUJE ZWIĄZEK
	81,5%		18,5%				

Tylko 30,2% przedsiębiorstw małych korzysta z kontaktów ze specjalistami spoza firmy w zakresie bezpieczeństwa biznesu, odsetek firm zatrudniających co najmniej pięćdziesięciu pracowników i korzystających z usług specjalistów pozafirmowych wynosi zaś 75,0%. 64,0% pracodawców korzystających z porad specjalistów to firmy małe. Wśród pracodawców nieutrzymujących kontaktów ze specjalistami spoza firmy aż 92,5% z nich zatrudnia nie więcej niż pięćdziesięciu pracowników.

H_0[41] – Nie ma związku między wielkością ośrodka miejskiego a ogólnym zaufaniem wobec swoich pracowników.

41	Do 50 000 mieszkańców		Powyżej 50 000 mieszkańców		Σ		Φ = -0,370
Ufa pracownikom	94,1%	32 61,5%	64,5%	20 38,5%	52	80,0%	X^2 = 8,880
Nie ufa pracownikom	5,9%	2 15,4%	35,5%	11 84,6%	13	20,0%	X = 0,370
Σ	34		31		65		WYSTĘPUJE ZWIĄZEK
	52,3%		47,7%				

94,1% przedsiębiorców prowadzących swe firmy w miejscowościach do 50 000 mieszkańców ufa swoim pracownikom, atoli w miejscowościach powyżej 50 000 mieszkańców odsetek zaufania wynosi już tylko 64,5%. Wśród ufających swoim podwładnym 61,5% prowadzi biznes w mniejszych miejscowościach. Wśród nieufających swoim pracownikom aż 84,6% respondentów stanowią przedsiębiorcy z większych miejscowości.

Omówienie wyników hipotez, których nie odrzucono

Przeprowadzone badania z zakresu bezpieczeństwa w biznesie wykazały, jak istotny wpływ na bezpieczeństwo w przedsiębiorstwie mają porady specjalistów zarówno spoza firmy, jak i tych w firmie zatrudnionych. Owe kontakty determinują zazwyczaj przedsiębiorców do działania na rzecz ochrony bezpieczeństwa w swojej firmie. Specjaliści od selekcji kandydatów na pracowników nie są jeszcze zbyt popularną metodą eliminacji niebezpieczeństw grożących przedsiębiorstwom; praktycznie nie użyczają swych usług firmom małym. Wynika to być może z przekonania,

że to pracodawca sam wie najlepiej, kogo potrzebuje i wie, jak wybrać najwłaściwszych pracowników. Być może jednak również z małej wiedzy o tym sposobie eliminacji zagrożeń, a także chęci osiągnięcia wzrostu efektywności przedsiębiorstwa (niedokładanie kolejnych kosztów). Specjaliści z zewnątrz oddziaływają swoją opartą na doświadczeniu pracą na biznesmenów, przez co ci drudzy formułują specjalne dokumenty określające zakres tajemnicy przedsiębiorstwa, choć wciąż pozostaje to rzadkością. Możliwe wydaje się, że pracodawcy nie tworzą tego typu aktów, albowiem uznają je za zbyt mało istotne w walce z niebezpieczeństwami, na jakie narażone są ich przedsiębiorstwa. Z kolei specjaliści od selekcji zatrudnieni również w firmie, choć w mniejszym stopniu, generują u przedsiębiorców prowadzenie szkoleń z zakresu profilaktyki antyprzestępczej, częściej są jednak pierwszym etapem troski o bezpieczeństwo biznesu, z jakim spotyka się pracownik w nowej firmie, kolejnym bywają choćby owe szkolenia. Przedsiębiorcy z małych firm bardziej wierzą w swoje metody eliminacji zagrożeń dla swoich zakładów niż w metody specjalistów spoza firmy. Dla większości przedsiębiorców średnich i dużych łącznie jest to z kolei normalną praktyką. Można zaryzykować tezę, iż firmy małe, które korzystają z usług specjalistów pozafirmowych w zakresie bezpieczeństwa biznesu, to zakłady pracy generujące duże zyski, na przykład kantory itp. Niewykluczone, iż przedsiębiorcy zatrudniający mniej pracowników czerpią doświadczenie od kolegów z branży.

Wiara w brak przydatności szkoleń jest zatrważająca. Może się to wiązać z brakiem zaufania do kogokolwiek, kto nie jest wewnątrz firmy, z obawy o niezrozumienie potrzeb tejże. Z drugiej strony rysuje się istotna – stuprocentowa – zależność między kontaktami ze specjalistami z zewnątrz w dziedzinie bezpieczeństwa firm a prowadzeniem szkoleń, co oznacza, że pracodawcy, jeśli już zdobędą się na taką współpracę, wówczas uznają bezgranicznie wręcz autorytet osób, których się radzą w sprawach bezpieczeństwa własnych zakładów pracy.

Niewiele ponad połowa przedsiębiorców uczestniczących w ankiecie korzysta z firm ochrony usług i mienia, co jest wynikiem – można by rzec – niepokojącym. Jest to o tyle dziwne, że przechadzając się chodnikiem, trudno jest znaleźć brak naklejki z nazwą agencji ochrony na witrynach

czy drzwiach przedsiębiorstw. Możliwe jednak, że owe naklejki pozostają mimo ustania współpracy z agencjami jako niegenerujący kosztów, acz ryzykowny, straszak. Zdecydowanie więcej przedsiębiorstw niezatrudniających ochrony jest wśród małych firm, złożonych z nie więcej niż pięćdziesięciu pracowników, co wydaje się zrozumiałe ze względu na koszty. Małe przedsiębiorstwa przeważają również wśród firm, które zatrudniają agencje ochrony usług i mienia (66,8%) – zapewne w większości to przedsiębiorstwa takie jak zakłady jubilerskie, kantory, kancelarie itp., których liczba zatrudnionych jest minimalna, a zyski duże.

Wielkość firmy również ma znaczenie, albowiem da się zauważyć istotny podział na firmy małe, które są niechętne wobec innowacji w zakresie bezpieczeństwa biznesu, jak i firmy średnie i duże łącznie, którym zdecydowanie łatwiej przyswoić takie metody zabezpieczeń, jak zatrudnianie specjalistów, określanie zakresu tajemnicy firmy w odrębnym dokumencie. Zazwyczaj przedsiębiorcy z firm małych (a także z mniejszych miejscowości) zdecydowanie bardziej ufają swoim pracownikom, zaś w przedsiębiorstwach średnich i dużych łącznie odsetek pracodawców mających zaufanie wobec swoich pracowników utrzymuje się na niskim poziomie, co wydaje się oczywiste z racji praktycznej niemożności spoufalenia się ze swoimi podwładnymi. W miastach do 50 000 mieszkańców można zaobserwować większe zaufanie superiorów do swoich podwładnych, co prawdopodobnie ma swoje miejsce w kulturze ludzi z mniejszych miejscowości, którzy zdecydowanie bardziej się znają, mówiąc kolokwialnie – „wiedzą wszystko o wszystkich". Możliwe też, że większa religijność tych ludzi wpływa na ich opinię dotyczącą człowieka w rozumieniu doktryny chrześcijańskiej. W przedsiębiorstwach w większych miastach, gdzie zwyczaje miejscowe i religia są mało istotne, oczywiste jest, że wskaźnik zaufania pracodawcy wobec pracowników będzie mniejszy.

Niewiele ponad połowa zmieniających zamki i kody dostępu po każdorazowym zwolnieniu pracownika mającego dostęp do informacji stanowiących tajemnicę firmy to niezbyt optymistyczny wynik, tym bardziej jeśli ci sami pracodawcy w większości uważają, że to pracownicy stanowią największe zagrożenie dla działalności firmy. Jednak jeśli wziąć pod uwagę li tylko tych, którzy zamki i kody dostępu zmieniają

każdorazowo w sytuacji zwolnienia pracownika mającego dostęp do informacji stanowiących tajemnicę firmy, wychodzi, iż prawie 90% (a konkretnie 88,5%) z nich za największe zagrożenie dla działania firmy wskazuje nielojalność pracowników oraz ich zmowę z osobami spoza firmy, co daleko posuniętą tezą pokazuje, iż najlepiej uczy się na własnych błędach.

Zatrważające, iż tak elementarna czynność jak niszczenie zbędnych dokumentów w sposób niedopuszczający do ich ponownego odtworzenia nie jest nawykiem ogółu. Przeważająca część niszczących owe dokumenty wskazała również na zagrożenie ze strony pracowników jako na największe niebezpieczeństwo dla działalności firmy, co może sugerować przykrą praktykę. Niemniej jednak nieniszczenie zbędnych dokumentów w sposób nieodwracalny jest dla sprytnie umiejącego wykorzystać informacje przestępcy tak samo kuszące jak otwarte okno w pomieszczeniu zamkniętym na cztery spusty. I tak samo warte podjęcia przez niego ryzyka.

W małych firmach nie ma zwyczaju określania zakresu bezpieczeństwa firmy w odrębnym dokumencie. Wynika to prawdopodobnie z racji, iż firmy te w dużej mierze są firmami rodzinnymi lub nie uważają, że z powodu małej – podług nich – liczby pracowników jest to konieczne. Acz wśród przedsiębiorstw, które mają taki dokument, większość to jednak firmy niezatrudniające więcej niż pięćdziesięciu pracowników, co stanowi swojego rodzaju zaskoczenie, albowiem właściciele średnich i większych firm winni uważać to wręcz za swój obowiązek zapewniający bezpieczeństwo przedsiębiorstwa. W takich przedsiębiorstwach pracują bowiem nie tylko pracownicy istotni dla firmy z merytorycznego punktu widzenia, lecz również pozostałe osoby swoją pracą przyczyniające się do (lepszego) działania przedsiębiorstwa (na przykład ekipa sprzątająca, informatycy, mechanicy itd.).

Podsumowanie badania

Bardzo pozytywne jest, co można by rzec na podstawie omówionych tu badań, iż przedsiębiorcy w dobie pieniądza i zysku tak cenią sobie bezpieczeństwo. Ochłodzić ów entuzjazm z pewnością może

ich niekonsekwencja na polu ochrony przed zjawiskami przestępczymi i wynikająca z tego nie tak znowu wielka troska o bezpieczeństwo w praktyce. Zapewne tę rozbieżność tłumaczyć można zaledwie kilkunastoletnim doświadczeniem działalności Polaków na łonie gospodarki wolnorynkowej, gdzie bardzo łatwo jest zyskać i jeszcze łatwiej stracić, gdzie bardzo istotna jest umiejętność dokonania prawidłowych wyborów. Mimo wszystko przedsiębiorcy starają sobie radzić jak mogą na własną rękę i tu ich dokonania, wciąż nieśmiałe, należy docenić. A dlaczego na własną rękę? Albowiem spośród ankietowanych przedsiębiorców aż 93,8% właścicieli firm stwierdziło, iż organy państwa nie zapewniają ogólnych warunków do wspierania biznesu w sposób choćby wystarczający! A bezpieczeństwo biznesu w bezsprzeczny sposób do ogólnych warunków działalności się zalicza. Choć to domniemanie, jest wielce prawdopodobne, iż pozostałe 6,2% respondentów to przedsiębiorstwa państwowe. Można więc przyjąć, że państwu nie zależy na istnieniu przedsiębiorstw, li tylko na zyskach tychże, które są wyprowadzane do budżetu. Państwo doskonale zdaje sobie sprawę, iż w miejsce jednej upadłej firmy wejdzie kolejna pełna nadziei co do swej przyszłości, przez co – mówiąc kolokwialnie – wpływów nigdy nie zabraknie, co w konsekwencji powoduje, iż problem ten jest wręcz niezauważany. Ta ze wszech miar brutalna praktyka pokazuje, że gdy samemu, krok po kroku, wytrwałą pracą z minimalnym wsparciem państwa zbiera się plony w postaci zysków, o wiele bardziej szanuje się biznes, niż gdy stoi się po drugiej stronie, która paradoksalnie żyje dzięki tym, którym nie daje za wiele w zamian, choćby nie spełnia ich elementarnych potrzeb. Przekładając to na sferę ludzką – elementarnych potrzeb, które nie tylko poprawiają możliwości życiowe człowieka, ale przede wszystkim pozwalają mu przeżyć.

Pozyskanie i ochrona informacji

Jolanta Stadnik

Czarny wywiad gospodarczy

Celem mojej pracy było ukazanie zjawiska czarnego wywiadu w biznesie, jakie występuje dość powszechnie na świecie i zaczyna pojawiać się także na rynku polskim. Moja praca stanowi jedynie wstęp do zagadnienia, które jest bardzo ciekawe, ale i bardzo rozlegle. Mam nadzieję jednak, że praca ta pozwoli czytelnikowi dostrzec owo zjawisko, jego skalę i mechanizmy, jakimi się posługuje.

Informacja

Działalność gospodarcza w ostatnim czasie stała się działalnością globalną, a przez to osoba prowadząca przedsiębiorstwo została zmuszona do pozyskiwania informacji o szerszym zasięgu niż kilkanaście lat temu. Powyższe stwierdzenie dotyczy nie tylko wielkich przedsiębiorstw działających na rynkach międzynarodowych, ale także małych i średnich przedsiębiorstw, które muszą być przygotowane na ewentualne pojawienie się na jego rynku konkurenta zagranicznego.

Utrzymanie się na rynku jest możliwe poprzez dotarcie do cennych informacji przed konkurencją. Dobra informacja to przede wszystkim niwelowanie ryzyka związanego z podejmowaniem decyzji czy wprowadzaniem nowych produktów lub technologii.

Przedsiębiorstwo działające globalnie to też przedsiębiorstwo trwale otwarte na nowe wyzwania i nowe potrzeby. Tu konieczne jest myślenie długofalowe, potrzebne są wizje, nowe pomysły, a przede wszystkim wiedza dotycząca technologii, rynku, sytuacji prawnej.

Informacja obok kapitału stanowi dziś główny element powodzenia działalności danego przedsiębiorstwa lub jego porażki. Takich informacji dostarcza wywiad gospodarczy.

DEFINICJA

Według definicji przedstawionej przez Francuski Generalny Komisariat do spraw Planowania Gospodarczego wywiad gospodarczy jest to zespół działań polegających na poszukiwaniu (gromadzeniu), przetwarzaniu i rozpowszechnianiu (w celu wykorzystania) informacji przydatnej podmiotom gospodarczym[1].

Termin ten pojawił się na początku lat osiemdziesiątych XX w. W Stanach Zjednoczonych, gdzie zaczęto go wykładać w college'ach biznesu, a jego intensywny rozwój rozpoczął się po ogłoszeniu pracy Leonarda M. Fulda *Competitor Inteligence*.

Jednakże wywiad gospodarczy jest praktyką liczącą sobie co najmniej 500 lat, instytucja ta powstawała równolegle z powstawaniem kapitalizmu i początkowo służyła przede wszystkim minimalizowaniu strat z tytułu udzielania kredytów kupieckich. Za kolebkę tej instytucji uważa się Republikę Wenecką, gdzie w 1491 r. Rada Dziesięciu utworzyła wykaz niesolidnych i niewypłacalnych kupców. Republika ta była w stanie utrzymać swoją świetność przez ponad 200 lat dzięki rozległej sieci wywiadowczej swoich ambasadorów we wszystkich krajach europejskich[2].

Należy jednak pamiętać, że wywiad gospodarczy ma dwie bardzo różne formy. Jedną z nich jest „biały wywiad", który należy rozumieć jako pozyskiwanie wszelkich informacji ze źródeł ogólnie dostępnych, sformalizowanych i niebędących przedmiotem szczególnego zabezpieczenia. Natomiast szpiegostwo gospodarcze zwane też „czarnym wywiadem" jest to sposób pozyskiwania informacji z otoczenia przedsiębiorstwa metodami niedozwolonymi, to znaczy zabronionymi przez prawo, normy etyczne lub zwyczajowe.

Ramy prawne

Aby dane działanie uznać za działalność w ramach białego bądź czarnego wywiadu, należy przyjrzeć się ramom prawnym, aby móc zakwalifikować je jako zgodne bądź niezgodne z prawem. W prawie

[1] M. Kwieciński, *Wywiad gospodarczy*, Warszawa–Kraków 1999, s. 160.

[2] B. Martinet, Y.M. Marti, *Wywiad gospodarczy*, Warszawa 1999, s. 14.

polskim uregulowania dotyczące wywiadu gospodarczego są dość ubogie. W polskim ustawodawstwie nie znajdziemy terminu „szpiegostwo gospodarcze", jednakże znajdziemy przepisy, które zakazują stosowania metod znanych i wykorzystywanych w czarnym wywiadzie gospodarczym.

Istotne przepisy znajdujemy w kodeksie karnym: w rozdziale XXXIII zatytułowanym „Przestępstwa przeciwko ochronie informacji", rozdziale XXXVI „Przestępstwa przeciwko obrotowi gospodarczemu" oraz w Ustawie o zwalczaniu nieuczciwej konkurencji.

Przepisy te wskazują, że zabronione są praktyki zmierzające do uzyskania informacji, „otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie" bądź zdobycia informacji, „zakładając lub posługując się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym" (art. 267 kk). Jak również zabrania się osobie nieuprawnionej niszczenia, uszkadzania bądź usuwania lub zmieniania zapisu istotnych informacji albo w inny sposób utrudniania osobie uprawnionej zapoznania się z nią (art. 268 kk).

Istotnym przepisem jest także art. 11 Ustawy o zwalczaniu nieuczciwej konkurencji, a mianowicie: „Czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy".

Skala zjawiska

Skala zjawiska czarnego wywiadu na rynku polskim jest bardzo duża. Można zaryzykować stwierdzenie, że większość ważnych strategicznych informacji uzyskiwanych jest w ramach działalności czarnego wywiadu. Dotyczy to wszystkich dziedzin działalności gospodarczej, od przemysłu spożywczego przez AGD, elektronikę, przemysł samochodowy, po przemysł zbrojeniowy.

Wszędzie tam, gdzie informacja wiąże się z dużymi zyskami, pojawia się pole do działania wywiadu gospodarczego.

W wielkich światowych firmach istnieją specjalne komórki do działań wywiadowczych, często funkcjonujące pod nazwą marketingu specjalnego. Prowadzą one zarówno działania legalne, jak i te przekraczające granice prawa.

Dość często jest to strategia wymierzona tylko w jednego głównego konkurenta. Wyobraźmy sobie dwie wielkie światowe firmy, które produkują bardzo podobny produkt. Siłą przebicia w takiej sytuacji jest reklama i wiedza o tym, co w zanadrzu ma konkurent, a ta wiedza uzyskiwana jest przede wszystkim na drodze czarnego wywiadu gospodarczego.

Posiadanie swoich działów wywiadowczych jest drogą inwestycją, na którą decydują się największe firmy, natomiast mniejsze firmy w momencie pojawienia się problemu zwracają się o pomoc do specjalistów. Najczęściej informacje, których oczekują, są niemożliwe do zdobycia zgodnie z prawem. Aby odpowiedzieć na pytanie, dlaczego firmy korzystają z takich usług, należy zauważyć, że dobra informacja daje przewagę nad konkurencją i tylko ta firma odniesie sukces, która jako pierwsza wypromuje nowy produkt bądź która poprowadzi trafnie skonstruowaną kampanię reklamową. Informacja może dotyczyć technologii, ceny, nowej linii produktu, grupy docelowej, do której jest on kierowany, czyli tego wszystkiego, co ma wpływ na wybór przez konsumenta tego a nie innego produktu.

Czasem może dotyczyć to jedynie ceny konkurenta i ona ma największe znaczenie. Dobrym przykładem jest przetarg na realizację wielomilionowego zlecenia, w którym wygrywa najtańsza oferta, więc tu każda złotówka jest ogromnie ważna, a wiedza o cenie zaproponowanej przez konkurenta jest równa wygranej.

Metody

Metody stosowane w wywiadzie gospodarczym są takimi samymi metodami jak stosowane w wywiadzie państwowym.

Pierwszym punktem takiego działania jest rozeznanie i wytypowanie potencjalnego źródła informacji. Każde źródło informacji musi posiadać dwie główne cechy: mieć motywację i mieć dostęp do informacji.

Motywacje mogą być najróżniejsze, mylne jest przeświadczenie, że chodzi tylko i wyłącznie o korzyści finansowe, często motywacją jest niechęć wobec szefa, chęć zemsty. Zdarza się również, że informacja uzyskiwana jest za pomocą szantażu.

Istotnym elementem wykorzystywanym przez specjalistów jest znalezienie usprawiedliwienia dla takiego działania. Osoby wykradające informacje przekonywane o tym, iż służą wyższym celom, że przynosi to korzyści im i ich rodzinom. Ma to na celu zagłuszenie wyrzutów sumienia i zniwelowanie oporów przed działaniem.

Drugim istotnym elementem wyboru osoby jako źródła jest jej naturalny dostęp do informacji, na przykład może to być sekretarka, osoba obsługująca ksero, kierowca, osoba sprzątająca, ochroniarz. Niekoniecznie musi to być pracownik na wysokim stanowisku, istotne jest, aby miał dostęp do informacji.

Dobrze to obrazuje przykład pewnej firmy, w której zatrudnił się młody człowiek na stanowisku ochroniarza. Był dobrym pracownikiem, nie stwarzał większych problemów, prosił jedynie o nocne zmiany ze względu na studia, na co się zgadzano. W pewnym momencie okazało się, że konkurencja zna tajne informacje firmy, i zaczęto szukać źródła przecieku. Okazało się, że spokojny student jest informatykiem pracującym dla konkurencji, który wykradał podczas nocnych dyżurów informacje z systemu komputerowego.

Sposobów uzyskania informacji jest bardzo wiele, np. przez wprowadzenie swojego człowieka do konkurencyjnej firmy, jak w wyżej wymienionym przykładzie, lub pozyskanie źródła informacji wśród pracowników tejże firmy. Przykładowo nietrudno sobie wyobrazić osobę sprzątającą, która oprócz swoich obowiązków wykrada bądź kseruje dokumenty znajdujące się w biurach zarządu.

Pozyskanie źródła informacji wiąże się ze zdobyciem wszelkich informacji dotyczących danej osoby. Specjaliści dowiadują się o rodzinę, hobby itp., następnie stwarzają odpowiednie warunki i proponują współpracę. Czasem polega to na nawiązaniu „przyjaźni", zbudowaniu zaufania, podstawieniu osoby, z którą wiążą się miłe wspomnienia, np. kolegi z lat szkolnych. W odpowiednich warunkach pracownik często

sam zdradza tajemnice firmy, myśląc, że zwierza się osobie niezwiązanej ani z jego firmą, a tym bardziej z konkurencją.

Często informacje uzyskiwane są metodami technicznymi, na przykład przez podsłuchy, kamery, urządzenia ściągające dane z komputerów nawet z bardzo dużej odległości.

Sposoby

Jednym ze sposobów pokonania konkurencji jest jej dezinformowanie. Takie działanie jest zawsze dokładnie przemyślane, prowadzone wielokanałowo i przekonująco. W efekcie firma wybiera droższe metody produkcji, mniej skuteczne, a konkurent wprowadza szybciej produkt tańszy i lepszy.

Bardziej brutalnym sposobem wykorzystywanym przez niektóre firmy jest podstawienie firmy trzeciej, która składa bardzo specyficzne zamówienie, a potem nie realizuje umowy. Firma zostaje z towarem i długami, ogłasza bankructwo, a konkurent ją wykupuje.

Najbardziej powszechne i moim zdaniem najbardziej niebezpieczne działania stosowane w wywiadzie gospodarczym to działania socjotechniczne. Opierają się one na wprowadzeniu w błąd i manipulowaniu ludźmi.

Często socjotechnik uzyskuje poufne informacje, po prostu o nie prosząc. Działanie specjalisty może opierać się na różnych podstawach. Często jest to budowanie zaufania, wykorzystanie naturalnej chęci pomocy czy też wykorzystanie nazwiska i autorytetu osoby będącej na wyższym stanowisku.

W większości wypadków socjotechnicy to ludzie posiadający zdolność oddziaływania na ludzi, potrafią być uprzejmi, łatwo nawiązują kontakt z innymi, wzbudzają zaufanie.

Atak socjotechniczny zawsze zaczyna się od zebrania informacji, poznania w ten sposób języka i terminologii wewnętrznej. Dużym ułatwieniem jest poznanie struktury i nazwisk pracowników, a taka informacja dość często jest zamieszczana na stronach internetowych firmy. Często na tychże stronach pojawiają się też informacje dotyczące firm współpracujących, co daje dość szeroki obraz przedsiębiorstwa.

Dobrym przykładem ataku jest telefon od osoby, która przedstawia się jako pracownik firmy partnerskiej przeprowadzający ankietę dotyczącą współpracy między firmami. W ankiecie takiej pojawiają się obok pytań neutralnych pytania o istotne informacje, np. numer identyfikacyjny pracownika, adres e-mailowy.

Często tak zdobyte informacje mają służyć do podszycia się pod tę osobę w rozmowie z innym pracownikiem. Znając terminologię, nazwisko, numer identyfikacyjny, łatwo uśpić czujność pracownika i wykraść informacje. Podając tyle informacji, osoba dzwoniąca wydaje się wiarygodna. Często atak polega na prośbie o pomoc, np. pracownik odbiera telefon od „kolegi" z innego oddziału, któremu zawiesił się komputer, a ma na głowie bardzo nieprzyjemnego klienta. Normalnym ludzkim odruchem jest chęć pomocy osobie znajdującej się w sytuacji, którą znamy z własnego doświadczenia. W tak łatwy sposób można zdobyć informacje chronione przez wyspecjalizowane systemy komputerowe, hasła i numery identyfikacyjne. To człowiek jest piętą achillesową systemów bezpieczeństwa i o tym najbardziej należy pamiętać.

Socjotechnik przygotowany jest na podejrzliwość pracownika i ma przygotowany plan przełamania bariery nieufności. Czasem zaufanie budowane jest przez długi czas, osoba przedstawia się jako np. pracownik techniczny, informatyk oferuje swoją pomoc, pyta, czy wszystko działa jak należy, buduje w ten sposób akceptację drugiej strony jego jako pracownika. W takiej sytuacji atak jest o wiele prostszy. Prośba o zainstalowanie programu bądź sprawdzenie danych nie budzi podejrzeń, w końcu pochodzi ona od osoby, którą znamy. Ale czy na pewno?

Podobne działanie jest wtedy, gdy socjotechnik powoduje problem, a następnie go naprawia, zyskując naszą wdzięczność i chęć zrewanżowania się. W tym przypadku specjalista bazuje na potrzebie odwzajemnienia i to wykorzystuje.

Czasem atak polega na wykorzystaniu autorytetu wynikającego z pozycji w strukturze organizacji. Ludzie mają tendencję do podporządkowania się woli osoby, która ma władzę, wystarczy, że wierzą w to,

iż rozmówca rzeczywiście ją posiada. Ciężko jest się sprzeciwić osobie, która twierdzi, że jest naszym szefem, w dodatku gdy wyczujemy, że jest zdenerwowana.

Tu pojawia się niezwykle ważny aspekt bezpieczeństwa informacji, aby reguły weryfikacji osoby były jasne i przestrzegane przez wszystkich pracowników niezależnie od stanowiska, jakie zajmują.

Inny element wykorzystywany przez specjalistów to wzbudzenie sympatii, stworzenie sytuacji, w której osoba dzwoniąca wyda się bliska rozmówcy, np. ma podobną pracę, zainteresowania, co powoduje, że czujność zostaje uśpiona.

Dobrym celem do ataku jest nowy pracownik nieznający jeszcze nazwisk, procedur, który chce być zaakceptowany w nowym miejscu i jest chętny do pomocy. Telefon od specjalisty od bezpieczeństwa, który chce zweryfikować zgodność hasła oraz pomóc w konstruowaniu przyszłych haseł, nie budzi niepokoju u nowego pracownika, a powinien.

Ludzie także inaczej reagują, gdy wiedzą, że inni w podobnej sytuacji zachowali się tak a nie inaczej. Łatwiej się zgodzić na przykład na przeprowadzenie ankiety, gdy rozmówca poda nazwiska kolegów, którzy się na nią zgodzili.

Ochrona

Dobrze chroniona firma to połączenie rozwiązań technicznych, szkoleń dla pracowników i procedur przestrzeganych przez wszystkich pracowników niezależnie od stanowiska.

Kwestia rozwiązań technicznych jest szerokim polem do działania. Rozwiązań jest bardzo dużo, a ograniczeniem jest jedynie wielkość budżetu.

Najsłabszym ogniwem kompleksowej ochrony jest człowiek, jeżeli nie zostanie odpowiednio wyczulony na pewne działania, może stać się łatwym łupem dla specjalisty.

Odpowiednie szkolenia, które pokazują działania socjotechników, mogą zniwelować zagrożenie. Ta wiedza musi być wciąż przypominana, odświeżana. Pracownicy muszą mieć świadomość, że ujawnianie

danych firmy osobie bez wcześniejszego ustalenia jej tożsamości jest ściśle zabronione i stanowi zagrożenie dla firmy. Należy też pamiętać, że szereg teoretycznie pojedynczo bezwartościowych informacji tworzy całość. Szukanie informacji to łańcuch działań, specjaliści zaczynają od znalezienia terminologii firmy, poprzez nazwiska osób, w końcu uzyskując konkretną informację, o jaką im chodziło.

Procedury są po to, aby uszczelnić środowisko firmy i przebieg informacji, dlatego tak ważne jest, aby ich przestrzegać.

Należy także ograniczyć pole manewru pracownika, ścisła procedura pozwoli wyeliminować działania przeciwko firmie. Im ściślejsza procedura i mniejsze pole działania, tym trudniej jest się przebić do takich informacji.

Dobre zabezpieczenie firmy to kompleksowe połączenie środków technologicznych, procedur działania i ludzi. W ochronie informacji najważniejsza jest ochrona dostępu do nich. Na tym obszarze działania wiedza o tym, kto, kiedy i po co miał dostęp do informacji, jest podstawą. W razie utraty tych informacji mamy zawężony krąg osób za to odpowiedzialnych.

W takich sytuacjach często stosuje się badania poligrafem polegające na wykrywaniu śladów emocjonalnych dotyczących danego zdarzenia. W ten sposób z dużym prawdopodobieństwem możemy wytypować sprawcę. Badania te mają duże zastosowanie w biznesie na świecie, szczególnie w stosunku do ludzi mających dostęp do ważnych i cennych informacji.

Ochronę dostępu do pomieszczeń zapewniają dziś odpowiednie urządzenia identyfikujące osoby za pomocą kart dostępu, za pomocą identyfikacji głosu, linii papilarnych, siatkówki oka.

Odpowiednie zabezpieczenia to oczywiście też specjalistyczne programy komputerowe chroniące dane.

W Polsce, gdzie gospodarka wolnorynkowa jest dość młoda, wiele firm nie zdaje sobie sprawy z zagrożenia, a gdy padną jego ofiarą, często oznacza to dla nich bankructwo. Biały wywiad daje wiedzę o możliwościach działania konkurenta, czarny wywiad zaś informuje o wybranym działaniu, i to pokazuje, jak wielkie stanowi zagrożenie.

Dobrze przemyślana polityka bezpieczeństwa, połączona z odpowiednim szkoleniem, które zwiększy u pracowników świadomość zagrożenia, jest najlepszym sposobem ochrony firmy.

Podsumowanie

Czarny wywiad gospodarczy jest faktem, z którym muszą zmierzyć się wszyscy przedsiębiorcy niezależnie zarówno od wielkości swoich przedsiębiorstw, jak i skali działalności. Głównym dobrem, które jest pożądane przez konkurencję, jest informacja. Stanowi ona w dzisiejszych czasach najwyższą wartość, dlatego powinna być jak najściślej chroniona. Powodzenie jej ochrony zależy w dużej mierze od samych właścicieli i współpracy pozostałych pracowników. Odpowiedzią na pytanie o sposób zapewnienia bezpieczeństwa firmy jest procedura. Schemat zachowania wszystkich pracowników pozwala na zniwelowanie zagrożenia. Należy pamiętać, że bazowanie na ludzkich uczuciach, takich jak chęć pomocy, współczucie, potrzeba akceptacji w grupie bądź strach przed zwierzchnikiem, jest główną bronią socjotechnika. Wyuczony schemat działania nie pozostawia miejsca na takiego typu zachowania pracowników i stanowi świetną ochronę przed atakiem specjalisty. Najlepszym rozwiązaniem dla zapewnienia całościowej ochrony przedsiębiorstwa jest połączenie dobrych procedur, przestrzegających ich pracowników i środków technologicznych. Działania zapewniające bezpieczeństwo firmy muszą stanowić część jej normalnego funkcjonowania, muszą być prowadzone długofalowo i wielokanałowo.

Warto przypomnieć słowa Bruce'a Schneidera, światowego specjalisty do spraw bezpieczeństwa: „Bezpieczeństwo to nie produkt, to proces".

Dobra ochrona firmy i powierzonych jej informacji to przede wszystkim zaufanie klientów, a co za tym idzie sukces rynkowy.

Bibliografia

Martinet B., Marti Y.M., *Wywiad gospodarczy*, Warszawa 1999.

Winkler I., *Corporate Espionage*, Rocklin CA 1999.

Mendel T., *Badanie wiarygodności partnera gospodarczego*, Poznań 1993.

Kwieciński M., *Wywiad gospodarczy*, Warszawa–Kraków 1999.

Wypler K., Turek Z., *Działalność wywiadowni gospodarczych*, „Handel Zagraniczny dla Menadżerów", z. 4, Łódź 1996.

www.trade-secrets-inc.com.

http://www.schneier.com/.

Katarzyna Wójcik

Ochrona tajemnicy firmy w praktyce polskich przedsiębiorstw

Znaczenie informacji poufnych we współczesnej gospodarce jest kluczową sprawą dla osiągnięcia przewagi konkurencyjnej na rynku. Przedsiębiorcy jednak niejednokrotnie stosują nieuczciwe działania w celu zdobycia tajemnic innych przedsiębiorców, gdyż, jak zauważył D. Sarnoff, konkurencja na rynku zapewnia wprawdzie najlepsze produkty, lecz jednocześnie pociąga za sobą najgorsze zachowania ludzi. W związku z tym prawo powinno zapewniać skuteczne mechanizmy ochrony dla szeroko rozumianych informacji poufnych. Przedmiotem tajemnicy jest informacja. Sprecyzowania zatem wymaga zarówno samo pojęcie informacji, jak i jej charakter prawny. Nie ulega wątpliwości, że współcześnie informacja stała się samoistnym, cennym dobrem prawnym i tak wartościowym, że wymagającym ochrony prawnej. Gospodarcze znaczenie informacji we współczesnym świecie jest bezsporne. Ona sama traktowana jest coraz częściej jak specyficznego rodzaju towar, produkt, którego posiadanie stwarza możliwości osiągania wymiernych korzyści, porównywalnych z posiadaniem innych praw majątkowych. Dynamiczny postęp cywilizacyjny i rozwój wiedzy technicznej rodzi możliwości i jednocześnie niebezpieczeństwo różnego rodzaju przetwarzania, zdobywania i gromadzenia informacji, niekiedy przez podmioty do tego nieuprawnione. Sama informacja, jako że posiada statut dobra prawnego o wymiernej wartości ekonomicznej i społecznej, narażona jest na różnego rodzaju ataki i manipulacje, często środkami niedozwolonymi, które zmierzają do zdobycia bądź utrzymania przewagi politycznej, a przede wszystkim gospodarczej i ekonomicznej. Prawo do informacji z jednej strony i jej ochrona z drugiej stały się ważnym zagadnieniem wymagającym regulacji prawnej. Prawo dysponowania in-

formacją może mieć różnorodną podstawę i w związku z tym podlegać różnym reżimom ochrony prawnej. Kryterium pozwalającym na ustalenie tego prawa może być własność przedmiotu będącego nośnikiem informacji, fakt jej sporządzenia czy utrwalenia przez określoną osobę, czy też sama jej treść. Słusznie podkreśla W. Wróbel, że prawo do informacji może przybierać bardzo różne postaci, jak np. prawa do tajemnicy, prawa do wolności słowa, natomiast wyłączność dysponowania informacją obejmuje uprawnienia do zachowania jej w tajemnicy, prawo do zapoznania się z jej treścią z wyłączeniem innych osób, prawo do zachowania integralności zapisu, wyłączność w wykorzystywaniu oraz w rejestrowaniu i gromadzeniu informacji. Nie wszystkie wiadomości mogą być powszechnie dostępne – bądź ze względu na przedmiot, którego dotyczą, bądź też na wolę podmiotu, który nimi prawnie dysponuje. Dlatego prawny system ochrony informacji powinien być skonstruowany przy jednoczesnym uwzględnieniu i poszanowaniu prawa do nich, gwarantowanemu przez normy konstytucyjne. Realizowanie prawa do informacji może nastąpić tylko w przypadku, gdy gwarantowana jest jej jawność. Tajemnica stanowi natomiast jej zaprzeczenie i tym samym ogranicza prawo do uzyskania i dysponowania informacją. Prawo do informacji nie ma charakteru absolutnego i bezwzględnego, tym samym wpisane jest w nie jego ograniczenie. Istotą tajemnicy jest natomiast to, że informacje nią objęte nie są przeznaczone do udostępniania osobom postronnym, nieuprawnionym, z pewnych względów mogą czy też muszą pozostać znane tylko ściśle oznaczonym jednostkom czy grupom.

Nadeszła pora na próbę zdefiniowania zakresu informacji, które przez swoją wagę i znaczenie dla przedsiębiorstwa, w razie ich ujawnienia mogą narazić przedsiębiorstwo na powstanie szkody. Zagadnienie to wbrew pozorom stanowi największy problem. Jakie informacje są najważniejsze z punktu widzenia bezpieczeństwa funkcjonowania firmy i jej pomyślności w prowadzonych przedsięwzięciach? Jakiego typu informacje niemające charakteru strategicznego czy też szczególnej wagi powinny jednak zostać, ze względu na dobro firmy, objęte tajemnicą? Jakie informacje takiego charakteru nie mają i nie wymagają specjalnej

troski w zakresie ich ochrony? Odpowiadając na te niezwykle istotne pytania, postanowiliśmy odwołać się do przepisów obowiązującego prawa, które zawierają definicję informacji podlegających ochronie wraz z enumeratywnie bądź przykładowo wymienionym katalogiem takich informacji.

Zgodnie z art. 11 u.z.n.k.: ,,1. Czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy"; warto wspomnieć o zasadach ochrony zamieszczonych w komentarzu do ustawy o zwalczaniu nieuczciwej konkurencji. Art. 11 ma na celu ochronę interesów przedsiębiorcy tak, aby w posiadanie pewnych danych nie weszły osoby nieuprawnione, w tym przede wszystkim konkurenci. Warunkiem koniecznym uznania informacji za podlegające ochronie jest podjęcie niezbędnych działań w celu zachowania ich w poufności. Nie przesądzono, jakie to mają być mianowicie działania. Wydaje się więc, że każdy sposób działania, który wskazuje, że określone informacje są traktowane jako poufne, stanowić będzie realizację omawianego zalecenia ustawowego. Z tego względu ustawowy wymóg podjęcia niezbędnych działań spełni także podjęcie pewnych czynności konkludentnych, jak np. dopuszczenie do informacji jedynie wąskiego kręgu pracowników. W konkretnych okolicznościach o obowiązku dochowania tajemnicy może przesądzać sam charakter informacji w powiązaniu z poziomem wiedzy zawodowej osób do nich dopuszczonych. Wykorzystanie przez pracownika we własnej działalności gospodarczej informacji, co do których przedsiębiorca nie podjął niezbędnych działań w celu zachowania ich poufności, należy traktować jako wykorzystanie powszechnej wiedzy, do której przedsiębiorca nie ma żadnych ustawowych uprawnień. Ustawa nie precyzuje, jakie konkretnie działania prowadzą do ujawnienia, a więc powodują utratę przymiotu tajemnicy. Zapewne będzie to miało miejsce w przypadku, gdy informacja zostanie rozpowszechniona w taki sposób, iż zainteresowany może się z nią zapoznać bez zgody dysponenta, chociażby łączyło się to z pewnymi trudnościami czy kosztami. Przepisy nie wskazują również,

w jaki sposób należy badać zasięg stanu tajemnicy. Może się zdarzyć, że w posiadaniu określonych informacji może być wiele osób w różnych przedsiębiorstwach i w bardzo odległych miejscach. Powstaje pytanie, jaki sposób ujawnienia uchyla ochronę. Trudno jest generalnie tę kwestię przesądzić, wydaje się jednak, iż badać należy przede wszystkim rynek geograficzny i asortymentowy, na którym przedsiębiorca funkcjonuje, gdyż na nim właśnie materializują się interesy, o których mowa w art. 11 ust. 1. W art. 11 ust. 1 bardzo ważna jest również przesłanka odpowiedzialności tj. przekazania, ujawnienia lub wykorzystania poufnych informacji. O przekazaniu można mówić wówczas, gdy sprawca podejmuje działania zmierzające do udostępnienia osobie nieuprawnionej treści wiadomości poufnej. Przez ujawnienie należy rozumieć postępowanie, w wyniku którego informacja doszła do wiadomości osób trzecich, niezależnie od ich liczby, a więc nie jest to równoznaczne z rozpowszechnieniem. Z wykorzystaniem cudzej informacji będziemy mieli do czynienia zarówno w wypadku, gdy nabycie od nieuprawnionego umożliwi zastosowanie wiadomości poufnej we własnej praktyce gospodarczej, jak i wówczas, gdy wykorzystanie polega na zamieszczeniu informacji poufnej w publikacji prasowej czy książkowej, gdyż wykorzystanie jest równoznaczne z osiągnięciem z czegoś pożytku, skorzystaniem z czegoś. Każde naruszenie tajemnicy, jaką objęta jest cudza informacja poufna, jeśli tylko wpływa negatywnie na pozycję gospodarczą danego podmiotu, może stanowić delikt nieuczciwej konkurencji. Dlatego też podkreśla się w literaturze, iż za czyn nieuczciwej konkurencji może również zostać uznane np. ujawnienie informacji, z których uprawniony z jakichś względów nie korzysta, bądź rozwiązań stanowiących wprawdzie tajemnicę, jednak nienadających się do stosowania np. ze względu na duży koszt wdrożenia. W każdym wypadku musi zostać wykazane, że działanie sprawcy naruszyło interesy uprawnionego. Trudno jest generalnie przesądzić, kiedy ma to miejsce. W konkretnej sytuacji będzie to zależeć od okoliczności towarzyszących, w tym przede wszystkim od rynkowego znaczenia treści informacji poufnej. W świetle omawianego przepisu przedsiębiorca może bowiem otoczyć ochroną także obiektywnie mało ważne dane, np. do-

tyczące sposobu obsługi klienta. Jeśli sięgnięcie przez osobę trzecią po takie dane naruszy w jakikolwiek sposób interesy ich legalnego posiadacza, powstaje po jego stronie odpowiednie roszczenie. Jego zasadność w sytuacji, gdy gospodarczy walor informacji poufnej jest nikły, podważać można, kierując się korygującą funkcją klauzuli generalnej. Ustaleń takich dokonywać będzie sąd *casu ad casum*, kierując się konkretnymi okolicznościami rozpatrywanej sprawy.

Natomiast art. 23 u.z.n.k.: ,,Kto wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2. Tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej". Obok ochrony cywilnoprawnej ustawodawca wprowadził dla tajemnicy przedsiębiorstwa także ochronę karnoprawną. W ten sposób wzmocniona została pozycja prawna przedsiębiorcy wobec działań, które przynoszą skutek w postaci poważnej szkody. Odpowiedzialność karna dotyczyć może konkretnej osoby, wskazanej w art. 11, która bądź ujawniła tajemnicę przedsiębiorstwa, bądź wykorzystała je we własnej działalności. Jest to zatem przestępstwo indywidualne.

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji w art. 11 ust. 4 stanowi, iż: „przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności". Analizując przedstawioną definicję, określającą zakres tajemnicy informacji, należy zwrócić uwagę na kilka podstawowych jej elementów. Po pierwsze, jako informacje podlegające zachowaniu tajemnicy traktowane są te z nich, które celowo nie zostały ujawnione do wiadomości publicznej. Czyli w sposób świadomy ich jawność została ograniczona lub nawet wyłączona przez przedsiębiorcę. Idąc dalej, analizowany

przepis wymienia w szczególności pewne kategorie informacji, które, ze względu na ich szczególny walor, uznaje za informacje niejako z zasady objęte obowiązkiem zachowania tajemnicy. Wśród nich wymienia informacje techniczne, technologiczne oraz organizacyjne. Zawarcie w owym katalogu informacji tego rodzaju wydaje się oczywiste, bowiem są to informacje dotyczące podstawowych dziedzin sprawnego funkcjonowania każdego przedsiębiorstwa. Katalog ten nie jest jednak katalogiem zamkniętym, bowiem już sam ustawodawca w dalszej części przedmiotowego przepisu określa, że za tajemnicę przedsiębiorstwa mogą zostać uznane inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania zmierzające do zachowania ich poufności.

Zgodnie z literalną wykładnią art. 11 ust. 4 ustawy uznać należy, że to przedsiębiorca swoim działaniem, zmierzającym do zachowania poufności pewnych informacji, może nadać im walor tajemnicy przedsiębiorstwa. Pamiętać jednak trzeba, że nie mogą to być informacje każdego rodzaju, a jedynie te informacje, o których można powiedzieć, czy też przypisać im walor posiadania pewnej wartości gospodarczej. Ustawodawca tym samym dokonał wyznaczenia, choć nie do końca, wyraźnej granicy oddzielającej informacje mogące stanowić tajemnicę firmy od informacji innego rodzaju, którym przymiotu tajemnicy przedsiębiorstwa przypisać już nie można. Omawiany przepis, dając pewną granicę swobody w określaniu, czy dana informacja może zostać uznana za tajemnicę, pozwala przedsiębiorcy współtworzyć, współdefiniować zakres informacji, które mają dla niego oraz dla prowadzonego przez niego przedsiębiorstwa charakter strategiczny i z tego względu podlegają ochronie. Ponadto przez element uznania, że dana informacja ma określoną wymierną wartość gospodarczą, oraz jednoczesne podjęcie działań mających na celu zachowanie poufności tej informacji przedsiębiorca może rozbudować zakres informacji podlegających ochronie.

Ostatnim wnioskiem płynącym z treści analizowanego przepisu jest stwierdzenie, że informacje pozbawione przymiotu posiadania wartości gospodarczej nie mogą zostać, w myśl przepisów omawianej ustawy, uznane za informacje stanowiące tajemnicę przedsiębiorstwa. W tym

miejscu zaznaczyć należy, że przyznanie pewnym informacjom przymiotu posiadania wartości gospodarczej nie może być dokonywane na podstawie kryteriów subiektywnych, choć często taki sposób wydawałby się z punktu widzenia zainteresowanego przedsiębiorcy najwłaściwszy. Tutaj właściwym kryterium oceny należy uznać obiektywnie istniejącą wartość gospodarczą w danej sytuacji i dodatkowo umiejscowić na osi czasu ów moment, w którym dokonywana jest ocena obiektywnego istnienia wartości gospodarczej danej informacji. Naturalne jest bowiem, że pewne informacje w danym momencie, stosując obiektywne kryterium, mogą zostać uznane za posiadające wartość gospodarczą, a oceniane na podstawie tego samego kryterium w innym czasie tracą ten walor.

Określiliśmy zakres informacji, które uznane mogą być za tajemnicę przedsiębiorstwa, i doszliśmy do kolejnego niezwykle istotnego zagadnienia związanego z problemem bezprawności ujawniania informacji, które są lub mogą być uznane za tajemnicę firmy. Oczywiste jest bowiem, że nawet pewne informacje o strategicznym znaczeniu dla przedsiębiorstwa, bez cienia wątpliwości uznane za objęte tajemnicą, w pewnych wypadkach mogą, a w innych muszą, zostać ujawnione pewnym organom lub instytucjom państwowym (np. organom kontroli skarbowej, prowadzącej dochodzenie policji lub prokuraturze) czy też prawnie podane zostają do wiadomości publicznej (chociażby informacje zawarte w Rejestrze Przedsiębiorców w zakresie osób wchodzących w skład organów zarządzających osobą prawną, jej organów nadzorczych czy też o wysokości kapitału założycielskiego). Próba wymienienia wszystkich potencjalnych sytuacji, w których ujawnianie informacji stanowiących tajemnicę przedsiębiorstwa będzie uzasadnione lub wręcz konieczne, jest niecelowa i prowadziłaby do rozmycia głównego zagadnienia – czyli jak ustrzec się przed bezprawnym i niekontrolowanym wyciekiem informacji dotyczących firmy.

A zatem o istnieniu chronionej tajemnicy przedsiębiorstwa nie decyduje tylko subiektywne przekonanie przedsiębiorcy, które wyraża się w konieczności podjęcia przez niego niezbędnych działań w celu zachowania poufności informacji go dotyczących, ale także posiadanie

przez daną informację wartości gospodarczej. Wątpliwość budzić może nieostrość tego sformułowania, zwłaszcza w kontekście rozstrzygnięcia, czy wartość gospodarczą należy oceniać obiektywnie, czy też chodzi o wartość określonej informacji dla danego przedsiębiorcy. W kontekście powyższych rozważań opowiedzieć się jednak należy za zobiektywizowanym kryterium oceny istotności gospodarczej określonej informacji. Wymóg posiadania przez określoną informację wartości gospodarczej oznacza, że powinna ona mieć zastosowanie w działalności gospodarczej. Wydaje się również, że z dysponowaniem taką informacją wiązać się będą określone korzyści materialne czy majątkowe dla przedsiębiorcy. O wartości gospodarczej danej informacji przesądza jednakże możliwość jej praktycznego wykorzystania w działalności gospodarczej. Gospodarcza wartość informacji wyraża się w tym, że z jej posiadaniem, dysponowaniem czy wykorzystaniem wiązać się mogą określone korzyści, wpływające na osiągnięcie przewagi konkurencyjnej w działalności gospodarczej. Inaczej rzecz ujmując, można stwierdzić, że określona informacja posiada wartość gospodarczą, jeżeli jej pozyskanie przez innego przedsiębiorcę – konkurenta – pozwoliłoby mu na zaoszczędzenie określonych wydatków lub czasu, które musiałby ponieść lub przeznaczyć na osiągnięcie stanu wynikającego z posiadania tych informacji. Ponadto, co wynika zresztą z samej istoty tajemnicy, aby określone informacje mogły stanowić tajemnicę przedsiębiorstwa, muszą być niepodane do publicznej wiadomości, tzn. znane tylko pewnym, ściśle określonym osobom czy grupom, a nie powszechnie dostępne. Nie mogą być to również informacje, o których każdy konkurent może się dowiedzieć zwykłą i legalną drogą np. z fachowych publikacji. Taki pogląd wyrażony został zarówno w doktrynie, jak i w orzecznictwie. W uzasadnieniu wyroku z dnia 3 października 2000 r. (I CKN 304/00, OSNC 2001, nr 4, poz. 59) SN stwierdził, że „informacja nieujawniona do wiadomości publicznej traci ochronę prawną, gdy każdy przedsiębiorca (konkurent) dowiedzieć się o niej może drogą zwykłą i dozwoloną, a więc np. gdy pewna wiadomość jest przedstawiana w pismach fachowych lub gdy z towaru wystawionego na widok publiczny każdy fachowiec poznać może, jaką metodę produkcji zastosowano". Podobnie w wyro-

ku z dnia 5 września 2001 r. (I CKN 1159/00, OSNC 2002, nr 5, poz. 67). Sąd ten uznał, że: „Przepis art.11 ust. 1 i 4 u.z.n.k. nie pozwala na objęcie tajemnicą informacji powszechnie znanych lub takich, o treści których określony podmiot ze względu na rodzaj prowadzonej działalności jest zainteresowany ich posiadaniem i może się o nich dowiedzieć w zwykłej i dozwolonej drodze. Co więcej, informacja dotychczas nieznana traci swój tajny charakter i tym samym ochronę. Wówczas, gdy zostanie rozpowszechniona w sposób pozwalający każdemu zainteresowanemu na zapoznanie się z nią bez zgody dysponenta". Wątpliwości może budzić problem, czy jeżeli większość konkurentów na danym rynku posiada określoną informację, lecz wciąż uznaje ją za poufną, może ona stanowić prawnie chronioną tajemnicę przedsiębiorstwa. Przyjmuje się, że za tajemnicę można uznawać także takie informacje, którymi dysponuje nie tylko jeden przedsiębiorca. Kwestię tę rozstrzygał już w wyroku z dnia 22 kwietnia 1938 r. SN, stwierdzając, że ,,tajemnica nie traci swojego charakteru poprzez to, że wie o niej pewien ograniczony krąg osób, które przedsiębiorca wtajemnicza w proponowane im przedsięwzięcie, zastrzegając wyraźnie lub w sposób dorozumiany dochowanie tajemnicy na wypadek niezawarcia umowy". Aby informacja mogła stanowić chronioną prawnie tajemnicę przedsiębiorstwa, przedsiębiorca musi podjąć w stosunku do niej niezbędne działania w celu jej utajnienia. Znaczy to, że powinien przedsięwziąć określone środki chroniące informacje przed ujawnieniem, zapobiegające dotarciu do nich przez osoby postronne. Przykładem może być fakt, iż pracownik powinien zostać poinformowany o poufnym charakterze danej wiedzy, techniki czy urządzenia. Ustawa o zwalczaniu nieuczciwej konkurencji nie zawiera żadnych regulacji w zakresie sposobów ochrony tajemnicy przedsiębiorstwa. W uzasadnieniu do wyroku z dnia 5 września 2001 r. (I CKN 1159/00, OSCN 2002, nr 5, poz. 67) SN zwrócił uwagę, że działania przedsiębiorcy „powinny zmierzać do osiągnięcia takiego stanu, w którym osoby trzecie, chcąc zapoznać się z treścią informacji, muszą doprowadzić do wyeliminowania przyjętych przez przedsiębiorcę mechanizmów zabezpieczających przed niekontrolowanym wypływem danych. Wybór informacji, które mają zostać objęte poufnością,

należy oczywiście do przedsiębiorcy, jednakże wybór ten co do stanu tajemnicy nie może być oderwany od możliwości podjęcia niezbędnych działań w celu zachowania w poufności wybranych informacji". Z kolei w wyroku z dnia 3 października 2000 r. (I CKN 304/00, OSNC 2001, nr 4, poz. 59), Sąd wskazał, że „decyzja o utajnieniu danych informacji nie może wynikać tylko ze swobodnego uznania przedsiębiorcy, lecz powinna opierać się na uzasadnionym przypuszczeniu, że: dana wiadomość nie była jeszcze publicznie znana, jej ujawnienie zagrażałoby istotnym interesom przedsiębiorcy, wiadomość ta może być uważana za poufną w świetle zwyczajów i praktyki danej branży lub zawodu". Działania podjęte celem zachowania poufności muszą być rozpoznawalnym dla osób trzecich przejawem woli przedsiębiorcy – dysponenta informacji co do korzystania z określonych informacji z wyłączeniem innych osób, które uznaje za nieuprawnione. Ponieważ ustawa nie precyzuje, jakiego rodzaju środki prewencyjne mają być przez przedsiębiorcę podjęte, przyjąć należy, że każdy sposób, który wskazuje treść informacji poufnych i zabezpiecza dostęp do nich, wystarczy do realizacji tego ustawowego wymogu. Przepis nie wymaga bowiem, aby były to jakieś szczególne zabezpieczenia, stanowiące przeszkodę, którą trzeba by było pokonać, żeby móc zapoznać się z chronionymi informacjami. Wystarczy bowiem, aby wola przedsiębiorcy co do nieujawniania i zachowania w poufności określonych informacji była dostatecznie wyrażona na zewnątrz i rozpoznawalna dla osób trzecich.

Istnieją niezbędne działania, które są konieczne do zapewnienia informacjom ochrony, jednocześnie precyzyjnie określające sferę i zakres poufności. O tym, czy podjęte działania są wystarczające do zabezpieczenia sekretów, decydują oczywiście konkretne okoliczności i warunki funkcjonowania danego przedsiębiorcy. Słusznie zauważa S. Hoc w głosie aprobującej do powołanego orzeczenia SN z dnia 3 października 2001 r., że użycie ,,słowa »niezbędnych« wskazuje, że nie chodzi o jakiekolwiek działania przedsiębiorcy, ale o takie, które dają gwarancję nieuzyskania tajemnicy przez osoby nieuprawnione. Przedsiębiorca ma obowiązek podjęcia działań, które zgodnie z wiedzą i doświadczeniem zapewniają ochronę przed rozpowszechnieniem czy ujawnie-

niem. Wskazuje to na obiektywną ocenę użytego w przepisie zwrotu »niezbędność«. Działanie przedsiębiorcy ma stworzyć warunki dające duże prawdopodobieństwo, że informacja nie zostanie ujawniona. Wydaje się, że przedsiębiorca, który chce zapewnić swoim tajemnicom naprawdę skuteczną ochronę, powinien podjąć środki składające się na kompleksowy system ochrony takich informacji, zarówno przez wykorzystanie formalnych, fizycznych zabezpieczeń o charakterze systemowym, jak też przez wyraźne poinformowanie pracowników o poufności określonych informacji". Dowodem przedsiębrania niezbędnych działań zmierzających do zachowania stanu tajemnicy może być zatem posługiwanie się przez dysponenta tajemnicy (zwłaszcza wobec kontrahentów czy osób trzecich) odpowiednimi instrumentami prawnymi i mechanizmami zabezpieczającymi przed niekontrolowanym przepływem danych, jak: zapewnienie odpowiedniego obiegu dokumentów podlegających utajnieniu, ograniczanie dostępu do pewnych dokumentów lub miejsc, określenie w regulaminie pracy czy innych aktach wewnętrznych informacji objętych tajemnicą, wprowadzenie do umów klauzul poufności, wprowadzenie systemu monitoringu i identyfikacji pracowników, oznaczenie materialnych nośników poufnych informacji odpowiednimi ostrzeżeniami, wdrażanie okresowych wewnętrznych procedur lustracyjnych, ograniczanie dostępu do komputerów, przez wprowadzenie technicznych zabezpieczeń, wprowadzenie procedur kontroli pracowników i innych osób oraz procedur na wypadek ujawnienia informacji. Tak więc określona wiadomość, nawet o dużej wartości obiektywnej czy też szczególnej istotności dla przedsiębiorcy, może nie zostać uznana za chronioną prawnie tajemnicę przedsiębiorstwa, jeśli niefrasobliwy czy też niedbały przedsiębiorca nie podejmie żadnych kroków w celu zapewnienia jej poufności. Zgodnie z tezą orzeczenia SN z dnia 3 października 2000 r. „wykorzystanie przez pracownika we własnej działalności gospodarczej informacji, co do których przedsiębiorca (pracodawca) nie podjął niezbędnych działań w celu zachowania ich w poufności, należy traktować jako wykorzystanie powszechnej wiedzy, do której przedsiębiorca nie ma żadnych ustawowych uprawnień". Podkreślenia także wymaga, że tajemnicą nie mogą być objęte

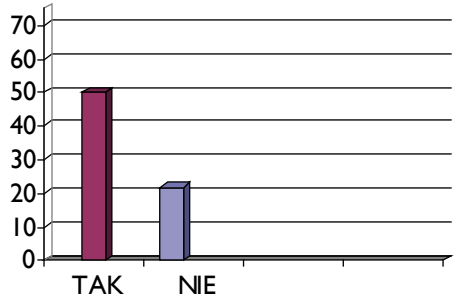
takie informacje dotyczące działalności gospodarczej, które na podstawie przepisów innych ustaw muszą być ujawniane lub co do których obowiązuje zasada jawności, niemogąca być wolą przedsiębiorcy wyłączona. I tak na przykład ustawa z dnia 29 września 1994 r. o rachunkowości, zawiera z jednej strony przepisy służące ochronie informacji zamieszczonych w księgach rachunkowych, z drugiej jednak nakłada na przedsiębiorcę obowiązek upublicznienia niektórych dotyczących go informacji. Podobnie zakres informacji chronionych ograniczają przepisy ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (tekst jedn. Dz.U. z 2001 r. nr 17, poz. 209 z późniejszymi zmianami), które jako zasadę przewidują jawność i powszechną dostępność Rejestru – art. 8 – oznaczającą, że każdy ma prawo dostępu do danych zawartych w Rejestrze za pośrednictwem Centralnej Informacji. Ponadto każdy ma prawo otrzymywać poświadczone odpisy, wyciągi i zaświadczenia o danych zawartych w Rejestrze. Treść danych umieszczanych w poszczególnych działach rejestru przedsiębiorców określają art. 38––44 powołanej ustawy. Na przedsiębiorcach podlegających obowiązkowi wpisu do rejestru ciąży również obowiązek zgłaszania informacji wymienionych w art. 38–40 i art. 44 ustawy oraz wszelkich ich zmian. Poufność niektórych wiadomości wyłączają także przepisy ustawy z dnia 14 lutego 2003 r. o udostępnianiu informacji gospodarczych (Dz.U. nr 50, poz. 424), która określa zasady i tryb udostępniania przez przedsiębiorców informacji gospodarczych dotyczących wiarygodności płatniczej innych przedsiębiorców i konsumentów, w szczególności danych o zwłoce w wykonywaniu zobowiązań pieniężnych, osobom trzecim nieoznaczonym w chwili przeznaczenia tych danych do udostępnienia. W wymienionych wyżej przypadkach, tzn. gdy przepisy ustaw zakładają jawność niektórych informacji, wykluczone jest objęcie ich tajemnicą, a przedsiębiorcy nie wolno w stosunku do nich podejmować działań zmierzających do zachowania ich poufności.

Współczesne ustawodawstwa regulują kwestie ochrony szeroko rozumianych tajemnic przedsiębiorstwa na dwa sposoby, tzn. po pierwsze: uchwalenie osobnych ustaw regulujących ochronę tajemnic przedsiębiorstwa np.: Japonia, Szwecja, USA, gdzie obowiązuje Uniform

Trade Secret Act z 1985 r. i wydane na jego podstawie poszczególne ustawy stanowe, a drugi sposób normowania oznacza w zasadzie brak kompleksowej regulacji, tzn. nie tworzy się osobnego i jednolitego aktu w zakresie ochrony tajemnicy przedsiębiorstwa, lecz chroni tajemnice komercyjne w różnych aktach prawnych, w szczególności w ustawach dotyczących zwalczania nieuczciwej konkurencji, przykładem są tutaj Brazylia, Niemcy i Polska. Spośród wskazanych powyżej metod regulacji korzystniejsza z punktu widzenia efektywnej ochrony jest metoda pierwsza, czyli opierająca się na tworzeniu osobnych aktów prawnych w zakresie ochrony tajemnic przedsiębiorstwa. Przede wszystkim dzięki istnieniu osobnej ustawy uzyskujemy spójną i mającą zastosowanie do wszystkich aktów prawnych definicję tajemnicy przedsiębiorstwa oraz bardziej czytelny system dochodzenia roszczeń. Istnienie takiej osobnej ustawy ułatwia znacząco interpretację przepisów i ujednolica system prawny. Jeżeli brakuje spójnego ustawodawstwa poświęconego ochronie tajemnic handlowych, ochrona tajemnicy przedsiębiorstwa ulega rozproszeniu i osłabieniu, gdyż podmioty stosujące prawo zmuszone są dokonywać interpretacji i stosowania prawa, opierając się na różnych postanowieniach ustawowych. Należy jednak podkreślić, że przy prawidłowej redakcji postanowień ustawy o zwalczaniu nieuczciwej konkurencji przepisy zawarte w takiej ustawie również mogą zapewniać skuteczną ochronę tajemnicy przedsiębiorstwa. Należy zauważyć, że liczba źródeł *sensu stricto*, a więc bezpośrednio poświęconych ochronie tajemnicy przedsiębiorstwa, jest w prawie polskim ograniczona i sprowadza się w zasadzie do ustawy o zwalczaniu nieuczciwej konkurencji. Natomiast w ramach źródeł prawa *sensu largo* istnieje znacząca grupa aktów prawnych, które na różne sposoby chronią tajemnicę przedsiębiorstwa. Ponieważ w prawie polskim brak jest osobnej ustawy poświęconej ochronie tajemnicy przedsiębiorstwa, należy poszukać regulacji, która stanowiłaby punkt odniesienia dla innych aktów prawnych i pełniłaby rolę swoistego wzorca w zakresie ochrony tajemnicy przedsiębiorstwa. Podstawą takiej wzorcowej regulacji powinien być art. 11 u.z.n.k., ponieważ definicja tajemnicy przedsiębiorstwa z ustawy o zwalczaniu nieuczciwej konkurencji wydaje się najbardziej

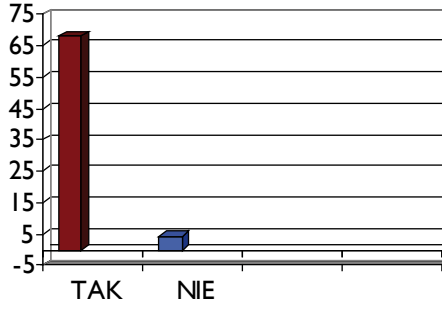
przejrzysta i kompleksowa. Oznacza to, że jeżeli przykładowo kodeks postępowania cywilnego używa pojęcia ,,tajemnice produkcyjne", to należy ten termin rozumieć właśnie w kontekście art. 11 u.z.n.k. Jest to w istocie próba ujednolicenia pojęcia tajemnicy przedsiębiorstwa poprzez stosowanie zasad wykładni systemowej. Należy zauważyć, że przyjęcie przedstawionej powyżej tezy nie jest rozwiązaniem doskonałym, ale w obecnym stanie prawnym wydaje się zabiegiem najbardziej rozsądnym, gdyż w przeciwnym razie nie można by rozwikłać wielu problemów interpretacyjnych. Zastosowanie takiej koncepcji pozwala na osiągnięcie efektu ujednolicenia, tak jak w wypadku obowiązywania odrębnej ustawy o ochronie tajemnicy przedsiębiorstwa. Z drugiej strony należy podkreślić, że podstawowy charakter u.z.n.k. dla ochrony tajemnicy przedsiębiorstwa nie oznacza, że cały system prawny oparty jest wyłącznie na tej jednej ustawie. Bliższa analiza przepisów dotyczących ochrony tajemnicy przedsiębiorstwa uzasadnia twierdzenie, że prywatnoprawna ochrona tajemnicy przedsiębiorstwa opiera się na zróżnicowanych podstawach i instytucjach prawnych.

Przeprowadzona przeze mnie ankieta w siedemdziesięciu dwóch przedsiębiorstwach na terenie województwa śląskiego pozwoliła mi w minimalnym procencie przedstawić uwzględniane zasady ochrony tajemnicy w przedsiębiorstwie oraz poznać skutki jej naruszenia.



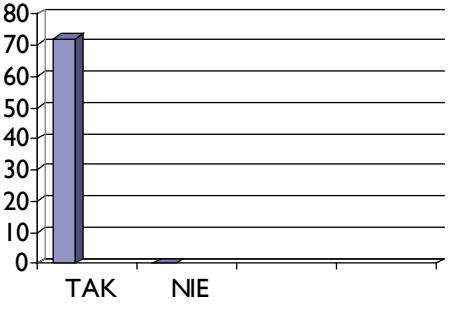
Wykres 1.

Wyniki przeprowadzonej przeze mnie ankiety pozwalają mi stwierdzić, że na 72 przedsiębiorstwa odpowiadające na pytanie: ,,4. Czy tajemnica przedsiębiorstwa w zarządzanym przez Pana/ Panią przedsiębiorstwie jest kontrolowana przez współpracowników?", 50 przedsiębiorców odpowiada TAK, 22 NIE (wykres 1).



Wykres 2.

Na pytanie: ,,9. Czy zgodnie z treścią art. 11 ust. 4 u.z.n.k. Pańscy/ Pani pracownicy są zobowiązani do konkretnego zachowania w celu nieujawnienia zachowania poufności owych informacji?", 68 zarządzających przedsiębiorstwem odpowiedziało, że pracownicy w ich firmach są zobowiązani do konkretnego zachowania w celu zachowania poufności informacji (wykres 2).



Wykres 3.

Na pytanie: ,,11. Czy zdarzyło się w zarządzanym przez Pana/Panią przedsiębiorstwie, że pracownik rozpowszechnił tajemnicę przedsiębiorstwa?" wszyscy zgodnie przyznali, że niestety w ich przedsiębiorstwach takie zjawisko miało miejsce (wykres 3).

Dogłębna analiza owej sondy pozwala mi stwierdzić, że działania do zachowania sekretności informacji, wytypowanych jako tajemnica przedsiębiorstwa, powinny osiągnąć stan wymagający od osób postronnych, pragnących się z nimi zapoznać, jakiegoś rodzaju wyeliminowania zastosowanych mechanizmów zabezpieczających. Ciągła ewolucja struktur organizacji firm, przedsiębiorstw i instytucji, fuzje, globalizacja, brak jednolitych międzynarodowych przepisów prawa ochrony danych oraz różnice w poziomie gwarantowanego bezpieczeństwa i ochrony informacji przez państwo skłaniają do stworzenia modelu pośredniego. Może być rozpatrywany jako zarządzenie centralne z pełnymi kompetencjami i odpowiedzialnością za strategię i jej realizację w ramach całej organizacji lub w ramach regionu. Główną zaletą przyjętej koncepcji tajemnicy jest obdarzenie przedsiębiorcy pełną wolnością w ochronie informacji, które uzna za godne ochrony. Zadaniem prowadzących przedsiębiorstwa jest racjonalne i adekwatne, a przede wszystkim zgodne z prawem nałożenie obligacji na informację, które dla dobra i rozwoju przedsiębiorstwa powinny być objęte tajemnicą. Wyniki Światowego Badania Bezpieczeństwa Informacji, przeprowadzonego juz po raz ósmy przez Ernst & Young, wskazują, że coraz ostrzejsze wymogi stają się głównym powodem skłaniającym przedsiębiorstwa do podejmowania działań związanych z bezpieczeństwem informacji. Badaniu poddano kierownictwo wyższego szczebla ponad 1300 organizacji z 55 krajów świata. W Polsce w badaniu wzięły udział 33 firmy z różnych branż, między innymi: finansowej, paliwowej oraz informatycznej. Po raz pierwszy respondenci wskazali konieczność dostosowania się do wymogów prawnych jako najważniejszy powód podejmowania działań związanych z bezpieczeństwem informacji. Na świecie było to 61% badanych, w Polsce aż 78%. Nowe regulacje, między innymi takie jak Ustawa Sarbanes–Oxley, Nowa Bazylejska Umowa Kapitałowa czy unijna VIII Dyrektywa, powodują, że wymagania wobec przedsiębiorstw są coraz ostrzejsze. Chcąc je spełnić,

firmy muszą podejmować nowe inicjatywy i zarządzać bezpieczeństwem informacji w sposób kompleksowy. W polskich warunkach wymogi te są szczególnie restrykcyjne w przypadku branży finansowej, co wyraźnie pokazują tegoroczne wyniki badania. Wiele przedsiębiorstw dostrzega istotne zagrożenie dla bezpieczeństwa informacji, wynikające ze stosowania nowych rozwiązań technologicznych. Na pierwszym miejscu znajdują się przenośne urządzenia informatyczne, które wskazało 53% badanych na świecie i aż 71% w Polsce. Wymienne nośniki danych to zagrożenie dla 49% firm na świecie i 59% w Polsce. Na trzecim miejscu wskazywane były sieci bezprzewodowe – 48% respondentów na świecie i 47% w Polsce. Wymienione rozwiązania technologiczne powodują, że kontrolowanie informacji istotnej dla przedsiębiorstwa jest coraz trudniejsze. Wyniki badania wskazują także, że wiele organizacji nie zarządza odpowiednio ryzykiem naruszenia bezpieczeństwa informacji przez ich dostawców, kontrahentów i klientów lub zarządza nim jedynie w sposób nieformalny. Certyfikaty bezpieczeństwa informacji, takie jak ISO 17790/BS 7799, CobIT, ITIL, stają się coraz popularniejsze. Najbardziej rozpowszechniony z nich – ISO 17799 – wdrożyło już 25% biorących udział w badaniu firm na świecie, kolejne 30% firm planuje takie wdrożenie. W Polsce wskaźnik ten wynosi odpowiednio 19 i 44%. Głównym celem tych działań jest chęć budowania pozytywnego wizerunku firmy. Światowe Badanie Bezpieczeństwa Informacji 2005 wskazuje na poważną dysproporcję pomiędzy rosnącą liczbą zagrożeń dla tego bezpieczeństwa a podejmowanymi w tej kwestii działaniami. Firmy powinny wykorzystać szansę, jaką daje im konieczność dostosowania się do wymogów prawnych. Wdrażając formalne procedury zarządzania ryzykiem związanym z dostawcami i partnerami biznesowymi, przedsiębiorstwa mogą zwiększyć korzyści wynikające ze współpracy z nimi. Podjęcie działań umożliwiających bezpieczne funkcjonowanie w świecie technologii mobilnej to kolejne wyzwanie, z którym należy się zmierzyć. Poddanie się procesowi certyfikacji lub wdrożenia uznanego standardu wymusi na firmach stosowanie najlepszych praktyk w zakresie bezpieczeństwa informacji, a także zwiększy ich przewagę konkurencyjną.

Dokonując oceny ochrony tajemnicy przedsiębiorstwa na podstawie obowiązujących przepisów prawa, stwierdzić należy, że najpełniejsza i najbardziej kompleksowa ochrona przewidziana jest w ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, w której zachowania godzące w tajemnicę przedsiębiorstwa zostały potraktowane jako czyny nieuczciwej konkurencji. Sprawca takich czynów narażony jest na odpowiedzialność cywilnoprawną, jak również prawnokarną, bowiem ochrona tajemnicy przedsiębiorstwa we wskazanej ustawie realizowana jest dwutorowo. Ponadto w przepisach innych aktów normatywnych odnaleźć można fragmentaryczne regulacje zapewniające zachowanie poufności informacji objętych tajemnicą przedsiębiorstwa – bądź przez nałożenie obowiązku zachowania poufności na podmioty mogące w zakresie swojego działania wejść w posiadanie takich informacji, bądź przez zapewnienie środków uniemożliwiających ich ujawnienie, rozpowszechnianie czy też zapoznanie się z nimi przez osoby trzecie. Istnieje także możliwość pośredniej ochrony tajemnicy przedsiębiorstwa w tych przypadkach, w których informacje nieobjęte wchodzą jednocześnie w zakres innych tajemnic prawnie chronionych, a przepisy prawa zapewniają tym tajemnicom także odrębne, niezależne środki ochrony. Z przeprowadzonej analizy definicji tajemnicy przedsiębiorstwa wynika, że stanowi ona samodzielny, odrębny rodzaj tajemnicy chronionej instrumentami prawa. Tajemnicy tej nie można bowiem utożsamiać z tradycyjnymi pojęciami np. tajemnicy państwowej, zawodowej czy służbowej, choć częstokroć nie da się przeprowadzić wyraźnej granicy między nimi, tym bardziej że informacje wchodzące w ich zakres pokrywają się przedmiotowo. Aby określone informacje stanowić mogły tajemnicę przedsiębiorstwa, muszą należeć do rodzajów informacji określonych w art. 11 ust. 4 u.z.n.k., a ponadto za zachowaniem sekretu musi przemawiać wola i interes przedsiębiorcy. Wynika to z ustawowego wymogu podjęcia przez przedsiębiorcę niezbędnych działań celem zachowania poufności takich informacji (teoria woli). Ujawnienie ich, wykorzystanie czy nabycie musi natomiast zagrażać istotnym interesom przedsiębiorcy (teoria interesu). Reasumując, wydaje się, że tajemnica przedsiębiorstwa na gruncie obowiązujących przepisów ma

zapewnioną ochronę. Wtórną kwestią jest natomiast praktyczna realizacja tej ochrony. Pomimo przedstawionych wątpliwości interpretacyjnych dotyczących analizowanej problematyki wydaje się jednak, że wraz z tempem rozwoju życia gospodarczego i w kontekście integracji europejskiej omawiane przepisy znajdą szersze zastosowanie.

Bibliografia

Borowiecki R., Kwieciński M., *Monitorowanie otoczenia – w stronę inteligencji przedsiębiorstwa*, Kraków 2003.

Kodeks cywilny, stan prawny na 1 września 2005 roku, Bielsko-Biała 2005

Kodeks karny, stan prawny na 1 września 2005 roku, Bielsko-Biała 2005.

Kodeks pracy 2006, z komentarzem J. Chałusa i H. Kwiatkowskiej, stan prawny na 1 stycznia 2006 roku, Warszawa 2006.

Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu*, Warszawa 2004.

Korzeniowski L., *Podstawy zarządzania. Menedżment*, Kraków 2003.

Kozłowska-Kalisz P., *Odpowiedzialność karna za naruszenie tajemnicy przedsiębiorstwa*, Kraków 2006.

Michalak A., *Ochrona tajemnicy przedsiębiorstwa – zagadnienia cywilnoprawne*, Kraków 2006.

Nowińska E., Du Vall M., *Komentarz do ustawy o zwalczaniu nieuczciwej konkurencji*, Warszawa 2005.

TRIPS, *Agreement on Trade Related Aspects of Intellectual Property Rights* [Porozumienie w sprawie handlowych aspektów praw własności intelektualnej; Obwieszczenie Ministra Spraw Zagranicznych z dnia 12 lutego 1996 r. w sprawie publikacji załączników do Porozumienia ustanawiającego Światową Organizacje Handlu WTO], Dz.U. nr 32, poz. 143.

Ustawa o zwalczaniu nieuczciwej konkurencji, stan prawny na 3 marca 2004 roku, zmiany: 2003.11.28, Dz.U. z 2003 r. nr 153, poz. 1503.

Iga Bałos

Atak socjotechniczny – skala zagrożenia

Czym jest socjotechnika?

Socjotechnika (ang. *Social Engineering*)[1] to ogół metod świadomego wywierania wpływu na grupy ludzi lub jednostki. Skuteczne oddziaływanie powinno prowadzić do zmiany postaw i zachowań. Efektem manipulacji może być na przykład udzielenie informacji lub wykonanie czynności, o które zostanie się poproszonym. Metoda opiera się na wykorzystywaniu uniwersalnych skłonności ludzi, co niejednokrotnie pozwala na schematyczne postępowanie w podobnych sytuacjach.

Stosowane są różnorodne techniki manipulacji. Dzięki socjotechnice często można uniknąć fizycznego pojawienia się w miejscu, które jest inwigilowane. Wystarczy na przykład wykonanie telefonu, celem rozmowy o perswazyjnym i manipulacyjnym charakterze. Niektórzy wzbudzają w ofiarach zaufanie, zmieniając swoją tożsamość. Podają się za pracowników tej samej firmy, kolegów z pracy, zwierzchników. Nakłaniając swoje ofiary do udzielania informacji o różnym stopniu poufności, skutecznie opóźniają lub eliminują fakt popełnienia przestępstwa. Proszą innych o wykonanie drobnych czynności. Nie grożą i nie zastraszają rozmówcy. Z pozoru nie wyrządzają żadnej szkody. W każdym razie żadnej, której skutki można odczuć natychmiast.

Stosowane metody socjotechniczne muszą pozostawać w ścisłym związku z rozwojem technologii. Informacje są przechowywane za pomocą nośników elektronicznych lub wirtualnych baz danych i przekazywane również drogą elektroniczną. Okazuje się jednak, że czynnik ludzki wciąż ma ogromne znaczenie w procesie zarządzania informacją.

---

[1] W polskiej literaturze można także spotkać kalkę językową *inżynieria społeczna.*

Pokonanie rozwiązań technicznych jest jedynie jednym z etapów jej pozyskiwania. Gdy do osiągnięcia celu kontakt z maszyną jest niewystarczający, niezastąpiona jest właśnie socjotechnika. Metody socjotechniczne, stosowane w tego typu atakach, nie różnią się od tych standardowych. Zdobywana informacja nie jest jednak celem sama w sobie. Zazwyczaj jest potrzebna, by włamać się do danej sieci, ustalić hasło czy zdobyć konkretny plik. Socjotechnika jest ogniwem, które składa się na atak o wydłużonym cyklu. W przypadku kontaktu z żywą osobą, niezależnie czy przez Internet, czy rozmowę telefoniczną, wykorzystywane są te same mechanizmy. Wiedza technologiczna może być użyteczna dopiero, gdy ofiara ataku w jakiś sposób ułatwi skorzystanie z niej.

Statystyki dotyczące przeprowadzonych ataków socjotechnicznych nie są wiarygodne. Zwłaszcza tych, które dotyczą szeroko pojętego biznesu i pieniędzy. Należy wziąć pod uwagę niechęć do ujawniania faktu, że atak w ogóle nastąpił. Jest to motywowane względami bezpieczeństwa lub obawą przed utratą prestiżu przez daną placówkę. Pewne statystyki, obejmujące wyłącznie rynek amerykański, przeprowadziła Federalna Komisja Handlu (FTC)[2]. Dotyczyły one strat poniesionych przez instytucje finansowe w wyniku kradzieży tożsamości ich klientów. Oszuści uzyskiwali dane ofiar, takie jak numer polisy ubezpieczeniowej, numery kont i informacje o charakterze osobistym. Otrzymywali dostęp do konta lub zakładali nowe, posługując się cudzą tożsamością. W latach 1998–2003, ofiarą takich oszustw padło łącznie 27,3 mln Amerykanów. Ponad połowa wiedziała, w jaki sposób do tego doszło. Jedna czwarta z nich była pewna, że dane zostały skradzione. Natomiast aż 75% przyznało, że być może samodzielnie udostępniło informacje. Ta niepewność świadczy, iż prawdopodobnie nastąpiło to w wyniku ataku socjotechnicznego. W 2002 straty instytucji finansowych wyniosły ponad 48 mld dolarów. Średnio każdej firmie skradziono 4,8 tys. dolarów.

Cele i ofiary ataku socjotechnicznego

Socjotechnika jest wygodnym narzędziem do pozyskiwania różnego typu informacji. Aby inwestycja w proces gromadzenia danych była

[2] Dane za: Sz. Augustyniak, *Ofiary kradzieży tożsamości mówią*, 2003, www.networld.pl.

opłacalna, najczęściej dotyczą one sfery gospodarczej. Ściślej ujmując, powiązanej w jakiś sposób z pieniądzem. Stworzenie uniwersalnej definicji terminu „informacja o znaczeniu gospodarczym" nie jest możliwe. W związku z tym sfera zainteresowań socjotechniką pozostaje nieograniczona. Informacja o znacznej wartości nie musi bezpośrednio dotyczyć finansów. Znaczenia nabiera często umiejętność jej wykorzystania. Warto więc traktować informację jako kapitał, który może zaowocować konkretnym zyskiem w przyszłości.

Poniższa klasyfikacja przedstawia informacje o różnym charakterze. Jedynie niektóre z nich dają bezpośredni dostęp do pieniędzy. Inne, sprytnie wykorzystane, mogą stać się źródłem finansowego sukcesu. Warto także podkreślić, że użyteczność informacji zależy od konkretnej perspektywy.

Informacje użyteczne z punktu widzenia przedsiębiorstwa:
- lista nazwisk wykwalifikowanych pracowników, którzy mieliby ochotę rozpocząć pracę dla konkurencyjnej firmy,
- tematyka badań rynku prowadzonych przez konkurencyjną firmę,
- informacje dotyczące bezpośrednio innowacyjnych projektów konkurencji, w tym specyfikacje produktów, przewidywane rynki zbytu *etc*.

Informacje pozyskiwane do użytku osobistego:
- poziom zarobków pracowników piastujących to samo stanowisko co osoba poszukująca informacji,
- dane umożliwiające kradzież wirtualnego pieniądza, np. numery kart kredytowych, hasła i kody umożliwiające przelew osobie nieuprawnionej *etc*.

Informacje pozyskiwane z powodów osobistych, nie bez znaczenia dla danego przedsiębiorstwa:
- wszelkie dane gromadzone przez niezadowolonych, byłych lub obecnych, pracowników, mające na celu kompromitację zwierzchnika i uniemożliwienie realizacji zaplanowanej strategii gospodarczej.

Socjotechnik, nawet jeśli realizuje zlecenie, sam dokonuje wyboru ofiary. Jest wynagradzany między innymi za to, że będzie potrafił dotrzeć do pożądanej informacji. Często korzysta z informatorów pośrednich. Pozyskana informacja może się okazać jedynie kolejnym ogniwem, zbliżającym do zrealizowania konkretnego zadania.

Odpowiedź na pytanie, kto tak naprawdę jest ofiarą socjotechnika, jest dyskusyjna. Można stwierdzić, że to osoba lub jednostka, która ponosi straty w wyniku jego działania. Uważam jednak, że ofiarą jest osoba udzielająca danej informacji. To jej umysł został zmanipulowany i odwiedziony od racjonalnego działania. Fakt, że osoba ta nie zawsze dozna szkody finansowej, ma drugorzędne znaczenie.

Opisane poniżej metody manipulacji nie zawsze są wyrafinowane. Ich skuteczność świadczy o niskim poziomie świadomości zagrożenia wśród potencjalnych ofiar.

Cykl socjotechniczny

Każde realizowane zadanie, nazywane dalej atakiem socjotechnicznym, wymaga podzielenia na etapy. Sama umiejętność manipulowania i sztuka perswazji nie są wystarczające. Prawdą jest, że socjotechnik musi często polegać na instynkcie i improwizować. Dopóki jednak wydarzenia będą rozwijać się zgodnie z założeniem, działa w myśl przygotowanego planu.

W pierwszej kolejności atakujący gromadzi informacje dotyczące celu zlecenia. Wiedza merytoryczna jest konieczna, by uzyskać potrzebne dane. Dzięki znajomości tematu, atakujący trafnie wybiera źródła informacji i, co najważniejsze, potrafi zbudować z nich kompletną całość. Szpieg przemysłowy pozyskujący specyfikacje i projekty premierowego oprogramowania w pierwszej kolejności jest informatykiem, dopiero później socjotechnikiem. Nawet jeśli nie jest znawcą w danej dziedzinie, musi sprawiać wrażenie, że nim jest. W początkowej fazie socjotechnik przechodzi swoisty proces edukacyjny i zbiera możliwie najwięcej informacji powszechnie dostępnych. Dane łatwe do zdobycia stworzą podstawę, dzięki której można będzie dowiedzieć się tego, co jest właściwym celem zadania. Można je

czerpać ze źródeł służących, teoretycznie, interesom celu ataku. Należą do nich wszelkie broszury informacyjne, promocyjne artykuły w prasie *etc.* Ważne mogą okazać się także ogólne zasady funkcjonowania firmy, sposób realizacji jej zadań. Nie bez znaczenia pozostają zasady naboru nowych pracowników. Tego typu informacje są pozyskiwane w całkowicie legalny sposób, ponieważ pochodzą ze źródeł powszechnie dostępnych, a nawet dostarczanych bezpośrednio do potencjalnego klienta. Inna metoda poszukiwania danych, która jest bardziej ryzykowana, to przeszukiwanie śmieci, których pozbywa się ofiara ataku. Może się także zdarzyć, że pewne aktualne dokumenty lub elektroniczne nośniki informacji zostaną umieszczone w koszu. Wynik przypadku lub bezmyślności. Firma Fellows przeszukała 614 worków na śmieci, wyrzucane przez pracowników. W jednej trzeciej z nich znaleziono 544 dokumenty zawierające informacje istotne z punktu widzenia przedsiębiorstwa. Były to dane o partnerach biznesowych, pracownikach i klientach. Natomiast w 2001 r. pracownicy Procter & Gamble znaleźli w kontenerach na śmieci konkurencyjnego Unilever trzyletni plan marketingowy sprzedaży szamponów w USA[3]. Wszystkie przedstawione okoliczności są wykorzystywane przez socjotechnika, który na tym etapie może realizować swoje zadanie, zazwyczaj nie wchodząc w konflikt z prawem[4].

Jeśli zdobyta informacja nie jest bezpośrednim celem, a jedynie środkiem, socjotechnik powtarza cykl od stosownego etapu. To, do którego ogniwa się cofnie, będzie zależało między innymi od źródła informacji. Jeśli uzna, że trzeba szukać zupełnie w innym miejscu niż dotychczas, cykl może rozpocząć od pierwszego kroku. Jeśli wybrana technika pozwoli mu na stałą interakcję z jedną ofiarą, kluczowe okażą się etapy pogłębiania zaufania i wykorzystywania go.

Techniki manipulacji

Robert B. Cialdini w artykule zamieszczonym w „Scientific American" (luty 2001) przedstawia pięć „podstawowych cech ludzkiej na-

[3] Dane za: K. Garski, A. Szymborska-Sutton, *Szpieg w firmie*, „Manager Magazine" marzec 2006.

[4] Unilever domagał się 20 mln dol. odszkodowania. Otrzymał połowę.

tury”[5]. Zalicza do nich także pewne priorytety i wartości. Katalog ten można rozszerzyć o dodatkowe elementy, stanowiące łącznie fundament, na którym w pierwszej kolejności opiera się socjotechnik, planując atak.

a) AUTORYTET*

Posiadanie autorytetu często wiąże się z piastowaniem wysokiego stanowiska w danej firmie. Personel bez większego zastanowienia podporządkowuje się poleceniom prominentnej osoby. Ludzie wykazują się w takim wypadku następującym schematem postępowania. Przede wszystkim dochodzą do wniosku, że rozpatrywanie merytorycznego aspektu prośby nie ma sensu. Skoro jest ona pomysłem osoby, której w jakiś sposób się podlega, ryzyko związane z przykrymi konsekwencjami jej realizacji wydaje się niewielkie. Wpływ na odruchowe działanie ma także obawa przed posądzeniem o niesubordynację. Z drugiej strony pracownik oczekuje, że natychmiastowa reakcja na prośbę przełożonego zostanie przez niego zapamiętana i doceniona. Dodatkowo do działania motywuje ewentualny szacunek, żywiony względem osoby posiadającej władzę w jakiejkolwiek postaci.

Socjotechnik, wykorzystując przedstawiony sposób rozumowania, może zasugerować ofierze, że jest pracownikiem zarządu firmy. W tym wypadku nie będzie nawet konieczne zgromadzenie dużej ilości pomocniczych informacji dotyczących struktury przedsiębiorstwa. Wystarczy, jeśli oszust po prostu poda się za prominentną osobę. Celami podobnego ataku są osoby o niskiej pozycji w hierarchii firmy. Jeśli są początkującymi pracownikami, jest bardziej prawdopodobne, że będą postępować instynktownie niż rozsądnie. Już samo wymienienie nazwiska szefa może podziałać paraliżująco, co nie dopuści do pracownika myśli o możliwości ewentualnego oszustwa.

Informacje są chętnie udzielane także osobom przedstawiającym się jako dziennikarze. Świadczą o tym przypadki ujawnionych ataków. Ofiara jest kuszona pozytywnym artykułem na temat firmy, co na

[5] Elementy oznaczone gwiazdką zostały wyróżnione przez Roberta B. Cialdiniego.

pewno zostanie docenione przez przełożonego. Bywa, że przedstawia się jej pytania niezbędne do weryfikacji oszczerczych informacji, jakie rzekomo rozpowszechnia konkurencja. W przypadku szeroko pojętych mediów decydujące znaczenie ma wpływ, jaki mogą wywrzeć na potencjalnych klientów. Jest to specyficzny rodzaj władzy, na której opiera się socjotechnik, podając się za dziennikarza.

b) SYMPATIA*

O wiele chętniej udzielamy pomocy osobom, z którymi nas coś łączy niż nieznajomym. Teoretycznie banał, ale okazuje się, że wystarczy zbudować jakąkolwiek więź opartą na sympatii, by móc wydobyć potrzebną informację. Niejednokrotnie jest to przełamanie formalnego stylu rozmowy, obowiązującego w danej firmie. To powoduje, że wydajemy się rozmówcy osobą bezpośrednią, co nierzadko łączone jest z domniemaniem uczciwości.

Najprostszą metodą stosowaną przez socjotechnika będzie przekonanie rozmówcy, że mają ze sobą coś wspólnego. Nie trzeba wyszukiwać drobiazgowych informacji na jego temat. Czasami wystarczy znajomość stanowiska, na którym pracuje, branża, przypadkowa zbieżność gustów (niejednokrotnie determinowana przez dwa pierwsze wyznaczniki). Ponieważ ufamy osobom do nas podobnym, socjotechnik po kilku zdaniach będzie próbował także naśladować ton głosu rozmówcy, spróbuje podobnie formować zdania. Wszystko w celu wywołania iluzji zażyłości.

c) WZAJEMNOŚĆ*

Skorzystanie z czyjejś pomocy zazwyczaj budzi chęć odwzajemnienia się. Gotowość do wyświadczenia przysługi jest tym większa, im mniej wymaga wysiłku. Dodatkowy bodziec do działania stanowi duża dysproporcja pomiędzy otrzymaną pomocą a tą, o którą jest się proszonym.

Oczekiwanie na zaistnienie powyższej wzajemności nie wydaje się efektywną metodą. Socjotechnik sam inicjuje sytuację, w której będzie

się mógł wykazać uczynnością. Swoisty instynkt wzajemności jest najłatwiej wykorzystywany przez oszustów łączących metody socjotechniczne z technologią. Wszelkie uszkodzenia w obrębie sieci niezbędnej dla działania komputerów w danej firmie paraliżują większość pracowników. Obawiają się, że nie będą w stanie poradzić sobie samodzielnie z usterkami, które spowolnią ich pracę lub też całkowicie zniweczą jej dotychczasowe efekty. Wykorzystując wiedzę (niekiedy jedynie terminologię) technologiczną, atakujący sugeruje, że jest w trakcie zapobiegania biurowej tragedii. Laik nie będzie w stanie rzeczowo zweryfikować tego, co usłyszy. Będzie natomiast w stanie zrobić wiele, by odwdzięczyć się za fikcyjną pomoc. Dalej pozyskiwanie informacji odbędzie się ponownie z wykorzystaniem technologii. Pracownik zostanie nakłoniony na przykład do zainstalowania jednego z programów, który umożliwi atakującemu stały dostęp do źródła potrzebnych danych.

d) KONSEKWENCJA*

Złożenie publicznie obietnicy wytwarza przymus jej spełnienia. Ludzie, nie chcąc uchodzić za niesłownych, będą postępować zgodnie z poczynionymi deklaracjami. Taka konsekwencja ma potwierdzać, że są osobami godnymi zaufania i świadomymi tego, do czego się zobowiązują.

Socjotechnik wykorzystuje tę skłonność, wyznaczając pracownikowi wykonanie danej czynności służbowej lub nakłaniając do podporządkowania się obowiązującym procedurom. Atakujący wyda mu szereg poleceń, które są przedstawiane jako kolejne etapy zleconego zadania. Pracownik będzie czuł się zobligowany do ich wykonania ze względu na wyrażoną uprzednio zgodę. Tą drogą napastnik może uzyskać swobodny dostęp do haseł zabezpieczających dostęp do systemów komputerowych firmy. Wystarczy poinformować pracownika o konieczności odbycia szkolenia w ramach bezpieczeństwa w miejscu pracy. Następnie pouczyć go, w jaki sposób owe hasła należy zabezpieczać. Socjotechnik poprosi o wprowadzenie nowego hasła i zakaże ofierze podania go. Nie stanowi to żadnego problemu dla przeprowadzającego atak. Zainstalował wcześniej, nierzadko z pomocą ofiary, program odczytujący kom-

binację użytych klawiszy. Poprzez realizację poszczególnych punktów polityki bezpieczeństwa (wyznaczanych w tym wypadku przez oszusta) pracownik potwierdza uprzednio wyrażoną chęć, by odbyć wspomniane szkolenie.

e) PRZYZWOLENIE SPOŁECZNE*

Ludzie często bez zastanowienia wykonują pewne czynności tylko dlatego, że zrobił to ktoś inny z ich otoczenia. Powielają zachowania, bo ich powszechność wydaje się świadczyć o celowości działania. Podświadomie oceniają je dodatnio, nawet jeśli nie mają żadnych informacji o jego skutkach.

Ta skłonność również jest często wykorzystywana przez socjotechników. Mogą oni próbować pozyskać potrzebne informacje, wcielając się w postać ankietera. Ofiara usłyszy kilka nazwisk osób znanych jej osobiście, mogą to być współpracownicy, którzy rzekomo już odpowiedzieli na identyczne pytania. Przekonanie o społecznej aprobacie tego pomysłu każe pracownikowi współpracować z ankieterem.

Dodatkowo istnieje małe prawdopodobieństwo próby weryfikacji tożsamości ankietera. Ludzie wychodzą z założenia, że gdyby mieli do czynienia z oszustem, ktoś wcześniej na pewno już by to wykrył i ostrzegł pozostałych.

f) LENISTWO

Każdy chętnie da się wyręczyć z realizacji części swoich obowiązków. Zwłaszcza gdy pojawią się one nieoczekiwanie. Nawet jeśli pracownik potrafi wykonać daną czynność samodzielnie, raczej nie zawaha się skorzystać z oferowanej pomocy.

Lenistwo usypia czujność niezbyt sumiennych pracowników, ułatwiając zadanie socjotechnikowi. Podszywając się pod osobę, której obiecuje wyręczenie z obowiązków, ma szansę otrzymać to, do czego była ona uprawniona. Niechęć do dodawania sobie pracy przejawia się także w rzadkiej weryfikacji tożsamości osoby, z którą się rozmawia. Wygodniej jest założyć, wbrew wytycznym polityki bezpieczeństwa, że ataki socjotechniczne nie zdarzają się zbyt często.

g) SOLIDARNOŚĆ Z OSOBAMI, Z KTÓRYMI ŁĄCZY DĄŻENIE DO WSPÓLNEGO CELU

W niektórych firmach kładzie się nacisk na udzielanie pomocy nowym pracownikom. Odgórne wytyczne nie zawsze są potrzebne. Doświadczone osoby wspominają swoje pierwsze dni w firmie. Socjotechnik może zasugerować, że ma problemy wynikające z konieczności zaaklimatyzowania się w nowym miejscu. Ponieważ każdy był kiedyś początkującym pracownikiem, z łatwością przypomni sobie siebie w podobnej sytuacji. Socjotechnik buduje więź ze swoją ofiarą w oparciu o jej własne doświadczenia. Tego typu relacja może również wzbudzić pewnego rodzaju sympatię. Stworzy to możliwość późniejszej wymiany doświadczeń, dyskusji o wspólnych problemach. Oszukany w ten sposób pracownik stanowi źródło informacji, do którego można wielokrotnie powracać, bez wzbudzania podejrzeń. Udawanie nowego pracownika zmniejsza więc ryzyko wykrycia ataku. Wszelkie niedostatki wiedzy czy też znajomości wewnętrznej etykiety biura raczej nie wzbudzą podejrzeń. Prawdopodobnie zostaną odebrane jako brak doświadczenia lub objaw zdenerwowania.

h) NIECHĘĆ DO PONOSZENIA ODPOWIEDZIALNOŚCI

Ludzie mają skłonność do unikania odpowiedzialności za czynności, które mogą doprowadzić do nieprzyjemnych reperkusji. Szukają kogoś, kto w razie ewentualnego niepowodzenia, poniesie konsekwencje podjętych działań. Wolą czasami w ogóle nie podejmować prób rozwiązania problemu samodzielnie. Czekają, aż ktoś zaoferuje im pomoc. Ta cecha ujawnia się w przypadkach, gdy niedostatki wiedzy w danej dziedzinie są tak duże, że na pewno wpłynęłyby niekorzystnie na obrót sytuacji. Można zaobserwować, że owa specyficzna bezradność cechuje częściej osoby zajmujące w firmie niższe stanowiska. Strach przed poniesieniem konsekwencji za błąd w działaniu jest powodowany obawą o utratę posady.

Socjotechnik szybko może się zorientować, które obowiązki służbowe są realizowane przez ofiarę z trudem. Orientacja w strukturze organizacyjnej firmy pozwoli na wybór rozmówcy z odpowiednie-

go działu. Selekcji dokona tak, by wzrosło prawdopodobieństwo, że pracownik nie będzie potrafił samodzielnie na przykład dokonać zestawień finansowych. Socjotechnik najpierw poprosi o wykonanie dla niego którejś z takich czynności. Następnie poinformuje, że zna sposób, jak mógłby sam zrealizować to zadanie. Potrzebuje jednak kilku informacji, których może udzielić pracownik. Powyższa skłonność sprzyja zamiarom socjotechnika, który działa, używając metod technologicznych. Nieświadoma ofiara, nieumiejąca poruszać się bezpiecznie po wirtualnej przestrzeni, może ułatwić atakującemu dostęp do wewnętrznego systemu komputerowego firmy, zainstalować programy niszczące ten system, a także podać hasła, z których znaczenia nie zdaje sobie sprawy.

i) SOCJOTECHNIKA W WYWIADZIE KONKURENCYJNYM

Socjotechnika jest powszechnie stosowaną metodą w ramach wywiadu konkurencyjnego (Competitive Intelligence, CI). Polega on na legalnym zdobywaniu zastrzeżonych informacji o konkurentach, partnerach handlowych i rynku. W Polsce znany jest także jako „wywiad gospodarczy". Jego praktyczne zastosowanie, w porównaniu ze Stanami Zjednoczonymi czy zachodem Europy, jest jednak znikome.

Wywiad konkurencyjny poprzedza kampanie reklamowe bądź kampanie PR. Daje możliwość znacznych oszczędności w przypadku znajomości planów konkurencji. Poza tym pozwala zweryfikować krążące w danym środowisku plotki i pogłoski, od których prawdziwości zależą posunięcia danego przedsiębiorcy. Ułatwia pomnożenie kapitału, gdy wiadomo, gdzie można go pewnie ulokować. O opłacalności stosowania wywiadu konkurencyjnego mogą świadczyć fundusze weń inwestowane przez amerykańskie korporacje. Wciąż rośnie liczba firm wysyłających pracowników na szkolenia do tzw. *Centers for Operational Business Intelligence*. Zajęcia są prowadzone przez byłych szpiegów amerykańskiego wywiadu i innych pracowników CIA. Uczestnicy uczą się, jak wydobywać interesujące ich informacje i jak skłonić partnera w czasie negocjacji, by ujawnił wartościowe dane.

Praktyki stosowane przez wywiadowców są zgodne z prawem, ale nie zawsze można je nazwać etycznymi. Umiejętność manipulacji, będąca domeną socjotechniki, jest wręcz nieodzowna.

Przydatna jest także znajomość specyficznego języka danej branży. Warto poznać organizację i powiązania charakteryzujące konkretny segment rynku. Szczególne znaczenie ma więc dobre przygotowanie pod względem merytorycznym. Z tego względu w celach wywiadowczych angażowane są firmy, specjalizujące się w takich usługach. Jedną z nich jest *AWARE*[6].

Cel działalności wyjaśnia jej slogan: „wywiad gospodarczy dla sukcesu w biznesie. Na stronie internetowej można przeczytać, że firma jest angażowana w liczne przedsięwzięcia, mające na celu pozyskiwanie informacji o różnych organizacjach. Skompletowany wywiad pozwala klientom na strategiczne i taktyczne podejmowanie decyzji[7]".

CASE STUDIES[8]

Prezentowane poniżej sytuacje to modelowe zastosowanie wywiadu konkurencyjnego. W celu pozyskania informacji przeprowadzono atak socjotechniczny.

1) Planowanie kampanii reklamowej

OPIS SYTUACJI

W ogólnie dostępnych źródłach informacji podano, że pewna firma wprowadzi niebawem na rynek nowy produkt. Konkurencyjne przedsiębiorstwo również pracuje nad podobną ofertą, skierowaną do tej samej grupy klientów.

---

[6] www.marketing-intelligence.co.uk.

[7] Tekst jest tłumaczeniem oferty AWARE z www.marketing-intelligence.co.uk.

[8] Opisy sytuacji (*case studies*) 1, 2 za: www.marketing-intelligence.co.uk.

POTRZEBNA INFORMACJA

Właściciel konkurencyjnej firmy chce poznać dokładną datę wprowadzenia produktu do sprzedaży. Pozwoli mu to lepiej zaplanować kampanię reklamową oraz ograniczyć koszty. Nie dojdzie do strat, które spowodowałoby wejście na rynek po konkurencyjnej firmie.

SPOSÓB UZYSKANIA INFORMACJI

Etap I

Wykonano telefon do działu PR, podając się za dziennikarza. Skierowano do firmy ofertę reklamową w zamian za sponsoring kilku okazjonalnych imprez. Zaproponowano kilka terminów, każdy związany z innym, odległym w czasie, wydarzeniem (np. Dzień Dziecka, Dzień Matki, Boże Narodzenie). Uwzględniono przy tym profil firmy. Można dokonać następującego założenia. Firmie będzie zależało na utrwaleniu się w świadomości potencjalnego klienta na niedługo przed wprowadzeniem nowości na rynek. Wybór konkretnej imprezy pozwoli zawęzić ramy czasowe do konkretnego miesiąca.

Etap II

Wykonano telefon do agencji reklamowej pracującej dla konkurencyjnej firmy. Podano się za jej pracownika. Poproszono o przysłanie materiałów promocyjnych, np. przed lub po 24 grudnia. Badamy reakcję. Przy sprzyjającym szczęściu, pracownik agencji, zdziwiony decyzją „zleceniodawcy", wymieni prawdziwą datę wprowadzenia produktu do sprzedaży. Możliwe są następujące reakcje: a) Jak to przed 24? Nie zdążymy! Przecież towar w sklepach ma być od 20 stycznia, skąd ten pośpiech?! b) Po 24? To chyba jakaś pomyłka?! Przecież chcieliście, żeby kupowano wasz produkt pod choinkę… nie rozumiem. Na pewno chodzi o 24 grudnia?

KOMENTARZ

W pierwszym etapie ataku wykorzystano przychylność ludzi względem potencjału informacyjnego, jakim dysponują media. Często zdarza się, że tożsamość osoby przedstawiającej się jako dziennikarz w ogóle nie

jest weryfikowana. Działa tutaj podświadoma chęć ofiary, by nadano jej działalności zawodowej rozgłos. Oferta zaproponowana przez fikcyjnego dziennikarza również jest kusząca. Socjotechnik przed przystąpieniem do ataku zdobył dane na temat profilu firmy. Dzięki temu był w stanie wybrać te imprezy, które z chęcią zostałyby zasponsorowane. Warto także zwrócić uwagę na ofiarę ataku. Zazwyczaj w takich przypadkach będzie to osoba o stosunkowo niskiej pozycji zawodowej. Może to być np. student odbywający praktyki. Myśl o zorganizowaniu dla firmy tego typu promocji i uznanie zwierzchnika będą w stanie uśpić czujność. W następnym etapie socjotechnik kontaktuje się z firmą świadczącą usługi na rzecz innego przedsiębiorstwa. Sprostanie wymaganiom klienta determinuje jej powodzenie. Gdy praca odbywa się w wielkim napięciu i szybkim tempie, już samo wymienienie nazwy klienta może stawiać wszystkich w stan gotowości. W konsekwencji tożsamość dzwoniącej osoby nie zostanie zweryfikowana. Na korzyść atakującego działa także fakt, że sprawia on wrażenie obeznanego w sytuacji klienta. Mówi przecież o produkcie, nad którego promocją trwają prace, co odsuwa podejrzenia. Trzeźwa ocena sytuacji i sprawdzenie, z kim rzeczywiście ma się do czynienia, ustąpiły w tym przypadku miejsca panice. Zasiał ją fikcyjny klient. Nagle żąda on spełnienia prośby, co w danym stadium pracy agencji reklamowej nie było możliwe lub sprzeczne z początkowymi ustaleniami.

2) Badanie możliwości konkurencji

OPIS SYTUACJI

Właściciel kilku magazynów otrzymał informację, że w danej części kraju jest zapotrzebowanie na nową przestrzeń do składowania. W okolicach znajduje się już jeden magazyn.

POTRZEBNA INFORMACJA

Mężczyzna chce wiedzieć, iloma wolnymi miejscami w magazynie dysponuje konkurent. Taka informacja pozwoli oszacować opłacalność otworzenia własnego magazynu w tamtej okolicy.

SPOSÓB UZYSKANIA INFORMACJI

Wykonano telefon do ochroniarzy pilnujących magazynu konkurenta. Był późny niedzielny wieczór. Dzwoniący przedstawił następującą historię:

„Jak dobrze, że zastałem kogoś o tak późnej porze! Widzę, że też pracujecie w niedzielę za marne pieniądze… Mam wielki problem. Tylko wy możecie mi pomóc! Miałem przywieźć towar dzisiaj wieczorem, ale moja żona miała wypadek. Zająłem się nią, więc nie zdążyłem na czas. Muszę dowieźć towar jutro, żeby się nikt nie zorientował. Od której zaczynają się kolejki? Przyjechałbym o świcie, a potem prosto do żony do szpitala. No chyba że macie wystarczająco wolnych miejsc i nie ma zastojów, to najpierw odwiedzę żonę, a potem przywiozę towar. A konkretnie ile macie wolnych miejsc? Będę wtedy mógł obliczyć, kiedy przyjechać".

KOMENTARZ

Socjotechnik od razu próbuje wzbudzić w rozmówcach sympatię. Osiąga to poprzez wywołanie wrażenia, że w jakiś sposób jest do nich podobny. Zakłada, że stróże nocni to raczej prości ludzie. Ciężko pracują, niewiele zarabiają, żyją w bliskich kontaktach z rodziną. Atakujący przedstawia się jako pracownik zależny od kogoś, kto może go zwolnić za niewykonanie usługi na czas. Jako powód podaje zagrożone życie żony. Ofiary automatycznie wczuwają się w sytuację rozmówcy. Sami oczekiwaliby pomocy, gdyby spotkało ich coś podobnego. I tak jak dzwoniący, nie wahaliby się, czy wybrać pracę, czy też żonę. Właśnie dlatego chętnie udzielają mu wszystkich informacji.

Fakt, że ofiary są ochroniarzami, może świadczyć o tym, że nie mają wiele wspólnego z wewnętrzną działalnością firmy. Nie wiedzą, jak odróżniać informacje poufne od ogólnie dostępnych. Nie potrafią także przewidzieć, co może spowodować odpowiedź na pozornie niewinne pytanie. O tym, w jaki sposób osoba przeprowadzająca atak, może wykorzystać szereg nawet połowicznych danych, powinni dowiedzieć się na specjalnym szkoleniu.

3) Modelowy atak socjotechniczny, przeprowadzony w celu poznania zasad bezpieczeństwa w firmie

OPIS SYTUACJI

W jednej z firm pojawił się „przedstawiciel amerykańskiej korporacji". Twierdzi, że przyszedł w celu nawiązania współpracy. Potrzebuje informacji, które nie powinny być udzielane osobom bez upoważnienia.

POTRZEBNA INFORMACJA

Socjotechnik po przedstawionym poniżej wstępie prawdopodobnie uzyska większość informacji, na których pozyskaniu mu zależy. Mogą to być wszelkie dane związane z działalnością firmy i jej pozycją na rynku.

SPOSÓB UZYSKANIA INFORMACJI

Elegancko ubrany mężczyzna przedstawił szefowi jednej z firm cel swojej wizyty:

„Dzień dobry. Jestem przedstawicielem amerykańskiej korporacji, która szuka partnerów w Europie Środkowowschodniej. Przychodzimy tylko do najlepszych. Sami decydujemy, kto jest najlepszy, na podstawie naszych wnikliwych badań i analiz wyników firm. Nie słyszał pan o nas? Hmm… bardzo mi przykro, ale widocznie nie spełniali państwo dotychczas naszych wyśrubowanych wymagań. Nie, ale to nie może być pomyłka. Pańska firma musi być na odpowiednim poziomie, skoro szef mnie tu przysłał. Musiał pan znacznie podnieść poziom działalności firmy. Gratuluję! Pańscy pracownicy brali udział w konferencji organizowanej pod patronatem ambasady amerykańskiej. W swoim wystąpieniu zobowiązali się do poprawiania stosunków z amerykańskimi partnerami. W związku z państwa prośbą – jestem. Muszę panu zadać kilka pytań, skoro wyraził pan chęć współpracy".

KOMENTARZ

Mężczyzna nawet się nie przedstawił. Podał jedynie, czym się zajmuje i w jakim celu przychodzi. Ofierze, zamiast podstawowych informacji, jak imię i nazwisko oraz nazwa firmy, którą reprezentuje mężczyzna,

wystarczy wygląd i sposób mówienia socjotechnika. Na tej podstawie uznano, że jest to szczery i wpływowy potencjalny współpracownik.

Ofiara już na wstępie słyszy, że znalazła się w wąskim gronie wybranych. Przedsiębiorca może być z siebie dumny, bo jego firma spełniła tak wymagające kryteria. Dodatkowo ma pewne poczucie winy, że do tej pory jego przedsiębiorstwo nie prezentowało odpowiednio wysokiego poziomu. Dzięki kolejnym słowom socjotechnika po raz kolejny rozpiera go duma. Wmówiono mu, że to wyłącznie dzięki jego usługom jest teraz w firmie tak dobrze. Trzeba więc skorzystać z tej sytuacji, bo nie wiadomo, jaki obrót przyjmą sprawy za kilka miesięcy.

Następnie atakujący wspomina o jakiejś konferencji, która niedawno się odbyła. Jej tematyka jest luźno związana ze składaną ofertą. Socjotechnik wmawia ofierze, że zostało tam poczynione zobowiązanie. Wiadomo, że profesjonalistom nie wypada wycofywać się ze złożonych, w dodatku publicznie, obietnic.

Dalej zasugerowano, że wizyta mężczyzny jest wynikiem prośby ofiary. Oznacza to, że obecność fikcyjnego przedstawiciela amerykańskiej korporacji jest odpowiedzią na pewne potrzeby właściciela atakowanej firmy. Konieczność uzyskania odpowiedzi na zadane pytania umotywowano współpracą, do której *de facto* nawet nie doszło.

Bibliografia

Augustyniak S., *Ofiary kradzieży tożsamości mówią*, 2003, www.networld.pl.

Belle-Isle D.A., „Social Engineering" 2006.

Cialdini R.B., *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańsk 1999.

Cialdini R.B., Demaine L.J., Sagarin B.J., Barrett D.W., Rhoads K., Winter P.L., *Managing social norms for persuasive impast,* „Social Influence" 2006, vol. 1, s. 3–15.

Garski K., Szymborska-Sutton A., *Szpieg w firmie*, „Manager Magazine" marzec 2006.

Krzyżowska O., Szczepanik R., *Nietypowe przypadki PR*, OnePress.pl.

Martinet B., Marti Y-M., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Warszawa 1999.

Mitnick K., Simon W., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice 2003.

Szczepaniak R., Krzyżowska O., *Nietypowe przypadki public relations*, Gliwice 2003.

Warhole A., *Atak z Internetu*, INTERMEDIA PL, 1999.

Winlker I.S., *Case study of industrial espionage through social engineering*, National Security Association, http://csrc.nist.gov.

Źródła internetowe

www.marketing-intelligence.co.uk

www.onwpress.magazyn.pl

www.computerworld.pl

www.consumer.gov/idtheft

www.informationbuilders.com

Sebastian Bakalarz, Piotr Szlachetka, Grzegorz Grzegorczyk

Podsłuch jako zagrożenie współczesnego świata biznesu

Wprowadzenie

W obecnych czasach straty ponoszone przez firmy w wyniku szpiegostwa są kolosalne. Dzieje się tak, ponieważ konkurencja jest zbyt duża i ci, którzy chcą uzyskać przewagę w interesach, uciekają się coraz częściej do nielegalnych środków. W tym celu powszechniejsze stało się korzystanie z usług detektywów, firm, do których należy zbieranie odpowiednich informacji. Można powiedzieć, że dziś głównym i najbardziej dochodowym zajęciem detektywów jest łapanie szpiegów w firmach. Niewiele osób zdaje sobie bowiem sprawę, że współczesne technologie umożliwiają nieograniczoną ingerencję ze strony intruzów w ich prywatne zasoby. Poufne informacje wyciekają już z około 80% firm. Kradzieże danych to jedna z najbardziej dochodowych branż ówczesnych lat. To, przed czym chcą się uchronić zarówno firmy, jak i osoby fizyczne, to szpiegostwo gospodarcze i podsłuchy umieszczane w najbardziej strategicznych punktach.

Celem niniejszej publikacji jest próba charakterystyki problemu, jakim jest podsłuch. Chcielibyśmy opisać metody, czyli jak i gdzie takie podsłuchy można instalować, następnie przedstawić, jakie płyną z tego powodu zagrożenia, i wreszcie, jak możemy sprawdzić, czy nie jesteśmy podsłuchiwani, i jak możemy zabezpieczyć się przed podsłuchem.

Podsłuch był jednym z najefektywniejszych narzędzi pracy szpiegów od najdawniejszych czasów. Wtedy jednak wystarczyło dobre ucho przystawione do ściany bądź drzwi. Te, można by rzec, profesjonalne podsłuchy zaczęły funkcjonować i sprawdzać się w okresie I wojny

światowej. Nasłuchiwano wówczas za ich pomocą linie radiowo-telegraficzne. Natomiast II wojna światowa to już prawdziwy przełom w tej dziedzinie, mikrofon i nadajnik bowiem musiały stawać się coraz mniejsze i skuteczniejsze.

Współcześnie podsłuchy wykorzystywane są m.in. przez pracodawców, którzy chcą sprawdzić, co robią ich podwładni. Korzystają z agencji detektywistycznych, a także z pracy wywiadów i osób zajmujących się szpiegostwem gospodarczym. O technicznych możliwościach podsłuchów będzie w dalszej części opracowania.

Wiele firm nie zdaje sobie sprawy, w jak dużym stopniu wywiad przemysłowy może wpływać niekorzystnie na wyniki ich działalności gospodarczej. Mogą one przykładowo kontrolować tajemnice firmowe, dotyczące m.in. wprowadzania nowych planów reorganizacyjnych, nowych produktów sprzedaży czy też problemów prawnych przedsiębiorstwa. Nie ulega wątpliwości, że do najcenniejszych dóbr firmy należy informacja. Musimy ją zabezpieczyć, by nie dostała się w ręce intruza.

Powinniśmy zdawać sobie sprawę, jak istotne jest zabezpieczenie się przed działaniami, które tego bezpieczeństwa chcą nas pozbawić. Oczywiście mowa tu o uchronieniu się przed podsłuchem. Chociaż stuprocentowe bezpieczeństwo nie istnieje, należy dążyć do jego optymalnego stanu. Trzeba w tym celu opracować strategię, często ją modyfikować i myśleć o wdrażaniu coraz to nowszych systemów zabezpieczających przed podsłuchami. W dobie miniaturyzacji bowiem założenie podsłuchu nie wymaga ani dużych nakładów, ani specjalistycznych umiejętności. Żeby ustrzec się przed szpiegostwem przemysłowym i wyciekiem informacji, musimy pamiętać, że należy chronić takie dobra, jak tajemnice handlowe i bezpieczeństwo pracowników.

Oto przykład, jak należy zabezpieczać pomieszczenia, sale obrad, biura przed utratą informacji. Jest to jednak procedura antypodsłuchowa, służąca jednorazowemu wykorzystaniu. Jej etapy przedstawiają się następująco. Najpierw należy przeprowadzić elektroniczną kontrolę antypodsłuchową pomieszczenia. Następnie trzeba sprawdzić i zamknąć badaną salę. Później postawić przed pomieszczeniem pracowników

ochrony sprawdzonych wcześniej na poligrafie. Musimy przygotować w ten sposób kilka innych pomieszczeń i przed samym spotkaniem wylosować jedną z wcześniej sprawdzonych sal. W czasie już trwających obrad należy pamiętać, by takie spotkanie zabezpieczać fizycznie.

Współczesne podsłuchy są tak miniaturowe, że trudno je zauważyć, a nadajniki wyposażone są w długo działające baterie. Urządzenia, które możemy kupić w sklepach, na bazarach czy w Internecie są maskowane jako kontakty, kalkulatory czy elementy wyposażenia biurowego. Składają się one z nadajnika i odbiornika, który przekazuje sygnał nawet z odległości kilku kilometrów.

Niektóre bogate firmy w trosce o tajność swoich informacji decydują się na sposoby ogólnie niedostępne, a przy tym niebagatelnie drogie. Do takich sposobów możemy zaliczyć m.in. programy chroniące przed ulotem elektromagnetycznym. Są to specjalnie przygotowane i fizycznie zabezpieczone przed emisją komputery. Plusem takiego rozwiązania jest to, że w takim przypadku nie będą nam już potrzebne inne środki bezpieczeństwa. Natomiast użytkowanie takiego systemu obowiązującego w Stanach Zjednoczonych podlega ścisłej kontroli Narodowej Agencji Bezpieczeństwa USA.

Inna metoda pozwala na tłumienie sygnałów za pomocą ekranów skonstruowanych na bazie folii aluminiowych. Nie pozwalają one na wydostanie się emisji na zewnątrz pomieszczenia. Ale należy wtedy pamiętać o odpowiednim zabezpieczeniu okien i drzwi. Gdybyśmy pominęli takie zabezpieczenie, moglibyśmy zniweczyć efekt ekranowania ścian. Jeśli zależy nam na jak najlepszym zabezpieczeniu niewielkiej ilości sprzętu komputerowego, to powinniśmy zastosować kabiny elektromagnetyczne. Mają one bowiem bardzo dużą siłę tłumienia. Ale czasem tańsze środki mogą okazać się skuteczniejsze. Chcielibyśmy opisać kilka spośród bardzo dużej liczby podsłuchów oferowanych w sprzedaży internetowej, które są ostatnio popularne. Są to urządzenia używane do podsłuchiwania oraz zabezpieczania przed podsłuchiwaniem. Szpieg może umieścić swoje podsłuchy praktycznie w każdym miejscu.

Na przykład urządzenie o nazwie KeyKatcher to mały podsłuch, który montuje się pomiędzy wtyczkę klawiatury a komputer. Nie wy-

maga ono dodatkowego oprogramowania ani zasilania. Zapisuje w wewnętrznej pamięci każdy znak wpisany do komputera przez klawiaturę. Odczyt następuje poprzez wpisanie odpowiedniego hasła. Po wpisaniu hasła pojawia się menu, w którym można odczytać dane. Urządzenie pozwala zapisać nawet do 30 000 znaków. Jest ono łatwe i szybkie w montażu. Może być swobodnie przenoszone pomiędzy komputerami. Praktycznie nie do wykrycia przez użytkownika.

Innym zestawem podsłuchowym jest zestaw SPY-5. Wyłapuje on z powodzeniem każdy szmer, wypowiedziane słowa nawet w większych pomieszczeniach. Dźwięk przez niego pobierany jest klarowny i czysty. Pluskwa posiada stabilizację częstotliwości. Powoduje to, że urządzenie posiada pełną stabilność, nawet podczas przenoszenia. Zasięg takiego podsłuchu to nawet 400 metrów. W terenie zabudowanym jest troszkę bardziej ograniczony.

Z naszego punktu widzenia ważniejsze będą raczej systemy antypodsłuchowe, które cieszą się zainteresowaniem nie tylko osób fizycznych, które chcą sprawdzić, czy nie są podsłuchiwane, ale coraz częściej średnich firm, które nie chcą, by ich informacje dostały się w niepowołane ręce. Najczęściej stosowane są wszelkiego rodzaju zagłuszacze dyktafonów i nadajników podsłuchowych. Są też takie, które zabezpieczają szybko i skutecznie określone powierzchnie przed wyciekiem informacji. Coraz bardziej powszechne stały się też blokatory telefonów komórkowych.

Do tych pierwszych zaliczyć możemy takie systemy jak: Generator Białego Szumu „WNG-023”, Generator Harmoniczny Mowy SZAMAN, czy też Generator Harmoniczny Mowy SZAKAL. Wszystkie trzy służą do zagłuszania dyktafonów i nadajników podsłuchujących. Ich działanie jest podobne. Ich głównym zadaniem jest całkowite zatkanie mikrofonów we wszystkich urządzeniach nagrywających i transmitujących informacje. Różnią się one zasilaniem i powierzchnią chronioną, która dochodzi nawet do stu metrów sześciennych. Efektywnie działają także takie urządzenia, jak: Vibro Akustyczny Generator Szumu „FORUM” i Analizator AW-1000.

Zasada działania systemu FORUM polega na wprowadzaniu wibracji w ścianach poprzez zamontowane w nich specjalnych urządzeń, których moc generowanych drgań wynosi 10 W. System FORUM zabezpiecza pomieszczenia przed stosowaniem mikrofonów laserowych, kierunkowych i kontaktowych. Natomiast Analizator AW-1000 pozwala na szybkie i skuteczne sprawdzenie pomieszczeń, linii elektrycznych, linii telefonicznych i wszelkiego innego okablowania pod kątem istnienia aktywnych źródeł promieniowania elektrycznego.

Ostatnio bardzo popularne stało się zakładanie podsłuchów w telefonach komórkowych. Pozostawiony podczas narady czy też innego poufnego spotkania aktywny telefon, w którym bardzo szybko i sprawnie można zainstalować podsłuch, może przekazać treść rozmów osobom niepowołanym. W tym celu stworzono szereg urządzeń antypodsłuchowych, które blokują i neutralizują takie podsłuchy. Należy do nich Paralizator i Neutralizator Działania Telefonii Komórkowej CTN-100. Urządzenie to sprawia, że telefony są całkowicie niezdolne do transmitowania i przyjmowania rozmów. Całkowicie blokuje wszystkie telefony komórkowe w określonym promieniu ich działania. Można go umieścić praktycznie wszędzie, np. w walizce, zakamuflować wewnątrz zwykłego odbiornika radiowego lub telewizyjnego.

Pokrótce postaramy się opisać też zagrożenia związane z telefonią internetową i słynnym ostatnio programem Echelon.

Telefonia internetowa jest nam znana stosunkowo od niedawna. VoIP (Voice over Internet Protocol) to technologia zapewniająca przesyłanie dźwięku za pomocą łączy internetowych. Pozwala to wykonywać połączenia głosowe przez bramkę internetową lub komunikatory na numery stacjonarne, komórkowe, a nawet na telefony satelitarne. Jest to tzw. telefonia internetowa. Ten sposób komunikacji głosowej na początku przeżywał duże trudności. Aby jakość rozmowy była idealna, musi być odpowiedni zakres przesyłania danych w sieci. W przypadku zbyt wolnego połączenia dźwięk jest zniekształcony, a słowa mogą dochodzić z dużym opóźnieniem, co uniemożliwia płynną konwersację.

W tej pracy chcieliśmy przybliżyć tę problematykę, gdyż jest ona dość nowa. Większość z nas nie uświadamia sobie zagrożeń płynących

z podsłuchu telefonii stacjonarnej. Te połączenia wydają się nam dlatego bezpieczne, bo literatura o nich nie wspomina.

Telefonia Internetowa (IP) zdobyła sobie tak wielką popularność, ponieważ połączenia te są dużo tańsze, a nawet bezpłatne. Najbardziej znanymi komunikatorami tego typu są GlobalPhone, Skype, Tlen, Gadu-Gadu, NetPhone. Wymagają one szybkości łącza minimum 54kb/s, co jest obecnie standardem.

Oprócz użytkowników prywatnych zaletę bezpłatności telefonii IP wykorzystują coraz częściej firmy. Wiadomo, jak cenna dla konkurencji może być zwykła rozmowa pracowników, którzy mogą się komunikować przez komunikatory internetowe nawet będąc w jednym pomieszczeniu. Trzeba również zauważyć, że dla firm telefonia ta zapewnia magazynowanie danych w systemach bilingowych, zawierających wykazy klientów i poczty głosowe. Firmowe centrale IP potrafią również zawierać informacje dotyczące czasu, długości, a nawet przebiegu rozmowy. Dla pracodawcy informacje te są wyznacznikiem wydajności pracownika, a dla konkurencji jest to możliwość znalezienia słabych punktów firmy i wyciek technologii. Tak ścisłe powiązanie systemu telefonicznego z przepływem informacji w firmie sprawia, że jego ochrona jest bardzo istotna.

Telefonia IP jest niebezpieczna z tego względu, że wysyłanie danych następuje przez publiczne serwery. By nasłuchiwać, nie trzeba wyrafinowanych urządzeń, które opisaliśmy wyżej. W przypadku telefonii internetowej wystarczy mieć przeciętny komputer z dostępem do Internetu. Jednym ze sposobów takiego podsłuchu jest nasłuchiwanie sygnału przekazywanego z przekaźnika transmisyjnego. Jest to metoda bardzo pożądana, gdyż w mniejszym stopniu narażona na wykrycie. Oprócz działań typowo inwigilacyjnych hakerzy mogą również zagłuszać transmisję, a nawet zalogować się jako dany użytkownik.

Najskuteczniejszym sposobem walki z podsłuchem w Internecie jest szyfrowanie transmisji głosu. Należy w tym miejscu podkreślić, że telefonia stacjonarna nie posiada takiej opcji. Dodatkowym zabezpieczeniem jest autoryzacja rozmówcy. Następuje ona poprzez wprowadzenie kodu dostępu lub karty z kluczem, a nawet autoryzacji samego urządzenia, z którego korzystamy. Jest to o tyle konieczne, gdyż obecny rozwój

techniki pozwala na podpięcie aparatu IP do Internetu w dowolnym miejscu na świecie. Po autoryzacji rozmówcy rozmowy będą kierowane do tego urządzenia.

Telefonia internetowa jest uważana za zagrożenie dla bezpieczeństwa państwa, gdyż nie daje się łatwo kontrolować, a przy zastosowaniu tzw. silnej kryptografii rozmowy są także niemożliwe do podsłuchiwania. W najbliższej przyszłości podejmowane będą próby ograniczenia swobody tworzenia sieci IP.

Na końcu postaramy się przybliżyć funkcjonowanie systemu Echelon. Od dłuższego czasu w Internecie pojawiały się informacje o tym, jakoby służby specjalne USA kontrolowały przepływ informacji w Internecie. Kontrola ta miałaby polegać na wykrywaniu w sieci słów kluczy, takich jak: „bomba", „narkotyki", „terroryzm". Wcześniej te pogłoski traktowano jak opowieść SF, jednak obecnie nie ma już wątpliwości co do tego, że system Echelon istnieje naprawdę.

Pierwsze informacje dotyczące projektu Echelon pojawiły się w mediach w II połowie 1988 r., kiedy to Angielka pracująca w amerykańskiej bazie Menwith Hill w hrabstwie Yorkshire zeznawała na Kongresie w sprawie nadużyć tajnych amerykańskich służb wywiadowczych. Wyszło wtedy na jaw monitorowanie rozmów telefonicznych amerykańskiego senatora, co było pogwałceniem prawa amerykańskiego. Przesłuchanie w Kongresie przyciągnęło uwagę brytyjskiego dziennikarza Duncana Cambella, który przeprowadził śledztwo mające na celu wyjaśnienie działalności amerykańskiego wywiadu w Anglii. Odkrył, że początki tego wszystkiego sięgają roku 1947, kiedy to NSA i Brytyjski Wywiad Elektroniczny zawarły porozumienie, tzw. UKUSA, które miało służyć współpracy wywiadowczej. Potem rozszerzono je o agencje wywiadowcze Australii, Nowej Zelandii i Kanady.

Kiedy w latach 70. pojawił się Internet, przedstawiciele służb wywiadowczych tych państw dostrzegli zagrożenia oraz korzyści wynikające z możliwości łatwej wymiany informacji między milionami ludzi na całym świecie. Postanowili stworzyć system, który w przeciwieństwie do klasycznych środków wywiadowczych będzie podsłuchiwał i ana-

lizował hurtowo wszystko to, co się podsłuchać da, i wychwytywał te informacje, które będą przydatne dla celów wywiadowczych.

Pierwsza wersja Echelona analizowała informacje zdobyte przez stacje nasłuchowe przechwytujące dane z satelitów telekomunikacyjnych. Stacje te znajdowały się w Morwenstow w Anglii oraz w Yakima w USA. Pod wpływem sukcesu tego systemu postanowiono go zmodernizować i rozbudować. Dodano lepsze i bardziej czułe urządzenia nasłuchowe i nowoczesną bazę komputerową. Echelon rozwija się ciągle, nawet dzisiaj. NSA nie żałuje pieniędzy na taki skuteczny środek wywiadowczy, który przechwytuje i analizuje do 90% danych z połączeń telefonicznych, teleksowych, faksowych i internetowych w ruchu międzynarodowym, a być może w niektórych państwach także w połączeniach krajowych.

Jak wspomnieliśmy wyżej, działanie systemu Echelon opiera się na masowym podsłuchiwaniu dużych ilości transmisji. Jedną z podstawowych metod zdobywania danych do analizy przez Echelon jest przechwytywanie transmisji radiowych. Klasyczny nasłuch radiowy, wykorzystywany w działalności wywiadowczej od przeszło 80 lat, traci obecnie coraz bardziej na znaczeniu z uwagi na stosowanie nowych technik łączności (mikrofale, łączność satelitarna), których podsłuchiwanie wymaga bardziej zaawansowanych środków. Środki te to m.in. specjalne stacje naziemne służące podsłuchiwaniu sygnałów, przesyłanych przez satelity telekomunikacyjne (stacje te często stanowią niemal wierne kopie prawdziwych stacji naziemnych używanych przez systemy łączności satelitarnej, takie jak np. Intelsat). Są również specjalne satelity szpiegowskie, wykonujące zadania niejako odwrotne: przechwytują z kosmosu sygnały emitowane przez naziemne systemy łączności, takie jak np. radiotelefony czy telefony komórkowe. Z uwagi na właściwości tych środków łączności, ich skuteczne podsłuchiwanie na ziemi możliwe jest tylko w stosunkowo ograniczonym obszarze geograficznym, niedaleko od nadajnika. Natomiast odbiór ich sygnałów z kosmosu nie stwarza większego problemu.

Największe zarzuty wobec Echelona wynikają nie z techniki jego działania, a z jej zakresu, ponieważ program ten podsłuchuje wszystko i każdego. Po raz pierwszy Parlament Europejski zainteresował się programem Echelon w 1998 r., kiedy to stwierdzono: „Jeżeli system ten rzeczywiście istnieje, byłby to atak na wolności obywatelskie, konkurencję i bezpieczeństwo państw".

Głównym zadaniem tego programu jest przechwytywanie informacji tekstowych zawartych w faksach, e-mailach, SMS-ach itp. O skali działania systemu może świadczyć raport „Interception Capabilities 2000", w którym stwierdzono, że: „jeden system podsłuchowy może dostarczyć miliona wiadomości w ciągu pół godziny. Z tego miliona filtry pozostawiają jedynie 6500; tylko 1000 spełnia kryteria przekazania do dalszej obróbki; analitycy wybierają dziesięć, z których wytwarzany jest zaledwie jeden raport – takie są typowe statystyki [...]".

Skala działania narusza integralność większości państw, co powoduje liczne protesty. Obecnie w wielu krajach są prowadzone dochodzenia rządowe w sprawie bezprawnego wykorzystywania Echelona przez grupę UKUSA. Jedną z form protestu przeciw istnieniu Echelona jest wyznaczona przez Międzynarodową Społeczność Hakerów na 21 października akcja nazwana „Dniem zakłócania Echelona" (Jam Echelon Day). Hasłem akcji było: „jeżeli rzeczywiście nas podsłuchują, to niech mają co podsłuchiwać". Nawoływano, aby w tym dniu każdy użytkownik Internetu umieszczał w wysyłanych przez siebie e-mailach dużo słów kluczowych, na które przypuszczalnie reaguje Echelon, takich jak np. FBI, CIA, NSA, Irak, MOSSAD, NASA, Clinton, *gun*, *assault*, *bomb*, *drug*, *terrorism*, *revolution*, *special forces* (broń, napad, bomba, narkotyk, terroryzm, rewolucja, oddziały specjalne) itp.

W opracowaniu przedstawiliśmy niebezpieczeństwa, na jakie narażony jest świat biznesu w XXI w. Zainteresowanie problemami biznesu trzeba bowiem rozpatrywać wielotorowo. Praca ta ma na celu uwrażliwienie czytelników na problem etyki w biznesie i zagrożeń, jakie czyhają na nas ze strony konkurencji. Każda inwestycja, która przynosi zysk, staje się obiektem zainteresowań przedsiębiorstw działających na

rynku. Wszak od wartości informacji zależy wysokość środków przeznaczanych na jej zdobycie.

Dzięki tej pracy można szerzej spojrzeć na problem ulotu informacji biznesowych. Mamy nadzieję, że nasze spojrzenie na bezpieczeństwo uchroni czytelników od niemoralnych zachowań w świecie biznesu i zwróci uwagę na wartość informacji. Stuprocentowe bezpieczeństwo nie istnieje. Nie ma też żadnej ogólnej recepty na znalezienie owego optimum bezpieczeństwa. Dlatego tak istotne jest wczesne rozpoznanie zagrożeń, wypracowanie odpowiedniej strategii bezpieczeństwa, a co za tym idzie: budowy optymalnego systemu bezpieczeństwa.

Przestępstwa finansowe

Piotr Migas, Elżbieta Koszel, Sebastian Piekoszowski, Patrycja Fiszer, Marcin Giliciński

Problem napadów na banki w Polsce na tle europejskim

Wstęp

Napady zarówno na instytucje czy osoby świadczące usługi finansowe, jak i na ich klientów są tak samo stare jak pieniądz. Obie strony tej cichej wojny doskonalą metody i strategie swojego działania, by z jednej strony ograniczyć ryzyko napadu, a z drugiej – by był on jak najkrótszy i jak najskuteczniejszy. Wojna, tak jak każdy konflikt o charakterze zbrojnym, wymusza postęp techniczny – niestety u obu stron. Pojawiają się nowe narzędzia, nowe metody, strategie, zarówno napadu, jak i ochrony przed nim. Powstały instytucje zajmujące się profesjonalnym zabezpieczeniem banków i ich klientów, a także profesjonalne gangi przestępców wyposażonych i wyszkolonych, by przechytrzyć tych pierwszych. Celem naszych badań jest przybliżenie tematyki napadów na banki w Polsce w odniesieniu do krajów europejskich, scharakteryzowanie metod działania obu stron „konfliktu" oraz przedstawienie prognoz na przyszłość.

Sytuacja w Polsce zostanie przedstawiona na tle wydarzeń w kilku krajach Unii Europejskiej: Francji, Włoch, Irlandii, Wielkiej Brytanii, oraz państwa neutralnego uważanego za bankowe centrum Europy, czyli Szwajcarii. Przedstawione dane obejmują okres od 1993 do 2004 roku.

Napady, straty i *modus operandi* sprawców

- WŁOCHY

Spośród wybranych krajów europejskich pod względem liczby napadów w czołówce od dawna znajdują się Włochy. Liczba napadów rosła do 1998 roku, w którym osiągnęła pułap 3144 przypadków, po czym

zaczęła powoli spadać. W roku 2004 notowano (po pewnym wzroście) około 2900 napadów. Liczba napadów nieudanych jest wyjątkowo niska – nigdy nie przekroczyła 200 rocznie. W omawianym okresie średnia roczna zrabowana kwota to około 70 mln dolarów do roku 1997, a następnie około 60 mln euro do dzisiaj.

Sposób działania sprawców: do roku 1995 napadami zajmowali się głównie profesjonaliści napadający albo we dwóch albo całym gangiem, najczęściej w przedpołudniowych godzinach pracy banku. Nie zniechęcała ich ani większa liczba pracowników banku, ani klientów. Rzadko używali maskowania, działali poprzez bezpośrednie zastraszenie kasjera. Czas trwania napadu to w większości przypadków do 3 min. Po roku 1997 obserwuje się bardzo wzmożoną aktywność przestępców amatorów i proporcje odwracają się: do roku 2004 od 60% do 80% napadów dokonali właśnie amatorzy. Niezmienne są godziny napadów, dni tygodnia (poniedziałek i piątek), maskowanie, liczba pracowników i klientów w oddziale, jak i liczba napadających – najczęściej dwie osoby. Włoscy przestępcy używają generalnie broni białej (noże) oraz ciężkich samochodów i pojazdów budowlanych służących do wjeżdżania do oddziałów banków. Bankomaty były najczęściej wysadzane gazem lub materiałami wybuchowymi bądź taranowane. Najczęstszą przyczyną niepowodzenia przestępców, jak się okazuje, jest interwencja pracownika banku – ok. 30% przypadków, interwencja policji − 13%, oraz co ciekawe – inne bliżej nieokreślone przyczyny – również ok. 30%

- FRANCJA

Druga na liście najaktywniejszych krajów pod względem liczby napadów jest Francja. W odróżnieniu od Włoch, od roku 1993 rejestruje się tutaj spadek liczby napadów – od ok. 1300 w roku 1993 do 490 w roku 2004. W latach od 1999 do 2001, tak jak w większości krajów europejskich, zanotowano nieznaczny wzrost napadów. Liczba nieudanych przedsięwzięć przestępczych w tej dziedzinie nie przekroczyła 130 rocznie. Do roku 1997 średnia roczna utrata walorów pieniężnych w wyniku napadu sięgnęła w przybliżeniu 17 mln dolarów, do 2004 około 10 mln euro. *Modus operandi* sprawców napadów: do roku 1996

Francuzi nie stwierdzili, czy banki były rabowane przez amatorów czy profesjonalistów. Spowodowane to mogło być tym, że w ponad 50% przypadków sprawcy byli zamaskowani i działali pojedynczo albo w parach. Po roku 1996 ustalono, że w większości wypadków atakowali profesjonaliści. Najczęściej spotykaną formą napadów było bezpośrednie zastraszenie kasjera w godzinach normalnej pracy oddziału, najczęściej w oddziałach zatrudniających poniżej 7 pracowników. Od tegoż roku zaobserwowano wzmożone zainteresowanie przestępców bankomatami i konwojami przewożącymi gotówkę. Jeśli chodzi o tygodniowy rozkład napadów, to wzmożoną aktywność rejestruje się od wtorku do piątku. Po roku 2000 proporcje, jeśli chodzi o przygotowanie zawodowe napastników, odwracają się – tym razem prawie 80% ataków dokonują amatorzy działający solo lub w parach. Średni czas napadu wynosi do 3 min w 52% oraz 3–10 w 42%. Na znaczeniu zaczyna zyskiwać również pośrednie zastraszenie kasjera oraz dostęp wymuszony jako forma napadu. Należy również wspomnieć, że w 97% sprawcy byli uzbrojeni w broń palną. Ze statystyk wynika, że w 90% przypadków napad nie powiódł się w wyniku interwencji pracownika.

- WIELKA BRYTANIA

W przeciwieństwie do dwóch wyżej omówionych państw w Wielkiej Brytanii średnia liczba napadów w roku w omawianym okresie nie przekracza 300. Od 1993 roku, gdy zarejestrowana liczba napadów wyniosła 693, odnotowuje się spadek działań przestępczych o tym charakterze. Liczba napadów nieudanych lub udaremnionych waha się od 50% do 30% w poszczególnych latach. Średnia roczna kwota zrabowana w Wielkiej Brytanii wynosi ok. 2 mln dolarów do roku 1997 i około 2 mln euro do 2004. Z powodu braku danych nie można stwierdzić, w jakich proporcjach atakowali amatorzy i profesjonaliści, czy byli zamaskowani, czy też nie, jak długo trwały napady oraz jakich metod używali, by wyegzekwować wydanie łupu. Wiadomo tylko tyle, że atakowano najczęściej oddziały w miastach, a liczba obecnych pracowników była zwykle większa niż 7 osób. Sprawcy najczęściej posługiwali się bronią palną, chociaż niekiedy (nawet w 30% wypadków) używali

innych narzędzi, jak strzykawki czy materiały wybuchowe. Należy zauważyć, że od roku 1996 rejestruje się wzrost liczby napadów na bankomaty oraz załogi je obsługujące.

- IRLANDIA

Kolejnym krajem, któremu postanowiliśmy się przyjrzeć, jest Irlandia. Można by było podejrzewać, że w związku z działaniem na terenie tego państwa organizacji terrorystycznej IRA napady na banki powinny być bardzo liczne. Otóż nic bardziej mylnego. Od roku 1993, gdy liczba napadów osiągnęła 123 przypadki, obserwuje się generalnie spadek tej aktywności przestępczej, z niewielkimi wzrostami w poszczególnych latach. Pomimo okresowych wzrostów liczba przypadków nigdy już nie przekroczyła 100. Liczba nieudanych lub udaremnionych napadów waha się od 22 do 7 w poszczególnych latach. Kwoty zrabowane też nie są duże – oczywiście w porównaniu z wyżej wymienionymi krajami – do roku 1997 nie przekraczały 820 tys. dolarów, utrzymując się generalnie na poziomie do 650 tys., a po roku 1997 – do 500 tys. euro, tylko w roku 1998 sięgając kwoty 880 tys. euro. Do roku 1997 sprawcami napadów byli głównie amatorzy atakujący oddziały w miastach. Przy napadach obecnych było więcej niż 7 pracowników banku. Napady generalnie następowały w normalnych godzinach pracy banku, najczęściej od wtorku do piątku. Sprawcy działali najczęściej solo albo w parach, generalnie zamaskowani, napady trwały najczęściej do 3 min. Od tegoż roku zarejestrowano wzmożoną aktywność gangów, jednakże działających amatorsko. Dzienny okres napadów przesunął się z rannych godzin pracy banku na popołudniowe. Od roku 2000 obserwuje się powrót do akcji dwuosobowych. Najczęściej stosowaną metodą jest bezpośrednie zastraszenie kasjera przy użyciu broni białej. Do tegoż roku ataki na bankomaty, ich załogi czy klientów nie występowały lub występowały incydentalnie. Później sytuacja się zmieniła w kierunku coraz częstszych ataków na załogi serwisujące lub zasilające bankomaty oraz zastraszania ich klientów.

- SZWAJCARIA

Szwajcaria uznawana jest za bankowe centrum Europy, więc można by sądzić, że napady na banki zdarzają się tam nader często. Nie jest to prawda. W omawianym okresie liczba dokonanych napadów w roku nie przekroczyła 30, a od roku 2000 obserwuje się ich drastyczny spadek. Napady udaremnione lub nieudane stanowią od 25 do 50% wszystkich wypadków. Pomimo małej liczby napadów straty banków są dość duże – do roku 1997 wyniosły około 2,5 mln dolarów rocznie, a następnie około 2 mln euro. *Modus operandi* sprawców napadów znacznie się różni od występującego w wymienionych już państwach. Napastnicy atakowali najczęściej oddziały znajdujące się poza miastami. Oddziały były napadane w godzinach przed ich otwarciem, w czasie ich pracy i po zamknięciu w równych proporcjach. Liczba pracowników obecnych w oddziale w czasie napadów była mniejsza lub równa 7 osobom. Napad trwał najczęściej do 3 minut, chociaż zdarzały się dość często również trwające do 10 minut. Niestety, nie dysponujemy informacjami dotyczącymi przygotowania zawodowego przestępców oraz metod oddziaływania na pracowników. Wiadomo tylko tyle, że w około 50% przypadków byli zamaskowani i atakowali pojedynczo lub w parach. Dniami najwyższej aktywności przestępczej są czwartek i piątek, chociaż od roku 2000 występuje też wtorek. Od roku 2002 pojawiają się pierwsze informacje dotyczące przygotowania zawodowego napastników – w prawie 80% byli to profesjonaliści. Sam napad zaczyna trwać dłużej niż pierwotnie – od 3 do 10 min. W 86% przypadków sprawcy byli uzbrojeni w broń palną, a wydanie łupu egzekwowali poprzez bezpośrednie zastraszenie kasjera. Akcje napastników najczęściej udaremniały kasy z zamkami zwłocznymi. Ataki na bankomaty są sporadyczne – najczęściej skierowane na samo urządzenie.

- POLSKA

Po zapoznaniu się z sytuacją wybranych krajów UE i Szwajcarii możemy przyjrzeć się bliżej sytuacji w Polsce. Pierwsze dane o napadach na banki w naszym kraju pojawiają się dopiero w roku 1995. Liczba napadów – od 7 w roku 1997 ustawicznie rośnie, by w roku 2002

osiągnąć 88. Do roku 2004 obserwujemy spadek do 70 przypadków. Liczba nieudanych lub udaremnionych napadów waha się od 18 do 3 w poszczególnych latach. W porównaniu z wyżej omawianymi krajami, straty rodzimych banków są niewielkie, wręcz marginalne – największa roczna kwota to około 570 tys. euro w 1998 roku, najmniejsza natomiast to 134 tys. dolarów w roku 1995. Napady były początkowo dokonywane przez amatorskie gangi w godzinach normalnej pracy oddziałów, środkiem przymusu było bezpośrednie zastraszenie kasjera, a napad trwał od 3 do 10 min. Przestępcy atakowali najczęściej oddziały banków usytuowane poza dużymi miastami. Napastnicy generalnie byli zamaskowani, starali się wkraczać, gdy w oddziałach nie było klientów. Personel napadanych placówek najczęściej nie przekraczał 7 osób. Znamienne jest, że w kraju, w którym dostęp do broni palnej dla obywateli jest praktycznie niemożliwy, przestępcy posługiwali się nią w 92% przypadków. Od roku 1999 obserwuje się skrócenie czasu akcji przestępczej do maksymalnie 3 minut oraz wzrost dbałości o ukrycie tożsamości napastników, pozostałe czynniki nie ulegają zmianie. Należy zauważyć, że zakusy przestępców najczęściej niweczył alarm. W roku 2004 zaobserwowano pewne przesunięcie w liczbie napadających – z akcji zbiorowych w kierunku akcji indywidualnych bądź wykonywanych parami. Przypadki napadów na bankomaty są wyjątkowo rzadkie; najczęściej zdarzają się wśród nich akty wandalizmu i zastraszanie klientów.

Przyczny spadku i wzrostu liczby napadów

Banki jako instytucje finansowe zawsze były atrakcyjnym celem dla przestępców, kojarzyły się bowiem z dużą ilością pieniędzy. Łup pochodzący z napadu na taką instytucję zawsze był większy od napadu na sklep czy stację benzynową. Przyjrzyjmy się teraz przyczynom wzrostu i spadku aktywności przestępczej w tym „dziale gospodarki".

Największy wzrost liczby napadów na banki notuje się w krajach, w których w danym okresie znacznie pogarsza się sytuacja ekonomiczna. Ważnym czynnikiem są też przepełnione więzienia, co owocuje krótkimi wyrokami, a zarazem nie działa odstraszająco na przestępców.

Duże znaczenie ma także sprawność policji w ściganiu sprawców przestępstw – im skuteczność mniejsza, tym większe poczucie bezkarności. Powstawanie małych, gorzej zabezpieczonych oddziałów zachęca do działania przede wszystkim przestępców amatorów nieposiadających na tyle wiedzy, by zaatakować większą placówkę. Czynnikiem sprzyjającym powodzeniu napadu jest nowy, niedoświadczony lub słabo przeszkolony personel, niewiedzący, jak reagować w sytuacjach zagrożenia. Kraje posiadające „rodzime" grupy terrorystyczne, sąsiadujące z terenami ogarniętymi wojną lub w których jest dobrze rozwinięta przestępczość zorganizowana, są dodatkowo narażone na wzrost liczby napadów. Niepokojący jest również wzrost współpracy z przestępcami pracowników banków, ułatwiających im aktywnie lub pasywnie napad.

Spadek liczby napadów powodowany jest wprowadzaniem nowych zabezpieczeń oddziałów oraz lepszą współpracą banków z policją. Lepsze zabezpieczenia zniechęcają w znacznej mierze napastników działających amatorsko, powodując zmianę orientacji ich działalności na obiekty handlowe, takie jak sklepy czy stacje benzynowe. Duży wpływ ma oddziaływanie na świadomość przestępców – wizja nieuchronności kary, ograniczenie łupu do minimum. Spadek liczby napadów uzyskano poprzez wprowadzanie bankomatów w miejsca niektórych oddziałów bankowych – jak wiadomo, bankomat ciężej zastraszyć od kasjera. Na wzrost bezpieczeństwa banków wpływają także szkolenia pracowników oraz wprowadzanie jasnych i klarownych procedur postępowania. Do spadku liczby napadów przyczyniło się znacznie wprowadzenie wspólnej waluty, czyli euro. Czynnikiem zniechęcającym jest również wprowadzenie oddziałów bezgotówkowych.

Metody ataku i obrony

Jak wspomniano we wstępie, wojna pomiędzy bankami a przestępcami wymusza opracowywanie przez obie strony nowych metod działania.

Przestępcy wykorzystują zarówno metody standardowe, np. wejście do banku i sterroryzowanie kasjera, jak i bardziej wyszukane czy brutalne. Często używane są materiały wybuchowe, sprzęt ciężki do

forsowania ścian zewnętrznych czy barier szklanych, zdarzają się też porwania menedżerów czy osób im bliskich w celu wymuszenia okupu lub dostępu do sejfów czy skarbców. Rejestrowano również napady połączone z włamaniem, kiedy sprawcy włamywali się do banku, a następnie czekali na personel, by wymusić dostęp do pieniędzy. Młodociane gangi znalazły sposób na zwiększenie łupu – oprócz stoisk kasowych rabowali też klientów – rodzaj takich napadów został nazwany *steamingiem*. W państwach sąsiadujących z strefami ogarniętymi wojną zaobserwowano gangi używające sprzętu wojskowego. Kolejnym typem napadów są *ramraids* – ataki z wykorzystaniem ciężkich pojazdów, np. ciężarówek czy dużych samochodów terenowych, używanych do taranowania ścian zewnętrznych i wewnętrznych barier. Stosowanie kamer i wykrywaczy metalu wymusiło na przestępcach częstsze maskowanie się i używanie broni alternatywnych, jak strzykawki, igły, kawałki szkła. Niestety dla profesjonalistów nie ma przeszkód nie do pokonania. Każde wprowadzone zabezpieczenie chroni tylko okresowo, do momentu aż zostanie rozpracowane przez napastników. Bankomaty, które zaczęły być coraz szerzej stosowane, nie umknęły uwadze przestępców. Szybko opanowano metody ich rabowania – od wyrywania ich ze ścian za pomocą wózków widłowych czy samochodów ciężarowych, otwierania za pomocą palników do wysadzania gazem lub materiałami wybuchowymi. Niektóre z tych metod zostały też użyte przeciwko kasom i automatom wydającym gotówkę. Kolejnymi metodami napadu na bankomaty wypracowanymi przez przestępców stały się ataki na załogi serwisujące lub uzupełniające bankomaty. Zaczęto też napadać klientów tych urządzeń. Skrócenie czasu reakcji policji czy służb ochrony zaowocowało większą stanowczością i brutalnością w działaniach przestępczych ukierunkowaną na skrócenie do minimum czasu napadu. Oczywiście, jest to tylko przykładowe wyliczenie metod działania przestępców, pełnej listy nie sposób przedstawić – nie wiadomo, co w tym momencie planują gdzieś zawodowcy.

Mimo tak drastycznych i urozmaiconych metod działania napastników banki nie są bezbronne – wręcz przeciwnie. To właśnie ich przy-

gotowanie wymusza opracowywanie nowych metod działania przez przestępców.

Jak się szybko przekonano, podstawą bezpieczeństwa banków jest szkolenie personelu oraz opracowywanie jasnych i klarownych procedur postępowania w sytuacji kryzysowej. W wypadku napadu na pracownikach banku spoczywa odpowiedzialność za życie i zdrowie swoje oraz klientów. Dzięki odpowiednio opracowanym dyrektywom postępowania i dobrej organizacji oddziału udaje się ograniczyć ryzyko napadu, a w wypadku jego nastąpienia – wysokość łupu. Mechaniczne i elektroniczne środki zabezpieczenia też nie są bez znaczenia. Stosowane są alarmy ciche i głośne, systemy telewizji przemysłowej ukrytej i jawnej. W niektórych bankach stosuje się wykrywacze metalu. Na szeroką skalę używane są systemy kontroli dostępu do wydzielonych stref, uniemożliwiające wstęp i przebywanie w nich osób nieuprawnionych. W oddziałach typu otwartego stosuje się urządzenia zwłoczne połączone w jeden system – po uaktywnieniu czujnika ostatniego banknotu w urządzeniu kasowym, pozostałe urządzenia wydające gotówkę blokują się na określony czas. Postanowiono też wykorzystać bankomaty jako alternatywę dla niektórych czynności lądowych. W oddziałach zamkniętych stosuje się ekrany ze szkła kuloodpornego lub wzmacnianego w celu zabezpieczenia kasjerów. Ciekawymi rozwiązaniami są inteligentne walizki do transportu gotówki na niewielkie odległości, kasety z urządzeniami barwiącymi oraz dymnymi mającymi na celu zniszczyć banknoty w wypadku próby nieautoryzowanego dostępu, gotówkowe pakiety-przynęty zawierające znaczone banknoty lub ładunki barwiące. Metodą ograniczającą wysokość łupu w wypadku napadu jest podział przechowywanej gotówki pomiędzy kilka stref chronionych zabezpieczeniami czasowymi i innymi. Na koniec można wspomnieć o niewdrożonym projekcie dotyczącym przechowywania w oddziale gotówki, niejako przeznaczonej dla przestępców w wypadku napadu. Projekt ten został zarzucony, ponieważ kwota przygotowana dla napastników mogłaby działać zachęcająco i prowokować częstsze odwiedziny nieproszonych gości. W miejsce tego rozwiązania zaczęto za pomocą wywieszek powszechnie stosować informowanie wszystkich obecnych w banku, że

w oddziale stosowane są urządzenia zwłoczne, na których działanie personel nie ma żadnego wpływu.

Wnioski i zakończenie

Jak widać, Polska na tle bardziej rozwiniętych krajów Unii Europejskiej wypada stosunkowo dobrze, w kwestii liczby napadów na banki i sposobów przeciwdziałania owym napadom. Należy podkreślić, że straty poniesione w wyniku napadów na banki w naszym kraju są niewielkie. Można je wręcz przyrównać do strat będących efektem błędnie przeprowadzonej operacji bankowej. Nie powstrzymuje to oczywiście banków przed rozwijaniem systemów bezpieczeństwa bankowego oraz dostosowywaniem standardów do tych panujących w Unii Europejskiej.

Nie należy się spodziewać znacznego zwiększenia liczby napadów na polskie banki w najbliższym czasie. Rozwojowi techniki stosowanej przez przestępców i wzrostowi liczby oddziałów towarzyszy rozwój technik zabezpieczających, tak więc sytuacja wydaje się stosunkowo stabilna. W porównywanych krajach także nie odnotowano znacznych wzrostów liczby napadów. Należy więc spodziewać się nadal tendencji do „równowagi" między przestępcami a systemami i służbami ochrony banków. Sytuacja gospodarczo-polityczna, jaka nastała w naszym kraju po 1989 r., postawiła rodzimą przestępczość w trudnej sytuacji. Szybki napływ technologii oraz wypracowanie odpowiednich rozwiązań organizacyjnych znacznie zwiększyły bezpieczeństwo banków. Jednak nie należy zapominać, że wraz z importem technologii zabezpieczeń nastąpił również import przestępczego *know-how* występujący pod postacią gotowych do zastosowania rozwiązań, wypróbowanych już w krajach Europy Zachodniej. (Należy również zauważyć, że nasi przestępcy dopiero uczą się nowej dla nich profesji, jaką jest rabowanie banków. Mają o tyle trudniejsze zadanie od swoich kolegów z zagranicy, że od razu muszą walczyć z najnowszymi zabezpieczeniami już sprawdzonymi w innych krajach).

Nowe pomysły, takie jak „oddziały bezgotówkowe", przyczyniają się wprawdzie do znacznego zwiększenia bezpieczeństwa banków. Na-

wet jednak całkowite przejście na oddziały bezgotówkowe nie rozwiąże problemu. Przestępcy podjęliby inne rodzaje działalności, takie jak napady na bankomaty czy osoby z nich korzystające.

Należy więc kontynuować badania dążące do polepszenia bezpieczeństwa banków oraz z całą stanowczością karać schwytanych przestępców, szczególnie tych, którzy dopuścili się przemocy w trakcie napadu. Zwiększenie liczby napadów z użyciem przemocy fizycznej to bardzo niepokojący trend, z którym należy walczyć.

Mamy nadzieję, że przedstawione wyżej porównanie Polski do innych krajów Unii Europejskiej pokazało, że w tej materii Polska nie jest w tyle za innymi krajami, a niektóre, np. Włochy, wyprzedza w dziedzinie bezpieczeństwa oddziałów bankowych.

Agnieszka Sagan-Jeżowska, Kinga Łukaszek

Transakcje przeciekowe w obrocie papierami wartościowymi w Polsce i ich zwalczanie

Czego dotyczy?

Transakcje przeciekowe, czyli *insider trading*, to transakcje dokonane przy ujawnieniu i z wykorzystaniem tajemnicy zawodowej lub informacji poufnej.

Tajemnica zawodowa to zakaz ujawniania informacji uzyskanych w związku z podejmowanymi czynnościami w ramach zatrudnienia, stosunku zlecenia lub innego stosunku prawnego. Tajemnica zawodowa ma charakter bezwzględny, nie ma bowiem ram czasowych, w jakich tajemnica obowiązuje. Zakaz ujawniania i wykorzystywania w obrocie papierami wartościowymi informacji stanowiących tajemnicę zawodową jest wyrażony w art. 179 Ustawy o nadzorze nad rynkiem finansowym. Jest to przestępstwo umyślne, czyli warunkiem niezbędnym jest świadomość sprawcy, że dana informacja jest chroniona tajemnicą zawodową i ma charakter niejawny; oraz indywidualne, gdyż odpowiedzialności z art. 179 podlegają wyłącznie osoby prawnie zobowiązane do zachowania tajemnicy zawodowej, których katalog zawarty jest w ustawie. Naruszenie tego przepisu jest naruszeniem dóbr uczestników obrotu publicznego papierami wartościowymi, zarówno interesów majątkowych, jak i niemajątkowych.

Informacja poufna to „określona w sposób precyzyjny informacja dotycząca bezpośrednio lub pośrednio jednego lub kilku emitentów instrumentów finansowych, jednego lub kilku takich instrumentów finansowych albo nabywania lub zbywania takich instrumentów, która nie została przekazana do publicznej wiadomości, a która po takim przekazaniu mogłaby w istotny sposób wpłynąć na cenę tych instru-

mentów finansowych lub na cenę powiązanych z nimi pochodnych instrumentów finansowych". Informacja poufna może mieć charakter trwale niejawny, czyli nie musi, a nawet nie może być podana do publicznej wiadomości, oraz charakter czasowo niejawny, takie informacje emitent jest zobowiązany w ciągu 24 godzin podać do publicznej wiadomości. W wyjątkowych sytuacjach emitent może uzyskać zgodę Komisji Nadzoru Finansowego na publikację danej informacji poufnej w terminie dłuższym, ściśle wyznaczonym przez Komisję. Przestępcze ujawnienie informacji poufnej zawarte w art. 180 Ustawy o nadzorze nad rynkiem finansowym jest przestępstwem umyślnym i indywidualnym, chociaż ustawa nie zawiera enumeratywnego spisu osób podlegających tej regulacji. Bezprawne wykorzystanie informacji poufnej z art. 181 wymienionej ustawy jest również przestępstwem umyślnym, ale i powszechnym, co oznacza, że sprawcą może być każda osoba wykorzystująca treść informacji poufnej w obrocie papierami wartościowymi. Wykorzystaniem informacji poufnej jest także nakłanianie do nabycia lub zbycia danych papierów wartościowych, gdy jest to działanie wywołane faktem posiadania informacji niejawnych. Artykuły 180 i 181 chronią i dotyczą tylko emitenta i papierów wartościowych oraz podmiotów z nimi współpracujących.

Zgodnie z rozróżnieniem źródeł informacji niejawnej osoby mające dostęp do tych informacji, czyli tzw. insiderów, można rozróżnić na insiderów pierwotnych, którzy mają dostęp do informacji z racji swego stanowiska lub wykonywanej funkcji; oraz insiderów wtórnych, czyli osoby, które weszły w posiadanie informacji niejawnej w sposób nielegalny, czy to na skutek własnego działania: nielegalnego podsłuchu, kradzieży dokumentów, szpiegostwa przemysłowego, czy za pośrednictwem insiderów pierwotnych.

Ujawnianie i wykorzystywanie informacji niejawnych podważa fundamenty obrotu, godzi w zasadę równego traktowania wszystkich uczestników obrotu papierami wartościowymi w dostępie do informacji, w zasadę uczciwości obrotu oraz w zasadę poufności działań podejmowanych przez poszczególnych uczestników. Osoby znające fakty niedostępne dla szerszego grona osób uzyskują przewagę. Przestępstwo

nadużycia poufnych informacji zakłóca funkcjonowanie rynku papierów wartościowych przez uszczuplenie zaufania inwestorów do zasady równego traktowania. Tworzenie regulacji prawnych, których zadaniem jest ochrona obrotu papierami wartościowymi przed użyciem informacji poufnych, uznawane jest za wyraz dojrzałości rynku kapitałowego. *Insider trading* na całym świecie jest uznawane za szczególnie niebezpieczną kategorię czynów zabronionych.

Komisja Nadzoru Finansowego

W dniu 19 września 2006 r., tj. z dniem wejścia w życie przepisów Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym rozpoczęła swoją działalność Komisja Nadzoru Finansowego. Ten nowy organ nadzoru przejął zadania zniesionych przepisami ustawy Komisji Nadzoru Ubezpieczeń i Funduszy Emerytalnych oraz Komisji Papierów Wartościowych i Giełd. Komisja Nadzoru Finansowego sprawuje nadzór nad rynkiem kapitałowym, nadzór ubezpieczeniowy, emerytalny oraz nadzór uzupełniający nad konglomeratami finansowymi, w których skład wchodzą nadzorowane podmioty. Celem skupienia nadzoru nad rynkiem finansowym w jednym organie jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku. Od dnia 1 stycznia 2008 r. nadzór finansowy sprawowany przez Komisję Nadzoru Finansowego obejmie też nadzór bankowy oraz nadzór nad instytucjami pieniądza elektronicznego sprawowany obecnie przez Komisję Nadzoru Bankowego. Nadzór nad działalnością KNF sprawuje Prezes Rady Ministrów.

Do zadań Komisji należy ponadto:

- podejmowanie działań służących prawidłowemu funkcjonowaniu rynku finansowego;
- podejmowanie działań mających na celu rozwój rynku finansowego i jego konkurencyjności;
- podejmowanie działań edukacyjnych i informacyjnych w zakresie funkcjonowania rynku finansowego;

- udział w przygotowywaniu projektów aktów prawnych w zakresie nadzoru nad rynkiem finansowym;
- stwarzanie możliwości polubownego i pojednawczego rozstrzygania sporów między uczestnikami rynku finansowego, w szczególności sporów wynikających ze stosunków umownych między podmiotami podlegającymi nadzorowi Komisji a odbiorcami usług świadczonych przez te podmioty;
- wykonywanie innych zadań określonych ustawami.

Wykrywanie przestępstw

Departament Nadzoru Rynku czuwa nad przestrzeganiem przepisów przez uczestników publicznego obrotu instrumentami finansowymi oraz towarami giełdowymi w zakresie czynów skutkujących odpowiedzialnością karną lub administracyjną, w tym *insider trading*, określonych w szczególności w ustawie Prawo o publicznym obrocie papierami wartościowymi, Ustawie o giełdach towarowych i Ustawie o funduszach inwestycyjnych.

Wydział Postępowań Administracyjnych Departamentu Nadzoru Rynku po dostosowaniu prawa polskiego do Dyrektywy Market Abuse może prowadzić postępowanie administracyjne niezależnie od postępowania wyjaśniającego oraz ma szerszy zakres odpowiedzialności administracyjnej. Aby zapewnić skuteczność egzekwowania prawa na rynku kapitałowym, dokonano dekryminalizacji niektórych naruszeń prawa zagrożonych dotychczas sankcjami karnymi i wprowadzono odpowiedzialność administracyjną przed KNF, która może w drodze decyzji administracyjnej nałożyć karę pieniężną w wysokości do 1 mln zł.

Karą do 200 tys. zł są zagrożeni insiderzy pierwszego stopnia: członkowie zarządów i rad nadzorczych spółek publicznych, którzy w czasie trwania okresu zamkniętego nabywają lub zbywają na rachunek własny lub osoby trzeciej akcje emitenta, prawa pochodne oraz inne instrumenty finansowe z nimi powiązane. Na insiderów, którzy naruszyli przepisy o obowiązku informacji o dokonywanych przez siebie lub przez osoby im bliskie transakcjach akcjami spółki lub innymi instrumentami finansowymi z nimi związanymi, KNF może nałożyć karę pieniężną

w wysokości do 100 tys. zł. Wydział Postępowań Administracyjnych prowadzi postępowanie administracyjne dotyczące deliktów administracyjnych, przygotowuje opinie i udziela wyjaśnień w sprawach związanych z funkcjonowaniem rynku kapitałowego.

Wydział Spraw Karnych prowadzi postępowanie wyjaśniające oraz sporządza zawiadomienia o podejrzeniu popełnienia przestępstwa Zajmuje się czynami zagrożonymi sankcjami karnymi, w tym *insider trading*:

- wykorzystaniem informacji poufnej;
- zaniedbaniem przez emitenta prowadzenia odrębnych list określonych osób fizycznych, które mają dostęp do informacji poufnej;
- wykorzystaniem i ujawnieniem informacji poufnej lub tajemnicy zawodowej;
- zaniedbaniem obowiązku publikacji informacji poufnych.

Departament Nadzoru Rynku współpracuje z policją, prokuraturą, sądami, Agencją Bezpieczeństwa Wewnętrznego i występuje w charakterze świadka przed tymi organami.

Departament Informacji i Analiz za pomocą systemu Warset działającego na Giełdzie Papierów Wartościowych wykrywa podejrzane ruchy kapitału, zwłaszcza jeśli nie ma o nich informacji ze spółki; podejrzany może być nagły wzrost wolumenu obrotu, czyli nadzwyczaj wysoka transakcja dla danego rachunku papierów wartościowych; ciągła zmiana właściciela rachunku lub rachunek, na którym zazwyczaj nic się nie dzieje, tylko od czasu do czasu dokonywane są transakcje zawsze przynoszące duże zyski. Może się na przykład okazać, że właścicielem takiego rachunku jest makler lub członek kancelarii, mający dostęp do informacji poufnych. Departament Informacji i Analiz przekazuje te dane do Departamentu Nadzoru Rynku.

Postępowanie wyjaśniające prowadzi upoważniony pracownik urzędu Komisji, upoważnienie przyjmuje formę dokumentu podpisywanego przez Przewodniczącego Komisji. Pismo powinno wskazywać przedmiot postępowania, jego zakres, miejsce prowadzenia, datę rozpoczęcia

oraz przewidywany czas zakończenia. Prowadzący postępowanie zwraca się do Domu Maklerskiego o podanie danych osobowych właściciela rachunku papierów wartościowych, inwestorów oraz osoby składającej zamówienie na daną transakcję; przegląda umowy o prowadzenie tego rachunku, kopie zleceń transakcji oraz analizuje historię rachunku pod kątem polityki inwestycyjnej: czy ta transakcja odbiegała od dotychczasowego sposobu zarządzania rachunkiem oraz czy była to wyjątkowo duża inwestycja, patrząc przez pryzmat statusu finansowego tego rachunku. Porównuje też listę insiderów firmy, na której niekorzyść dokonano transakcji. Dyrektywa Market Abuse wprowadziła uprawnienia *quasi*-operacyjne dla postępowania wyjaśniającego. Na żądanie prowadzącego postępowanie każda osoba jest zobowiązana do złożenia pisemnych lub ustnych wyjaśnień, jednak na tym etapie nie ma odpowiedzialności karnej za składanie fałszywych zeznań. Uczestnicy obrotu papierami wartościowymi najczęściej udzielają wyjaśnień, osoby postronne zazwyczaj podchodzą do sprawy z rezerwą. Bada się też ścieżkę zawodową świadków, aby ustalić krąg znajomych i ewentualne powiązania z insiderami. Przewodniczący Komisji ma prawo wstępu do siedziby i do lokalu spółki prowadzącej giełdę celem wglądu do ksiąg, dokumentów i innych nośników informacji; może też zarządzić zajęcie dokumentu lub innego nośnika informacji niezbędnego do dalszego prowadzenia postępowania, zwrócić się z żądaniem do podmiotu świadczącego usługi telekomunikacyjne o udostępnienie informacji stanowiących tajemnicę telekomunikacyjną w zakresie wykazu połączeń telefonicznych lub innych przekazów informacji: prywatnej korespondencji, w tym elektronicznej, nagrań telefonicznych; może zażądać zablokowania rachunku papierów wartościowych, może zwrócić się do Generalnego Inspektora Kontroli Skarbowej o przekazanie informacji stanowiących tajemnicę skarbową.

Po zakończeniu postępowania wyjaśniającego Przewodniczący KNF w zależności od rezultatów uprawniony jest do zarządzenia zamknięcia postępowania wyjaśniającego bez podejmowania jakichkolwiek dalszych kroków prawnych, do wszczęcia postępowania administracyjnego lub do złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa.

Zawiadomienie do prokuratury może też złożyć spółka pokrzywdzona, lecz najczęściej nie wie, że doszło do działań przestępczych. Komisja składa ponad 80% wszystkich zawiadomień. Przestępstwami giełdowymi zajmuje się osobna komórka śledcza w Prokuraturze Okręgowej w Warszawie. W 99% zawiadomień prokuratura wszczyna śledztwo. Członek Departamentu Nadzoru Rynku składa zeznania zawierające wszystko to, co KNF uzyskała w danej sprawie. Przewodniczący Komisji ma status pokrzywdzonego w rozumieniu prawa karnego nie tylko w sprawach karnych prowadzonych na podstawie ustaw regulujących funkcjonowanie rynku kapitałowego, ale również w sprawach prowadzonych na innej podstawie prawnej, o ile przestępstwa są skierowane przeciwko interesom uczestników rynku kapitałowego. Z uprawnień pokrzywdzonego może korzystać poprzez występowanie przed właściwymi sądami karnymi w charakterze oskarżyciela posiłkowego oraz poprzez czynną realizację uprawnień pokrzywdzonego na etapie postępowania przygotowawczego, w szczególności poprzez składanie wniosków o udział przedstawiciela Komisji w czynnościach dowodowych przeprowadzanych przez organy ścigania oraz stały monitoring najważniejszych spraw prowadzonych przez prokuraturę. Działa na równi z prokuratorem: wnioskuje zachowania, przegląda akta, przesłuchuje świadków – na tym etapie występuje już odpowiedzialność karna za składanie fałszywych zeznań. W praktyce okazuje się, że bardzo rzadko zeznania różnią się od tych złożonych w trakcie postępowania wyjaśniającego. Zdarza się, że zachodzi konieczność przesłuchania kilkudziesięciu świadków. Postępowania dotyczące *insider trading* są najczęściej bardzo przewlekłe, często są też umarzane ze względu na brak dowodów. Postanowienie prokuratury o umorzeniu postępowania Przewodniczący może zażalić do Prokuratury Apelacyjnej; jeśli ta podzieli stanowisko Przewodniczącego, sprawa wraca do Prokuratury Okręgowej. Powołuje się biegłych sądowych, których zadaniem jest ocena, czy doszło do popełnienia danego przestępstwa. Ponad 50% opinii jest twierdząca. Po takiej opinii biegłego prokuratura wnosi akt oskarżenia. Jeżeli natomiast Prokuratura Apelacyjna odrzuci zażalenie lub Prokuratura Okręgowa po raz drugi umorzy postępowanie, Prze-

wodniczący KNF może wnieść pozew z oskarżenia prywatnego. W sądzie Przewodniczący występuje jako oskarżyciel posiłkowy najczęściej reprezentowany przez radców prawnych. Sprawa toczy się przed sądem właściwym miejscowo dla oskarżonego, co jest dużą niekonsekwencją. Skoro stworzono jedną wyspecjalizowaną w takich sprawach jednostkę śledczą, analogicznie powinno być z wydziałem sądu. Prokuratura oraz przedstawiciele KNF jeżdżą do sądów na terenie całego kraju, a sędziowie regionalni spotykają się z przestępstwem giełdowym najczęściej pierwszy i najprawdopodobniej ostatni raz w życiu.

Granica informacji poufnej

Uczestnicy obrotu papierami wartościowymi korzystają z Elektronicznego Systemu Przekazywania Informacji. Przesyłanie informacji za pomocą ESPI odbywa się z wykorzystaniem Internetu. Transmisja jest zabezpieczana przez wykorzystanie certyfikatów bezpieczeństwa i protokołu SSL. W roku 2005 zostało uruchomione dodatkowe łącze komunikacyjne do siedziby Urzędu KNF. W ESPI publikowane są raporty bieżące. Emitenci mają obowiązek, generalnie w ciągu 24 godzin, podać do publicznej wiadomości każdą informację poufną. Ponieważ nie ma definicji legalnej ani zamkniętego katalogu informacji poufnych, emitent sam decyduje, czy dana informacja jest poufna, czy też nie. Kluczowy powinien być fakt, czy inwestor weźmie tę informację pod uwagę przy podejmowaniu decyzji. Emitent jest zobowiązany dostarczyć inwestorowi rzetelną i pełną informację, nie zasypując go przy tym niepotrzebnymi danymi. Gdy emitent ujawni informację uznaną za nieistotną, naraża się na sankcję za próbę manipulacji rynkiem, zmuszając niejako inwestora do zapoznania się z informacją oraz podjęcia kolejnych decyzji dotyczących tych papierów wartościowych. Ponadto inwestorzy cały czas otrzymują raporty bieżące i gdyby emitenci tą drogą publikowali informacje inne niż strategiczne, inwestorzy nie nadążaliby z reagowaniem na wszystkie przekazywane informacje i mogliby być tym sposobem pośrednio blokowani w podejmowaniu decyzji. Natomiast gdy emitent uzna, że dana informacja nie jest ważna i jej nie opublikuje, nie dość, że naraża się na sankcję za niepublika-

cję, to również ryzykuje, że ta informacja zostanie jednak wykorzystana przez innego uczestnika obrotu papierami wartościowymi. Całe ryzyko związane z każdorazowym określaniem granicy informacji poufnej leży po stronie emitenta.

Polska giełda w Unii Europejskiej

Ujednolicanie prawa obowiązującego w poszczególnych krajach Unii Europejskiej jest procesem długofalowym. W Polsce ciągle są wprowadzane nowelizacje ustaw w celu dostosowania regulacji krajowych do europejskich. Po zmianie polskich regulacji prawnych do dyrektywy w sprawie nadużyć na rynku giełdowym spółka, której prospekt zostanie zatwierdzony w Polsce, może bez dodatkowych przeszkód zabiegać o kapitał we wszystkich krajach Unii Europejskiej, jak również zagraniczne firmy z całej UE na identycznych zasadach mogą starać się o pieniądze polskich inwestorów. Spółki notowane na warszawskiej giełdzie mają w zdecydowanej większości charakter lokalny. Poza WIG20 mamy do czynienia z małymi firmami, które są zazwyczaj dopiero w początkowej fazie rozwoju. Jednak jest wśród nich grupa, która może śmiało stawić czoła zagranicznym konkurentom. Krajowe przedsiębiorstwa maklerskie dopiero zaczynają interesować się rynkiem europejskim. Natomiast implikacja prawa europejskiego znacznie uwiarygodniła Polskę w oczach zagranicznych emitentów i inwestorów. Prywatyzacja spółek Skarbu Państwa, Otwarte Fundusze Emerytalne, które z racji konstrukcji prawnej inwestują głównie na polskim rynku oraz debiuty dobrych i dużych spółek prywatnych przyciągają coraz więcej unijnych firm inwestycyjnych, zgłaszających chęć działania na polskiej giełdzie. Z jednej strony Polska otworzyła się na konkurencję ze strony podmiotów z krajów Unii, ale z drugiej strony stała się częścią wspólnego europejskiego rynku kapitałowego. To z kolei sprawia, że działania przestępcze coraz częściej mogą przybierać charakter międzynarodowy. Na polskim rynku działa coraz więcej spółek zależnych od spółek zagranicznych. Sytuacja finansowa jednej z tych spółek wiąże się automatycznie z sytuacją finansową tej drugiej. Jednak działają na dwóch różnych rynkach. Naturalną koleją rzeczy spółka zależna zawsze będzie szybciej i rzetelniej poinformowana. Cza-

sami dochodzi też do sytuacji, gdy spółka publikuje informację poufną za granicą. Powstaje wątpliwość, czy informacja, która została upubliczniona za granicą, nadal jest informacją poufną. Nie została ujawniona przez emitenta, nie jest też informacją powszechnie znaną, więc inwestorzy nie mają równego dostępu do informacji. Ale też taka informacja nie została pozyskana w sposób nielegalny, więc nie można mówić o łamaniu prawa. Takie stanowisko prezentuje linia prokuratury, wychodząc z założenia, że jeśli informacja jest dostępna szerokiemu audytorium, przestaje być informacją poufną. Analogicznie dzieje się w sytuacji, gdy informacja poufna zostaje zamieszczona w Internecie. Nawet jeśli znajduje się na mało znanej, trudno dostępnej stronie internetowej, taka informacja przestaje być poufna, a jej wykorzystanie nie ma charakteru przestępczego. Tym podobne sytuacje pozwalają na legalne wykorzystanie przewagi informacyjnej.

Prawo unijne obejmuje 25 różnych rynków finansowych i 25 różnych regulacji prawnych, jednak nie przesądza o wszystkich kwestiach, lecz pozostawia decyzję państwom członkowskim pozwalając dostosować rozwiązania przystające do sytuacji faktycznej w danym kraju. Tak jest z granicą między działaniami objętymi postępowaniem administracyjnym a objętymi postępowaniem karnym. Może się zdarzyć tak, że dany czyn w jednym państwie będzie podlegał postępowaniu administracyjnemu, a w innym postępowaniu karnemu. Jeśli przy tym przestępstwo zostało popełnione na terytorium Polski, ale przedmiot przestępstwa był emitowany w innym państwie, to według którego prawa powinno być sądzone? Wydaje się, że jeśli w prawie polskim czyn jest przestępstwem, a według prawa tego drugiego państwa czyn podlega postępowaniu administracyjnemu, to postępowanie powinno się toczyć w Polsce zgodnie z prawem karnym. Natomiast jeśli w obu państwach czyn podlega takim samym regulacjom, wtedy prokuratura powinna zawiadomić prokuraturę państwa, na którego terytorium był emitowany przedmiot przestępstwa. Niemniej jednak cała sprawa, jak wszystkie o charakterze międzynarodowym, jest bardzo delikatna, a praktyka nie zdążyła jeszcze wypracować zwyczajów postępowania. W 2003 r. Komisja Papierów Wartościowych i Giełd w ramach człon-

kostwa w Międzynarodowej Organizacji Komisji Papierów Wartościowych IOSCO podpisała globalne porozumienie Multilateral Memorandum of Understanding (MMoU) oraz w 2004 r. z racji przynależności do Komitetu Europejskich Regulatorów Rynku Papierów Wartościowych CESR Multilateral Memorandum of Understanding on the Exchange of Information and Surveillance of Securities Activities (MoU). Porozumienia te dotyczą wymiany informacji pomiędzy regulatorami rynku kapitałowego i zasad wielostronnej współpracy przy zwalczaniu przestępstw na rynkach kapitałowych. Dzięki współpracy krajów bardziej doświadczonych w zwalczaniu przestępstw giełdowych z tymi mniej doświadczonymi wyrównuje się także poziom merytoryczny jednostek odpowiedzialnych za walkę z przestępczością giełdową.

Prewencja

W walce z *insider trading*, jak w każdym innym przypadku, najważniejsze jest zapobieganie.

Giełda Papierów Wartościowych analizuje na bieżąco istniejące zabezpieczenia techniczne oraz regulacje stosowane na innych czołowych rynkach kapitałowych zajmujących się zwiększaniem bezpieczeństwa obrotu. Gdy tylko pojawiają się nowe narzędzia, giełda stara się je jak najszybciej wprowadzić na polski rynek. Nieodpłatnie udostępnia domom maklerskim oprogramowanie stworzone przez GL Trade SA – jedną z największych światowych firm dostarczających oprogramowanie tego typu. Program ten jest używany jako standard na terenie Europy, Ameryki Północnej i Azji. Umożliwia on kontrolę składanych zleceń. Użytkownicy sami, w sposób elastyczny dostosowują parametry kontrolne dla wybranych rodzajów transakcji oraz dla poszczególnych użytkowników, co umożliwia prawie stuprocentowe blokowanie błędnych zleceń, w tym również celowej manipulacji i działań przestępczych. Te kryteria mogą dotyczyć maksymalnej wartości lub wolumenu zlecenia, maksymalnej liczby wysłanych zleceń, dopuszczenia określonych typów ważności oraz rodzajów zleceń, dopuszczenia składania zleceń kupna lub sprzedaży, autoryzowania składania zleceń tylko na określone typy produktów giełdowych i inne.

Urząd Komisji posiada certyfikaty norm Zarządzania Jakością PN-EN ISO 9001:2001 oraz Zarządzania Bezpieczeństwem Informacji BS 7799-2:2002, które zdobył w marcu 2004 r. jako pierwsza jednostka administracji publicznej w Polsce oraz jako pierwszy regulator rynku kapitałowego. Mając na uwadze dalsze doskonalenie, w styczniu 2006 r. podjęto działania mające na celu wdrożenie Systemu Elektronicznego Obiegu Dokumentów, elektronicznej kancelarii i archiwum. Celem projektu jest wdrożenie w Urzędzie Komisji Systemu Elektronicznego Obiegu Dokumentów *Workflow*, obejmującego swym zakresem:

- procedury obowiązujące w Urzędzie, m.in. planowane jest wdrożenie około 45 procedur funkcjonujących w postaci elektronicznej,
- obsługę kancelarii ogólnej, sekretariatów, prowadzenie rejestrów korespondencji,
- podstawowe moduły funkcjonalne związane z elektronicznym obiegiem dokumentów, między innymi:

a) śledzenie stanu realizacji spraw oraz monitorowanie terminów oraz prawidłowości postępowania według zdefiniowanej procedury,

b) umożliwienie dowolnym podmiotom składanie do Urzędu dokumentów elektronicznych z powiadomieniem właściwej osoby – elektroniczny urząd,

c) umożliwienie prowadzenia spraw z wykorzystaniem podpisu elektronicznego.

Zakończenie całego przedsięwzięcia przewidywane jest w lutym 2007 r. Przechowywanie dokumentów w formie elektronicznej powinno przyczynić się do zwiększenia bezpieczeństwa informacji niejawnych.

W związku z wejściem w życie nowych regulacji prawnych znacznie rozszerzających uprawnienia Komisji w zakresie wykonywania nadzoru nad rynkiem kapitałowym, konieczna stała się organizacja szkoleń i seminariów z zakresu obrotu instrumentami finansowymi, ze szczególnym naciskiem na temat przestępczości w zakresie publicznego obrotu papierami wartościowymi. Szkolenia organizowane przez Wydział Informacji i Edukacji są kierowane do policji, Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Śledczego, Polskiej Agencji Praso-

wej, Izby Domów Maklerskich, Stowarzyszenia Emitentów Giełdowych, jak również banków i innych podmiotów zajmujących się obrotem instrumentami finansowymi. W roku 2006 szkolenia były też organizowane dla szkół ponadgimnazjalnych.

Poszerzenie uprawnień Komisji w walce z przestępczością giełdową już przynosi wymierne efekty. Nie można jednak zauważyć, że istnieje kilka kwestii, które mogłyby jeszcze uskutecznić te działania. Przede wszystkim *insider trading* powinno być o wiele bardziej surowo karane, grzywny powinny być naprawdę dotkliwe. Z pewnością wydzielenie jednego wydziału sądu do orzekania w sprawach giełdowych, analogicznie do prokuratury, przyspieszyłoby postępowanie, a składy orzekające byłyby wyspecjalizowane w tej – jednak specyficznej i mało powszechnej – dziedzinie. Podobnie jest z kwestią przesłuchań w postępowaniu wyjaśniającym. Gdyby była odpowiedzialność karna za składanie fałszywych zeznań, prokuratura otrzymywałaby od Komisji bardziej wiarygodny materiał niż dotychczas.

W ramach CESR-Pol pod koniec 2005 r. została powołana stała grupa robocza Surveillance and Intelligence w celu usprawnienia i zintensyfikowania wymiany doświadczeń i informacji bieżących związanych z nadzorem nad rynkiem kapitałowym. Praca podgrupy w roku 2006 skupiła się między innymi na problemie przypadków wykorzystania informacji poufnej, które zaistniały na rynkach państw członkowskich, metodach pracy poszczególnych organów nadzoru i na wykorzystywanych środkach prawnych i faktycznych oraz nad wytycznymi dla uczestników rynku kapitałowego publikowanymi przez poszczególne organy nadzoru.

Jednak najskuteczniejszą metodą zapobiegania *insider trading* jest dbałość o zachowanie tajemnicy informacji poufnej. Duże firmy same opracowują metody zapobiegania naruszeń tajemnic firmy. Podstawą jest sumienne oznaczanie dokumentów zawierających informacje poufne oraz tworzenie i ciągłe uaktualnianie list insiderów. Firmy tworzą własne wewnętrzne regulacje prawne, które każdy pracownik jest obowiązany podpisać. Dotyczą one zasad ochrony informacji zastrze-

żonych i poufnych oraz tajemnicy przedsiębiorstwa spółki, wymieniają, czego mogą dotyczyć informacje poufne, kiedy stają się informacjami publicznymi, regulują tryb dokonywania transakcji przez pracowników i członków ich rodzin również po rozwiązaniu umowy o pracę oraz zawierają katalog zakazanych transakcji. Często pracownicy i ich rodziny nie mogą dokonywać transakcji jeszcze przez określony czas po opublikowaniu danej informacji, np. aż do upływu dnia pierwszej sesji giełdowej przypadającej po dniu podania informacji do wiadomości publicznej. Takie działania firm skutecznie ograniczają występowanie *insider trading*, a nawet jeśli dojdzie do działania przestępczego, pozwalają szybko i skutecznie ustalić sprawcę.

Na polskim rynku działa **Stowarzyszenie Emitentów Giełdowych**, organizacja samorządowa spółek notowanych na Giełdzie Papierów Wartościowych, do której przynależność jest dobrowolna. Stowarzyszenie istnieje od 1993 roku. **SEG jest członkiem Europejskiego Stowarzyszenia Spółek Notowanych (EALIC).** Przedstawiciel SEG jest stałym członkiem Komitetu Prawnego EALIC, gdzie opiniowane są projekty aktów prawnych przygotowywanych na forum Unii Europejskiej. Stowarzyszenie jest członkiem **Porozumienia dla Rozwoju Polskiego Rynku Kapitałowego** oraz członkiem **Rady Rynku Kapitałowego przy Ministerstwie Finansów**. Przedstawiciel Stowarzyszenia zasiada w **Radzie Giełdy Papierów Wartościowych w Warszawie SA. Członkami Zwyczajnymi** Stowarzyszenia są prezesi, członkowie zarządów spółek giełdowych, same spółki jako osoby prawne mają status Członków Wspierających. SEG umożliwia współdziałanie emitentów na rzecz rozwoju świadomości i odpowiedzialności obywatelskiej, ewolucji polskiego życia gospodarczego i społecznego w kierunku tworzenia gospodarki rynkowej oraz doskonalenia zdolności organizacyjnej jego członków, a także pogłębiania zrozumienia i współpracy między ludźmi. Stowarzyszenie podejmuje prace na rzecz rozwoju rynku kapitałowego przez działania edukacyjne, promujące i lobbingowe. Działa na rzecz integracji środowiska emitentów papierów wartościowych, podejmując organizację szkoleń i seminariów. Podstawową metodą pracy Stowarzyszenia jest przekazywanie regulatorom rynku oczekiwań emitentów dotyczących poprawy

funkcjonowania rynku papierów wartościowych, a także formułowanie propozycji zmian regulacji prawnych zwiększających atrakcyjność giełdy jako miejsca pozyskiwania kapitału dla podmiotów gospodarczych.

Inwestorzy indywidualni również sami zadbali o swoje interesy. 29 grudnia 1999 roku we Wrocławiu założyli Stowarzyszenie Inwestorów Indywidualnych, którego głównym zadaniem jest integracja środowiska inwestorskiego w celu ochrony interesów oraz szeroko rozumiana edukacja. Stowarzyszenie podejmuje również interwencje w imieniu i w interesie poszczególnych inwestorów, umożliwia zasięgnięcie porady prawnej, a także oferuje spółkom publicznym możliwość prowadzenia relacji inwestorskich w sposób korzystny zarówno dla firmy, jak i dla inwestorów. We wrześniu 2000 roku Stowarzyszenie zostało przyjęte do World Federation of Investors (WFIC), federacji skupiającej organizacje inwestorskie z całego świata, od października 2001 roku jest też członkiem europejskiej organizacji inwestorskiej Eurosharehol ders. Członkowie wymieniają się doświadczeniami zdobytymi na ich własnych rynkach oraz przedstawiają działania, które w ich przypadku się sprawdziły.

Statystyki

Tabela 1. Zawiadomienia o podejrzeniu popełnienia przestępstwa skierowane do prokuratury

	2000	2001	2002	2003	2004	2005	2006*
Ujawnienie tajemnicy zawodowej	–	1	1	1	1	–	3
Ujawnienie lub wykorzystanie informacji poufnej	10	6	12	9	5	7	3/11
Razem: insider trading	10	7	13	10	6	7	17
Razem: przestępstwa giełdowe	32	47	61	49	44	45	36

* Statystyka w okresie 1.01.–18.09.2006 r.

Źródło: www.kpwig.pl

Tabela 2. Liczba aktów oskarżenia skierowanych do sądów powszechnych

	2000	2001	2002	2003	2004	2005	2006*
Ujawnienie tajemnicy zawodowej	–	1	–	–	–	1	–
Ujawnienie lub wykorzystanie informacji poufnej	–	1	1	2	2	–	–
Razem: insider trading	–	2	1	2	2	1	–
Razem: przestępstwa giełdowe	3	10	12	16	14	10	6

* Statystyka w okresie 1.01.–18.09.2006 r.

Źródło: www.kpwig.pl

Można zauważyć, że w bieżącym roku Komisja zgłosiła największą liczbę zawiadomień w ciągu ostatnich 7 lat. Może to wynikać z faktu, iż posiada o wiele szersze uprawnienia i częściej udaje jej się ustalić podejrzanych. Po implementacji Market Abuse prokuratura dostaje bardziej rzetelne i dokładne dane. Należy też pamiętać, że część wykrytych czynów zabronionych podlega postępowaniu administracyjnemu, co pozwala szybciej i skuteczniej wymierzać kary za *insider trading*, pomijając długie postępowanie sądowe. Mimo tych wszystkich czynników liczba aktów oskarżenia nadal nie wzrasta. Połączenie dawnych komisji w jedną KNF nadzorującą cały rynek finansowy jeszcze bardziej uskuteczni wykrywanie *insider trading*, nie zmienia jednak faktu, że bardzo trudno je udowodnić.

Podsumowanie

Insider trading należy do kategorii przestępstw najcięższych na rynku giełdowym, a zarazem najtrudniejszych do ujawnienia i udowodnienia. Może być ścigane tylko *post factum*, co bardzo ogranicza możliwości ścigania. Bardzo trudno jest udowodnić ujawnienie informacji poufnej, zwłaszcza gdy *insider* pierwotny i wtórny nie są powiązani w żaden sposób formalny ani towarzyski. Insiderzy pierwotni nie pozostawiają po sobie żadnych śladów, gdyż zapoznają się z informacjami w sposób

jak najbardziej uprawniony i legalny. Insiderzy sami są uczestnikami obrotu instrumentami finansowymi i znają działania maskujące ich nielegalną działalność, działają pod innymi personaliami, tworząc tak zwane firmy „krzaki", korzystają z formy identyfikacji hasłem przy składaniu zleceń, więc bardzo trudno ustalić ich tożsamość. Są też sytuacje, w których tożsamość insidera jest chroniona przepisami prawnymi z innych dziedzin, tak jak w przypadku ochrony danych osobowych źródła informacji na tle prawa prasowego. Jeśli informacja poufna pojawi się na łamach prasy i dziennikarza obowiązuje tajemnica dziennikarska, spółka nie ma żadnych podejrzeń, a przy tym nie doszło do wykorzystania informacji, Komisja nie ma punktu zaczepienia. Szanse natrafienia na jakiś ślad są w takiej sytuacji znikome. Insiderzy – jeśli jednak uda się ich postawić przed sądem, dostają karę grzywny, która w porównaniu z zyskiem, nie jest dla nich wysoka; lub karę pozbawienia wolności w zawieszeniu. Jeśli już insider trafia do więzienia, to najczęściej za przestępstwa dokonane niejako „przy okazji" *insider trading*, a które udało się udowodnić: podrabianie podpisów, wyłudzanie kredytów, inne oszustwa. Długotrwałe postępowanie sprawia, że ewentualna kara jest odległa w czasie, a pokusa dużego i szybkiego zysku ogromna.

Bibliografia

R. Kuciński, *Przestępstwa giełdowe*, Warszawa 2000.

www.kpwig.gov.pl;

www.knf.gov.pl;

Ustawa o nadzorze nad rynkiem finansowym, Dz.U. z 2006 r. nr 157, poz. 1199.

Ustawa o obrocie instrumentami finansowymi, Dz.U. z 2005 r. nr 183, poz. 1538.

Pragniemy szczególnie podziękować za pomoc Naczelnikowi Wydziału Spraw Karnych Departamentu Nadzoru Rynku Komisji Papierów Wartościowych i Giełd, panu Marcinowi Pachuckiemu, który zwrócił naszą uwagę na niektóre problemy związane z insider trading.

Sebastian Skrzyszowski, Rafał Wawrzyńczyk

Metody prania pieniędzy w polskiej praktyce

Definicja prania pieniędzy

Kilka lat temu międzynarodowa organizacja zajmująca się zwalczaniem procederu prania pieniędzy FATF (Financial Action Task Force) oceniła, że rocznie w Polsce pierze się od 3 do 9 mld dolarów. Transparency International wymienia kwotę między 2,5 mld a 3 mld dolarów. Australijska Agenda ds. Przeciwdziałania Praniu Pieniędzy (AUSTRAC) oceniała natomiast, że w Polsce roczne zyski z przestępstw wynoszą ok. 19,7 mld dolarów[1]. Należy zaznaczyć, że środki, których nie udaje się zalegalizować w Polsce, są transferowane za granicę do krajów, w których proceder ten ma większe szanse na powodzenie.

Czym tak naprawdę jest „pranie pieniędzy"? Określenie to pojawiło się prawdopodobnie w latach 20. XX wieku w związku z działalnością chicagowskiej mafii, na której czele stał Alfonso Capone. W owym czasie obowiązywała w Stanach Zjednoczonych prohibicja, a mafia czerpała olbrzymie zyski z produkcji, przemytu i sprzedaży alkoholu. Nielegalne zyski były potem legalizowane poprzez mieszanie ich z dochodami z legalnych działalności, takich jak sklepy czy pralnie, stanowiących przykrywki dla członków organizacji. Do codziennych utargów dopisywano pewne sumy, aby stworzyć pozory, że środki finansowe pochodzą ze zgodnych z prawem źródeł[2].

---

[1] D. Tokarz, „Puls Biznesu" 03.02.2006.

[2] J.W. Wójcik, *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa 2002, s. 23.

Ogólnie rzecz biorąc, pranie pieniędzy jest to pewna sekwencja następujących po sobie zachowań, których celem jest nadanie pozorów legalności korzyściom pochodzącym z działalności przestępczej[3].

Definicja ta może jedynie stanowić kryterium pomocnicze w zrozumieniu, czym jest opisywany proceder. Wydaje się, że na gruncie polskim najlepszą, dotykającą istoty zagadnienia jest definicja zawarta w tytule ustawy z 16 listopada 2000 r. (Dz.U. z 2003r. nr 153, poz. 1501). Mówi ona, że pranie pieniędzy to wprowadzanie do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł.

Źródła nielegalne to wszelka działalność przestępcza, która przynosi zysk, np.:

- produkcja i handel narkotykami;
- handel bronią;
- kradzieże samochodów;
- handel żywym towarem i przemyt nielegalnych imigrantów;
- afery gospodarcze;
- korupcja;
- oszustwa finansowe;
- przestępstwa podatkowe;
- oszustwa giełdowe;
- handel nielegalnym oprogramowaniem oraz pirackimi płytami CD i DVD.

Źródła nieujawnione są związane z działalnością tzw. „szarej strefy", czyli prowadzenia działalności gospodarczej bez zezwolenia, bez płacenia podatków i innych obowiązkowych świadczeń na rzecz państwa[4].

Ściganie procederu prania pieniędzy, którego znamiona opisane są w art. 299 kk, nastręcza wielu trudności, gdyż zarówno w przypadku tego przestępstwa, jak i innych przestępstw gospodarczych praktycznie nie ma zastosowania tradycyjna taktyka śledztwa, która sprawdza się przy przestępstwach pospolitych.

---

[3] W. Filipowski, *Zwalczanie przestępczości zorganizowanej w aspekcie finansowym*, Kraków 2004, s. 61.

[4] Por. J. Grzywacz, *Pranie brudnych pieniędzy*, Warszawa 2005, s. 18–19, W. Jasiński, *Przeciw szarej strefie. Nowe zasady zapobiegania praniu pieniędzy*, Warszawa 2001, s. 13–30, J.W. Wójcik, *op. cit.*, s. 47–63.

W przypadku prania pieniędzy kierunek wykrywania biegnie tu od sprawcy do przestępstwa, odwrotnie aniżeli w tradycyjnym śledztwie czy dochodzeniu. Organy ścigania bardzo często mają przed sobą osobę, w stosunku do której istnieją oczywiste przesłanki uprawiania powyższego procederu, np. na podstawie informacji uzyskanych z wywiadu finansowego, ale nie są w stanie udowodnić jej popełnienia przestępstwa[5].

Z tego też powodu tak ważną kwestią jest, aby takimi sprawami zajmowali się policjanci czy prokuratorzy posiadający specjalistyczną wiedzę na temat finansów, prawa gospodarczego czy podatkowego, bo bez tej wiedzy będą bezradni.

Należy jeszcze wspomnieć, że w przypadku metodyki zwalczania przestępstw gospodarczych, a do takich większość specjalistów zajmujących się tą tematyką zalicza pranie pieniędzy, mamy do czynienia z bardzo skomplikowanym nieraz *modus operandi* sprawców. Dlatego przy próbie wyjaśniania takich spraw kolosalną rolę odgrywa właściwie przeprowadzona analiza kryminalna[6].

W Polsce zwalczanie procederu prania pieniędzy należy do kompetencji Policji, Agencji Bezpieczeństwa Wewnętrznego, a w przyszłości ma się tym zajmować także Centralne Biuro Antykorupcyjne.

Nie można również zapomnieć o działalności powołanego wspomnianą już Ustawą o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu Generalnego Inspektora Informacji Finansowej w randze podsekretarza stanu w Ministerstwie Finansów oraz podległego mu Departamentu Informacji Finansowej.

Nie sposób jednak nie zauważyć, że mimo mnogości podmiotów zajmujących się zwalczaniem opisywanego procederu rezultaty ich działań można określić raczej jako mizerne.

Dlaczego tak się dzieje?

---

[5] Por. H. Kołecki, *Niemoc polskiej nauki kryminalistyki wobec problematyki współczesnej zorganizowanej przestępczości gospodarczej w Polsce*, „Przegląd Policyjny" nr 1(69), s. 22–42.

[6] *Ibidem*.

Znamienne może być tu zdarzenie, które miało miejsce jakiś czas temu w Krakowie, gdy do jednego z banków zgłosiły się dwie osoby: obywatel Rosji i obywatel Polski. Rosjanin założył konto, a Polaka ustanowił osobą uprawnioną do korzystania z niego. Po pewnym czasie na konto wpłynęła pewna kwota, wyższa niż 15 tys. euro podlegające zgłoszeniu do GIIF, którą bezzwłocznie wypłacił upoważniony do tego Polak. Transakcja ta nie spotkała się z najmniejszą reakcją banku. Sytuacja ta powtórzyła się jeszcze raz. Tym razem zareagował na nią dyrektor ds. bezpieczeństwa tego banku, choć nie musiał tego robić, bo takie sprawy nie należą do bezpośredniej sfery jego kompetencji. Zawiadomił on prokuraturę, a ta po pewnym czasie umorzyła postępowanie.

Mimo starań nie znaleźliśmy ani jednego prawomocnego wyroku skazującego za przestępstwo z art. 299 kk, choć nie wykluczamy, że gdzieś już taki się pojawił. Dlatego gdy w dalszej części pracy będziemy się posługiwać przykładami, to nie będą to przykłady spraw zakończonych wyrokami skazującymi, a jedynie spraw, w których ciążą lub ciążyły na osobach zarzuty.

Etapy prania brudnych pieniędzy

Analizowane przypadki prania pieniędzy pozwalają na wyróżnienie kilku etapów tego procesu oraz charakterystycznych dla niego technik. W literaturze przedmiotu najczęściej przyjmuje się trzystopniowy podział prania pieniędzy, jednak wielu autorów wskazuje, iż stadium pierwsze może być poprzedzone przygotowaniem całego procederu, tzw. fazą wstępną[7]. Polega ona na wywozie gotówki z miejsca prowadzenia działalności przestępczej do innego miasta, regionu, w celu utrudnienia organom ścigania powiązania gotówki z danym przestępstwem (bądź całą swoją działalnością) lub do innego kraju dającego lepsze możliwości dla przedsięwzięcia („kraje działalności kryminalnej" *criminal activity countries* i „kraje prania" *laundering countries*[8]).

---

[7] Por. W. Jasiński, *op. cit.,* s. 65–68, J.W. Wójcik, *op. cit.*, s. 94–96, W. Filipowski, *op. cit.*, s. 61–74.

[8] K. Wąsowski, *Pranie brudnych pieniędzy*, Warszawa 2001, s. 25.

1) **Umiejscowienie** (lokowanie, *placement*)

Pierwszy z właściwych etapów prania pieniędzy polega na fizycznym wprowadzeniu nielegalnie uzyskanych środków finansowych do obrotu finansowego[9]. Jest to moment uważany za najbardziej krytyczny dla całego procederu, gdyż daje największe możliwości wykrycia pieniędzy, a ponadto przejęcia wartości[10] ze względu na cechy charakterystyczne dla tego stadium: przedmiot prania na tym etapie pochodzi bezpośrednio z przestępstwa, występuje przeważnie w postaci gotówki.

Przed przejściem do omówienia poszczególnych metod tej fazy procederu należy zaznaczyć, iż na techniki prania pieniędzy składają się zarówno zachowania o legalnym charakterze (wpłaty gotówkowe, transfery środków pieniężnych, zamiana gotówki na instrumenty finansowe, zakup dóbr o znacznej wartości *etc.*), jak i nielegalne (korupcja, nakłanianie do przestępstwa, podrabianie dokumentów i inne przestępstwa towarzyszące – satelitarne[11]).

Przykładowe techniki wykorzystywane w fazie umiejscawiania

Wpłaty na rachunek bankowy. Wpłaty dokonywane są poniżej limitu wymagającego przeprowadzenia czynności identyfikacyjnych i rejestracyjnych. Wykorzystywany jest jeden lub wiele rachunków (później z reguły środki są przelewane na jedno konto zbiorcze), tak własnych, jak innych podmiotów – często fikcyjnych. W przypadku rozbicia kwoty na niższe i dokonywaniu wielu wpłat technikę tę nazywa się *structuringiem*. Ze względu na prostotę operacji mimo wielu wad jest ona bardzo popularna. Przede wszystkim pozostawia ślady audytorskie w dokumentacji bankowej[12]. Przestępcy, chcąc zwiększyć prawdopodobieństwo sukcesu, starają się pozyskać pracowników banków (przez łapownictwo, wymuszenia, szantaż), otwierają rachunki w wielu bankach często z wykorzystaniem fałszy-

[9] *Ibidem*, s.12–13.

[10] W. Filipowski, *op. cit.*, s. 64.

[11] Szerzej o przestępstwach towarzyszących przestępczości gospodarczej: H. Kołecki, *op. cit.*, s. 31–34.

[12] W. Jasiński, *op. cit.*, s. 76.

wych dokumentów, z pomocą figurantów czy przedsiębiorstw fikcyjnych (aby uniknąć kontaktu, wykorzystują sejfy nocne[13]).

Wykorzystywanie wielu takich figurantów do otwierania rachunków bankowych, a przede wszystkim do wpłacania kwot poniżej limitu jest jedną z form *smerfingu.* Inna forma *smerfingu* odbywa się przez zorganizowany zakup surogatów pieniężnych (czeków pieniężnych, podróżnych) przez grupy wynajętych *smerfów*[14]. Należy zaznaczyć, że *smerfing* może być wykorzystywany także w transakcjach z wykorzystaniem innych instytucji, takich jak kantory, kasyna czy poczta. Istnieje także towarowa forma *smerfingu.* Polega ona na zakupie towarów luksusowych za granicą (np. przez studentów, bezrobotnych), następnie towary wysyłane są do krajów pochodzenia brudnych pieniędzy, gdzie są sprzedawane po stosownie obniżonej cenie, a zyski zostają wpłacone na rachunki bankowe jako pochodzące z działalności handlowej[15]. Podobnie jest z wielokrotną zamianą walut czy wymianą banknotów na większy nominał (*refining*).

Mieszanie (*blending*), czyli łączenie brudnej gotówki z dochodami z legalnej działalności gospodarczej. Ta popularna technika wykorzystywana jest także w fazie maskowania i integracji. Podmioty gospodarcze wykorzystywane w tej działalności należą do branży o intensywnym i zmiennym przepływie gotówki (trudnych do oszacowania obrotach). Szczególnie sprawdzają się tu takie podmioty jak restauracje, bary, puby, dyskoteki, hotele, motele, solaria, kina, pralnie chemiczne, lombardy, kasyna, kafejki internetowe oraz inne podmioty o działalności przede wszystkim usługowej (przy działalności produkcyjnej podmiot musi wykazywać jakąkolwiek produkcję)[16].

Wiele czynników składa się na powodzenie tej techniki:

- podmiot taki prowadzi działalność nastawioną na osiąganie zysków (czym tłumaczy pochodzenie pieniędzy wpływających na rachunki bankowe);

[13] P. Guberow, *Techniki prania brudnych pieniędzy*, [w:] J. Grzywacz, *Pranie brudnych pieniędzy*, Warszawa 2005, s. 27.

[14] *Ibidem*.

[15] W. Filipowski, *op. cit.*, s. 65.

[16] *Ibidem*, s. 67.

- trudności w udowodnieniu prania pieniędzy tą metodą (mienie zakupione za brudne pieniądze przez to przedsiębiorstwo jest jego własnością);
- przestępca generujący brudne pieniądze ma stałą nad nimi kontrolę[17];
- ponadto taka mieszalnia daje członkom grupy możliwość legalnego zatrudnienia i miejsce do odbywania spotkań[18].

W tej technice właściciel pranych pieniędzy może być jednocześnie właścicielem podmiotu gospodarczego służącego do prania, może przejąć legalną firmę lub zawrzeć z jej właścicielem stosowną umowę[19]. Nie tylko za pomocą pieniędzy, ale także poprzez szantaż czy wymuszenie.

Umiejscawianiu mogą służyć inne metody. Duże możliwości dają **kasyna i systemy gier losowych**. Gracz zakupuje żetony w kasynie, następnie zwraca je z dyspozycją przelania należności na rachunek bankowy lub wypłaca pieniądze w postaci czeków gotówkowych. Chętnie odkupywane są również prawdziwe wygrane (kupony).

Podobnie **przetargi** tworzą doskonałe możliwości. Osoba składa ofertę niemającą szansy na wygranie przetargu. Gotówką wpłaca wadium, a po przetargu pieniądze zostają zwrócone na wskazany rachunek bankowy.

2) **Maskowanie** (warstwowanie, *layering*)

Etap ten ma na celu oddzielenie nielegalnych środków finansowych od ich pierwotnego źródła oraz ukrycie tożsamości posiadacza, a tym samym zmylenie organów kontrolnych. Warstwowanie odbywa się przez tworzenie całego kompleksu skomplikowanych transakcji finansowych, które powodują zagmatwanie ścieżki dokumentacyjnej i urywanie śladów rachunkowych[20].

---

[17] W. Jasiński, *op. cit.*, s. 72–73.

[18] W. Filipowski, *op. cit.*, s. 67.

[19] W. Jasiński, *op. cit.*, s. 73.

[20] J.W. Wójcik, *op. cit.*, s. 94.

Przykładowe techniki[21]:

Serie przelewów pieniężnych. Dla lepszego efektu maskowania:

- dzieli się operacje na mniejsze części;
- wykorzystuje się międzynarodowe przelewy do krajów o niewystarczających regulacjach zapobiegających praniu pieniędzy, a o restrykcyjnie przestrzeganej tajemnicy bankowej;
- korzystanie z pomocy ludzi profesjonalnie zajmujących się tworzeniem spółek i kont w takich krajach (w tym prawników);
- wykupywanie spółek w złej sytuacji ekonomicznej dla ich kont;
- wykorzystywanie figurantów (słupów) przy tworzeniu fikcyjnych podmiotów gospodarczych;
- posługiwanie się operacjami elektronicznymi (zalety: w znacznym stopniu zapewniają anonimowość, astronomiczna liczba takich operacji na całym świecie, szybkość);
- przelewy na nieistniejące konta w bankach zagranicznych dla nieistniejących klientów (wyjaśnianie przez bank takiej sytuacji trwa nawet do kilku tygodni, a w międzyczasie fundusze powracają).

Konwersja – zamiana środków pieniężnych na rzeczy ruchome (zazwyczaj luksusowe dobra), ale przede wszystkim na instrumenty finansowe (akcje, czeki, certyfikaty depozytowe). Aby osiągnąć zamierzony cel, takie transakcje powinny być powtarzane wielokrotnie[22].

3) **Integracja** (legitymizacja, *integration*)

Stadium mające na celu znalezienie wyjaśnienia, usprawiedliwienia (oczywiście prawnie dopuszczalnego) posiadanych środków w legalnym obrocie gospodarczym.

Przykładowe metody[23]:

Zakup i odsprzedaż dóbr, tj. nieruchomości i ruchomości znacznej wartości, po cenie zaniżonej w umowie (pozostała kwota płacona jest „pod stołem"). Zysk z odsprzedaży stanowi prawne i ekonomicz-

[21] P. Guberow, *op. cit.*, s. 29–30.

[22] W. Filipowski, *op. cit.*, s. 70.

[23] P. Guberow, *op. cit.*, s. 31–32.

ne uzasadnienie posiadanych wartości. Na podobnej zasadzie przy transakcjach handlowych może dojść do **zaniżania cen na fakturach**. W tej metodzie dochodzi do nałożenia się fazy umiejscawiania oraz fazy integracji (z pominięciem fazy maskowania).

Zaciągnięcie kredytu, a następnie jego spłata. W metodzie tej przestępcy wykorzystują podmioty gospodarcze znajdujące się pod ich kontrolą do zapłaty legalnie zaciągniętego kredytu oczywiście brudnymi pieniędzmi (często wykorzystywana jest też druga fikcyjna bądź zależna zagraniczna firma lub bank o wątpliwej reputacji z kraju będącego oazą podatkową, która udziela pierwszej firmie kredytu na spłatę).

Udzielanie pożyczek na atrakcyjnych warunkach legalnym firmom (niskie oprocentowanie, prolongata spłat, wykorzystywanie ciężkiej sytuacji firm).

Akredytywy. W przypadku spełnienia wszystkich warunków i dostarczenia niezbędnych dokumentów bank jest zobowiązany do wypłacenia pieniędzy bez obowiązku badania, czy i jaki towar został rozładowany.

Ceny transferowe (*transfer pricing*) – technika polegająca na świadczeniu sobie wzajemnych usług (fikcyjnych albo faktycznych) lub sprzedaży przedmiotów po cenach niemających ekonomicznego uzasadnienia przez całe „łańcuszki" spółek przykrywek[24].

Polska praktyka prania pieniędzy

Piorący jubilerzy

We wrześniu 2001 r. bydgoski sąd aresztował na wniosek prokuratury czterech tamtejszych jubilerów: Zbigniewa Z., Janusza S., Czesława S. i Piotra P. pod zarzutem przestępstwa z art. 299 kk, czyli prania pieniędzy, w tym przypadku pochodzących z handlu wyrobami jubilerskimi.

Kilka miesięcy wcześniej policjanci z CBŚ zaczęli przyglądać się ich działalności, gdyż podejrzane wydały się im przeprowadzone przez jubilerów transakcje warte setki tysięcy złotych, za pośrednictwem prowincjonalnego Banku Spółdzielczego w Lnianie w woj. kujawsko-pomorskim.

---

[24] W. Filipowski, *op. cit.*, s. 72.

O współudział w procederze prania pieniędzy podejrzewane są także pracownice banku w Lnianie: kierowniczka Małgorzata D., księgowa Danuta B. i kasjerka Regina R.[25]

Lewa kasa ze Wschodu (*structuring*)

Witold K. i Michał K. (ojciec z synem) prowadzili pod Warszawą firmę zajmującą się produkcją opakowań z tworzyw sztucznych. Ich kontrahenci z Rosji, godząc się na podwyższenie ceny kupna opakowań, zażyczyli sobie wpisywania niższych sum na fakturach. Panowie K. uzyskiwali dodatkowe nieopodatkowane dochody, które były transferowane za pomocą kont w bankach w Moskwie, Rydze i w niektórych stanach USA, aby wreszcie trafić na konta spokrewnionych z nimi Stefanii K. i Anny D. Na polskie konta dokonano kilkadziesiąt przelewów na kwotę ponad miliona dolarów.

Proceder ten wyszedł na jaw dzięki zawiadomieniu przez bank Generalnego Inspektora Informacji Finansowej. Kobietom postawiony został zarzut prania pieniędzy[26].

Hydrobudowa

23 lutego 2006 Sąd Okręgowy w Gdańsku skierował do ponownego rozpoznania sprawę 65-letniego Wiesława O. skazanego na trzy lata więzienia i jego pracownika Henryka O. skazanego na dwa lata za pranie brudnych pieniędzy. Sąd pierwszej instancji w uchylonym ze względu na zbyt lakoniczne uzasadnienie wyroku uznał, że mężczyźni próbowali zalegalizować pieniądze wyłudzone od inwestora budującego hipermarket.

Firma Wiesława O. Hydrobudowa SA budowała w Gdańsku centrum handlowe „Manhattan". Dyrektor budowy podpisał fikcyjną umowę na dodatkowe zbrojenia, wartą 3 mln zł. Umowę podpisała firma Inter-Hermes, która następnie zleciła wykonawstwo firmie Madex, ta następnie firmie Mobimex. Oczywiście żadnych wzmocnień fundamentów

[25] M. Kowalski, *Wielka pralnia*, „Gazeta w Toruniu" nr 228, 29-30.09.2001, cyt. za: A. Zientkiewicz, Ł. Leja, *Prawdziwe afery z życia gospodarczego*, [w:] J. Grzywacz, *op. cit.,* s. 107–108.

[26] *Rodzinne pranie*, „Gazeta Wyborcza" 17.09.2003, cyt. za: A. Zientkiewicz, Ł. Leja, *op. cit.*, s. 106–107.

nie było. Hydrobudowa przelała pierwszą ratę fikcyjnej należności na konto Inter-Hermes (970 tys. zł), ta zaś przelała 800 tys. na konto firmy Madex, a firma przelała 400 tys. na konto Mobimexu. Transakcja ta wydała się podejrzana GIIF i ten zawiadomił prokuraturę. Okazało się, że Mobimex to jednoosobowa firma handlująca złomem, a w rzeczywistości pralnia pieniędzy[27].

Gellwe

Grudzień 2003. Prokuratura Okręgowa w Katowicach zarzuciła prezesowi Gellwe oszustwa i pranie brudnych pieniędzy. Prokuratura skierowała do Sądu Rejonowego w Krakowie oskarżenie przeciwko Wiesławowi W., prezesowi właścicielowi spółki Gellwe, producenta ciast i deserów w proszku. Oskarżenie obejmuje zarzuty wyłudzenia podatku VAT na kwotę 1,5 mln zł, wyprowadzenie ze spółki 2,4 mln zł oraz pranie brudnych pieniędzy[28].

Międzynarodowe pranie w Bydgoszczy

Niemieccy prokuratorzy nabrali podejrzeń, że w Bydgoszczy prane są pieniądze przestępczej szajki. Poprosili bydgoskich śledczych, aby sprawdzili konto jednego z bydgoszczan. Okazało się, że właściciel bankowego rachunku regularnie co kilka tygodni wypłacał z niego po 12 tys. euro. Przesłuchiwany zaczął zeznawać. Wyznał, że jest podstawiony i opowiedział wszystko, co wie na temat transferów pieniędzy.

Funkcjonariusze na polecenie prokuratorów odszukali kolejne osoby, które cyklicznie wypłacały ze swoich kont nadsyłane z Niemiec pieniądze. Euro trafiało do banków w Bydgoszczy oraz Trójmieście. Od stycznia 2002 do września 2004 r. na bydgoskie konta wpłynęło 200 tys. euro. Pieniądze były wyłudzane z kont zamożnych niemieckich adwokatów i lekarzy. Następnie trafiały na konta podstawionych ludzi, którzy znali tylko swoich werbowników. Podstawione osoby za przekazywanie pieniędzy werbownikom otrzymywały od 500 do 2 tys. zł. Do sądu wpłynął

[27] *Hydrobudowa od nowa*, „Gazeta Wyborcza" 24.02.2006, *Ławnik nazbyt lakoniczny*, „Dziennik Bałtycki" 24.02.2006.

[28] G. Zięba, *Prezes stanie przed sądem*, „Puls Biznesu" 10.12.2003, *Kolejne zarzuty*, „Puls Biznesu" 25.02.2004.

stwa skarbowe i działanie w zorganizowanej grupie przestępczej. Akt oskarżenia wobec tej grupy zawiera 180 tomów. Szacowane szkody Skarbu Państwa z tytułu podatku VAT i akcyzy to co najmniej 218 mln zł. W grupie oskarżonych jest Piotr K., sprawca kierowniczy całej działalności grupy, która produkowała olej napędowy kiepskiej jakości, rozprowadzany później wśród indywidualnych odbiorców, m.in. na stacjach benzynowych. Praniem brudnych pieniędzy zajmowano się w krakowskiej firmie Techlex sp. z o.o., której właściciel Jarosław M. także jest oskarżonym w tej sprawie. Udowodniono, że przez konta bankowe spółki przepływały pieniądze z nielegalnych paliwowych transakcji[30].

PZU

Ze śledztwa „Rzeczpospolitej" ujawnionego we wrześniu 2004 r. wynika, że przez kilkanaście lat trzej kolejni prezesi PZU gromadzili miliony złotych na tajnych kontach w raju podatkowym. Pieniądze były prowizją za umowy reasekuracyjne. Wypłacał je brytyjski broker, który współpracował z państwowym gigantem ubezpieczeniowym.

Rok wcześniej „Rzeczpospolita" ujawniła, że na tajnych kontach w bankach na wyspie Jersey znajdują się miliony złotych wyprowadzonych z PZU i PZU Życie przez Grzegorza W. i Władysława J. „Rzeczpospolita" dotarła do dokumentów zarejestrowanej na wyspie Jersey firmy Warren Trustees Group, która zarządza dyskretnymi funduszami powierniczymi. Jej działalność polega m.in. na zakładaniu spółek, których prawdziwi właściciele pozostają w ukryciu. Jest to sposób wykorzystywany często do zacierania śladów prania pieniędzy przez skorumpowanych urzędników i przestępców. Wśród klientów firmy widnieją nazwiska m.in. obywateli Turcji, RPA, Hiszpanii, Mołdawii, Kuwejtu, a także Polski. W tych dokumentach gazeta znalazła dowody korupcji kolejnych szefów PZU: Krzysztofa J. (1990–1993), Romana F. (1993–1996) oraz Władysława J. (1998–2001). Zgromadzili oni na tajnych kontach miliony złotych. Pieniądze pochodziły z prowizji za zawarcie

[30] Opracowano na podstawie informacji zawartych w bazie internetowej *ISI Emerging Markets Polska*, www.securities.com.

akt oskarżenia przeciwko sześciu mężczyznom, którzy organizowali pralnię po stronie polskiej. Wszyscy są dobrze znani policji, przyznali się do winy. Strona niemiecka cały czas pracuje nad szefami gangu za Odrą[29].

Afera paliwowa

Sprawa mafii paliwowej jest jedną z największych, jeśli nie największą aferą w III Rzeczpospolitej. Ma kilkadziesiąt wątków i doskonale ukazuje niejasne, a wręcz korupcyjne układy między nieuczciwymi biznesmenami, niektórymi politykami i funkcjonariuszami służb specjalnych. Coraz to nowsze dowody wskazują na to, że członkowie grup przestępczych przez lata mogli czuć się bezkarnie i bez przeszkód prowadzić swoje interesy, narażając Skarb Państwa na gigantyczne straty. Jednak na potrzeby tego opracowania pragniemy się skupić na wątkach związanych z podejrzeniem o pranie pieniędzy, które czekają na wyjaśnienie przed krakowskim Sądem.

W kwietniu 2005 przed Sądem Okręgowym w Krakowie stanęło 18 osób oskarżonych o pranie pieniędzy, przestępstwa paliwowe i wyłudzanie akcyzy oraz działanie w zorganizowanej grupie przestępczej. Pierwszy akt oskarżenia dotyczy wyprania prawie 200 mln zł i wyłudzeń podatkowych na kwotę 280 mln zł.

Na ławie oskarżonych zasiadło 18 osób, w tym dwaj baronowie paliwowi: Jan B. (pierwszy przełamał zmowę milczenia i wyświetlił kulisy działania nielegalnego rynku paliwowego w Polsce) i Zdzisław M., właściciele największego prywatnego importera paliw – spółki BGM oraz boss lokalnej mafii paliwowej na Śląsku – Artur K. Zabrakło tylko trzeciego z trójki właścicieli BGM, Arkadiusza G., wobec którego śledztwo wciąż się toczyło. Prokuratura zarzuca mu m.in. współorganizowanie grupy, która zasiadła na ławie oskarżonych. Akt oskarżenia liczy ponad 600 stron. Prokuratura postawiła w nim blisko 60 zarzutów.

22 września Prokuratura Apelacyjna w Krakowie skierowała do sądu kolejny akt oskarżenia w aferze paliwowej. Tym razem oskarżonych jest jedenaście osób. Oskarżonym zarzuca się m.in.: pranie brudnych pieniędzy, oszustwa finansowe przeciwko Skarbowi Państwa, przestęp-

[29] *Szajka posiedzi za duże pranie*, „Gazeta Wyborcza" 06.01.2006.

kontraktów z brytyjskim brokerem ubezpieczeniowym Robertem B., z którym PZU blisko współpracował przez całe lata 90. Według obowiązujących wówczas przepisów posiadanie takiego konta za granicą było nielegalne. Dokumenty Warren Trustees Group są także w posiadaniu policji Jersey, która prowadzi dochodzenie w sprawie podejrzenia prania pieniędzy przez tę firmę.

Sprawa PZU to jedna z największych afer gospodarczych ostatnich lat. Grzegorz W. został oskarżony o spowodowanie w majątku PZU Życie strat przekraczających 170 mln zł. Ale proces zakończył się skandalem, okazało się bowiem, że ekspertyza biegłej, będąca podstawą oskarżenia, została sporządzona wbrew zasadom księgowości. Sąd zwolnił byłego szefa PZU Życie z aresztu, a sprawę zwrócił do prokuratury.

Wciąż toczy się proces byłego szefa PZU Władysława J., oskarżonego m.in. o to, że nie dołożył należytej staranności, podpisując umowy na zakup nieruchomości. Zdaniem prokuratury PZU przepłaciło przez to ponad 10 mln zł. Krzysztof J. i Roman F. oraz Krzysztof B., wówczas wiceprezes PZU, założyli na Jersey za pośrednictwem Warren Trustees pierwsze firmy już na początku lat 90. Ich działalność miała być zachowana w całkowitej tajemnicy. W dokumentach najczęściej pojawiają się nazwy Narai i European Risk Management. Na ich konta wpływały pieniądze. Rachunki były prowadzone w różnych walutach. Szefowie PZU korzystali z nich dzięki kartom kredytowym wystawionym przez banki działające na Jersey. Na kartach nie było nazwiska właściciela. Limit wydatków przekraczał 30 tys. złotych. Gromadzone na tajnych kontach aktywa szybko rosły. Już w 1995 r. na koncie Narai Ltd. znajdowała się równowartość ponad dwóch milionów złotych w markach niemieckich. Miliony znalazły się też na kontach innych firm. Pieniądze te były inwestowane. Za około 200 tys. złotych European Risk przejął udziały w warszawskiej firmie z branży ubezpieczeniowej Profibiz Krzysztofa B. i towarzystwie ubezpieczeniowym Kupala na Białorusi. W połowie lat 90. do grona „inwestorów" dołączył Władysław J. Z podsumowań znajdujących się w dokumentach wynika, że w 2000 r. należący do niego Portland Trust dysponował ponad 20 milionami złotych. Zarządzanie

fortunami odbywało się w całkowitej konspiracji. Właściciele kont nie pojawiali się na Jersey. Ważne dokumenty były przesyłane kurierem do hoteli w całej Europie, w których zatrzymywali się pod różnymi pretekstami. Takie przesyłki dla Krzysztofa J. dostał m.in. hotel Marriott w Wiedniu.

Ze śledztwa „Rzeczypospolitej" wynika, że szefów PZU skontaktował z Warren Trustees brytyjski broker reasekuracyjny Robert B. Jego majątkiem zarządzają dyrektorzy Warren Trustees. Robert B. w latach 90. był głównym brokerem reasekuracyjnym, z którym współpracowało PZU. Był on pośrednikiem w umowach reasekuracyjnych między PZU a zachodnimi firmami, które ubezpieczały działalność polskiego giganta. W Polsce prowadził interesy jeszcze w latach 80. Prawdopodobnie wtedy zetknął się z ówczesnym kierownikiem zespołu umów w biurze reasekuracji w państwowej Warcie. W peerelowskim systemie ubezpieczeniowym to właśnie Warta współpracowała z zagranicznymi kontrahentami. Robert B. pośredniczył w zawarciu szeregu umów reasekuracyjnych PZU z zagranicznymi firmami. Na każdej zarabiał miliony. W latach 90. Robert B. był nawet doradcą zarządu PZU w sprawach reasekuracji. Wszczęte przez polską prokuraturę w 2001 r. śledztwa w sprawie nadużyć w PZU i PZU Życie zaczęły zataczać coraz szersze kręgi. Latem został aresztowany Grzegorz W. W 2002 r. do aresztu trafił Władysław J. Prowadząca dochodzenie w sprawie Grzegorza W. prokuratura wpadła na ślad prania pieniędzy na wyspie Jersey. Śledztwo wykazało, że przelał on ponad trzy miliony złotych na tajne konto w banku Barclays, założone dla niego przez ludzi z Warren Trustees. Zanim prokuratura wystąpiła o zablokowanie rachunku, żona byłego szefa PZU Życie przelała pieniądze na inne konto. Prokuratura twierdzi, że w tej sprawie władze Jersey nie chciały z nią współpracować. Ale tej wersji nie potwierdza były urzędnik Generalnego Inspektora Informacji Finansowej zajmujący się sprawą.

Siedzibą Warren Trustees jest niepozorna kamienica w zabytkowym centrum St. Helier, stolicy wyspy Jersey. W wynajętym na drugim piętrze biurze 14 osób zarządza aktywami około setki firm. Prokuratura nie wpadła natomiast na ślad zagranicznego majątku Władysława J.

Niemal przez rok od publikacji „Rzeczypospolitej" o tej sprawie prokuraturze nie udało się zablokować jego kont. Rachunkiem w banku na Jersey dysponował również jeden z braci W., współoskarżonych w tej samej sprawie. Na koncie znajduje się pół miliona dolarów[31].

[31] Opracowanie na podstawie informacji zawartych w bazie internetowej *ISI Emerging Markets Polska*, www.securities.com.

Kontrola lojalności personelu

Justyna Śliwoń

Z badań nad systemem kontroli lojalności pracowników

Nowoczesne technologie umożliwiają dzisiaj pracodawcy szeroką kontrolę przedsiębiorstwa, w szczególności pracowników. Ich czasu, sposobu oraz jakości pracy. Kontrola może być prowadzona głównie przez monitoring. Pamiętać trzeba jednak, że wszelkie formy monitorowania pracowników stanowią przetwarzanie danych osobowych w rozumieniu Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r., nr 101, poz. 926 z późn. zm.). Pracodawca jest zobowiązany do odpowiedniego zabezpieczenia uzyskanych dzięki monitoringowi informacji o pracownikach oraz do zapewnienia ku temu właściwych warunków technicznych i organizacyjnych.

Pracodawca może też kontrolować pracowników poprzez przeszukanie. Jest ono stosowane w szczególności w większych zakładach produkcyjnych, hipermarketach, hurtowniach. Przeszukaniu mogą być poddane ubrania i rzeczy osobiste pracownika. Jednak aby działanie pracodawcy było zgodne z prawem i nie naruszało dóbr osobistych pracownika, musi on wykazać, że jego interes prawny ma większą wartość niż dobro pracownika. Przeszukanie może być dokonane po uprzednim poinformowaniu osób zatrudnionych o możliwości takiej kontroli i tylko w celu ochrony ważnego interesu pracodawcy. Stanowisko to wyraził Sąd Najwyższy w wyroku z dnia 13 kwietnia 1972 r. I PR 153/72; OSNC z 1972 r., nr 10, poz. 184), uznając, iż „stosowane szeroko w ramach przepisów regulaminów pracy lub ustalonych zwyczajów przeszukiwanie członków załogi w celu zapobiegania wynoszeniu mienia zakładów pracy jest zgodne z prawem i nie narusza dóbr osobistych pracowników wówczas, gdy pracownicy zostali uprzedzeni o możności stosowania tego rodzaju kontroli w celu ochrony mienia i gdy kontrola ta jest wykonywana w porozumieniu z przedstawicielstwem załogi

w sposób niepozostający w sprzeczności ze swym społeczno-gospodarczym przeznaczeniem lub zasadami współżycia społecznego".

Następną możliwością jest dopuszczalna kontrola e-maili i aktywności w Internecie. W rozumieniu art. 23 k.c. jednym z dóbr osobistych jest tajemnica korespondencji, a te pracodawca w myśl art. 11 k.c. ma obowiązek uszanować. Zachodzi więc wykluczanie się dobra osobistego pracownika i ochrony tajemnicy handlowej pracodawcy. W każdym przypadku pracodawca powinien zbadać dopuszczalność monitorowania komputerów zakładowych.

Monitoring, przeszukanie i przegląd komputerów zakładowych są jednymi z najczęściej stosowanych środków. Współczesna technika stwarza pracodawcy możliwość korzystania z coraz większej liczby urządzeń przeznaczonych do kontroli. Powinien on zawsze pamiętać, iż każde jego działanie musi być zgodne z prawem, a w szczególności z Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (tj. Dz.U. z 1998 r., nr 21, poz. 94 z późn. zm.); Ustawą z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. nr 16, poz. 93 z późn. zm.); Ustawą z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (tj. Dz.U. z 2002 r. nr 147, poz. 1231 z późn. zm.); Ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz.U. z 2003 r. nr 153, poz. 1503 z późn. zm.); Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.) oraz Rozporządzeniem ministra pracy i polityki socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U. nr 148, poz. 973).

Cele badania

Celem badania było sprawdzenie, jaki wpływ na lojalność pracowników mają monitoring, podsłuch, przeszukanie oraz co o działaniach służących kontroli sądzą pracownicy.

Pod uwagę zostało wzięte to, czy pracownicy chcą takiej kontroli, czy zgadzają się na jej zastosowanie, czy jest ona w ich opinii potrzebna i skuteczna, a także jaki ma ona wpływ na wzajemne relacje między pracownikami.

Sprawdzony został stopień oddziaływania środków kontroli na sferę prywatności pracownika. To kiedy, według pracowników, kontrola staje się nadmierna i uciążliwa, a w jakich przypadkach staje się skuteczna.

Badanie miało również pokazać, czy monitoring lub podsłuch stosowane na szeroką skalę mogą mieć wpływ na zaufanie do pracodawcy, a także na sam komfort pracy.

Przeprowadzone doświadczenie za swój cel przyjęło także poddanie kontroli jakość stosowanych środków oraz sprawdzenie, czy przynoszą one pracodawcy zamierzone efekty.

Metoda

W badaniu zastosowano metodę ankiety przeprowadzanej na 50 pracownikach firm oraz przedsiębiorstw, zarówno prywatnych, jak i państwowych. Badane zakłady pracy zatrudniały od 20 do 400 pracowników obydwu płci i w zróżnicowanym wieku.

Ankieta zawierała 20 pytań, z czego pierwsza jej część pozwalała zorientować się co do danych pracownika, następnie poznać jego stanowisko na temat monitoringu, podsłuchu oraz przeszukania, aż wreszcie reakcje i zjawiska wywoływane przez wyżej wymienione sposoby kontroli.

ANKIETA:

1. Płeć
Kobieta, mężczyzna
2. Wiek
Poniżej 25 lat, 26–35 lat, 36–45 lat, powyżej 46 lat
3. Pracuje w :
Prywatnej firmie, instytucji państwowej, przedsiębiorstwie państwowym, inne
4. Firma/Przedsiębiorstwo/Instytucja zatrudnia:
Mniej niż 20 pracowników, 20–100 pracowników, powyżej 100 pracowników, powyżej 400 pracowników
5. Czy zgadza się Pan/Pani z poglądem, że pracownicy stanowią główne zagrożenie przestępcze dla firmy?
Tak, Nie

6. Czy uważa Pan/Pani, że polskie prawo w dostatecznym stopniu pozwala na kontrolę pracowników?
Tak, Nie
7. Czy zgodziłby/zgodziłaby się Pan/Pani na stosowanie przez przełożonych podsłuchu telefonicznego w celu kontroli rozmów służbowych bez wiedzy podsłuchiwanego?
Tak, Nie
8. Czy zgodziłby/zgodziłaby się Pan/Pani na stosowanie przez przełożonych podsłuchu telefonicznego w celu kontroli rozmów służbowych za zgodą podsłuchiwanego?
Tak, Nie
9. Czy zgodziłby/zgodziłaby się Pan/Pani na stosowanie przez przełożonych ukrytych kamer w celu kontroli zachowania w miejscu pracy bez zgody kontrolowanego?
Tak, Nie
10. Czy zgodziłby/zgodziłaby się Pan/Pani na stosowanie przez przełożonych ukrytych kamer w celu kontroli zachowania w miejscu pracy za zgodą kontrolowanego?
Tak, Nie
11. Czy w przypadku wprowadzenia przez przełożonych nagród pieniężnych za poufne przekazywanie informacji o patologiach w firmie skorzystałaby/skorzystałby Pani/Pan z możliwości przekazywania takich informacji?
Tak, Nie
12. Jak powyższe środki kontroli wpłynęłyby Pani/Pana zdaniem na komfort pracy?
Komfort pracy wzrośnie, komfort pracy nie ulegnie zmianie, komfort pracy zmniejszy się
13. Czy wiedząc, że podpisanie umowy o pracę zależy od podpisania zgody na pełne monitorowanie swojej pracy, podjęłaby/podjąłby Pani/Pan taką pracę?
Tak, Nie
14. Czy zgodziłaby/zgodziłby się Pani/Pan na monitorowanie swojego służbowego komputera przez pracodawcę?
Tak, Nie
15. Czy sprzeciwiłaby/sprzeciwiłby się Pani/Pan możliwości przeszukiwania pracowników w celu ochrony mienia pracodawcy?
Tak, Nie
16. W jakim stopniu Pani/Pana zdaniem zaufanie pracodawcy do pracowników wpływa na ich lojalność?
W znacznym, w niewielkim, pozostaje bez wpływu

17. Czy system wnikliwej kontroli lojalności pracownika w miejscu pracy gwarantuje pracodawcy zlikwidowanie całości patologii?
Tak, Nie
18. Czy Pani/Pana zdaniem wprowadzenie tego typu kontroli (monitoring, podsłuch) powodowałoby zmniejszenie efektywności pracy?
Tak, Nie
19. Czy Pani/Pana zdaniem wprowadzenie tego typu kontroli spowodowałoby spadek wzajemnego zaufania pracowników?
Tak, Nie
20. Czy Pani/Pana zdaniem patologie w miejscu pracy będą istnieć niezależnie od wprowadzenia wszystkich z wymienionych form kontroli?
Tak, Nie

Wyniki

Spośród 50 ankietowanych, 35 stanowili mężczyźni, 15 kobiety.

Najliczniejsza grupa (bo aż trzydziestoosobowa) składała się z pracowników w wieku od lat 26 do lat 35. Pozostałe grupy, w skład których weszli pracownicy w przedziale wiekowym od 36 do 43 lat oraz pracownicy, którzy nie przekroczyli 25 roku życia, liczyły po 10 osób.

Najwięcej osób poddanych badaniu zatrudnionych było w prywatnych firmach i przedsiębiorstwach państwowych (odpowiednio po 20 osób). Najmniej liczną grupę ankietowanych stanowiły osoby zatrudnione w instytucjach państwowych (tych było bowiem 10).

Kluczowe okazało się pytanie, czy obowiązujące prawo polskie w wystarczającym stopniu zezwala na kontrolę pracowników.

Odpowiedzi twierdzącej udzieliło 39 osób. Na pytanie „Czy zgadzasz się z poglądem, iż pracownicy stanowią główne źródło zagrożenia dla bezpieczeństwa firmy?", 40 osób odpowiedziało przecząco.

Następna część ankiety stawia pytanie, czy pracownik zgadza się na zastosowanie wobec niego monitoringu za jego zgodą lub bez niej. Monitorowanie za zgodą pracownika popiera 40 zapytanych, natomiast tylko jedna osoba opowiedziała się za monitoringiem nawet bez posiadanej zgody.

Podobny liczbowo wynik uzyskany został w sprawie zastosowania podsłuchu, gdzie aż 40 osób wyraziłoby na niego zgodę (pod warunkiem że jego zastosowanie poprzedzone byłoby informacją o jego ist-

nieniu). Sześć osób jednak zgodziłoby się na podsłuch bez wiedzy, iż jest on stosowany przez pracodawcę.

Problem, czy pracownik skorzystałby z przyznanej przez pracodawcę pieniężnej nagrody za przekazywanie poufnych informacji na temat ewentualnie istniejących patologii w firmie, został klarownie wyjaśniony. Żaden z ankietowanych nie skorzystałby z takiej możliwości.

Kwestia potencjalnego wpływu zastosowanych środków kontroli na komfort pracy oraz na panującą w jej miejscu atmosferę przedstawia się w następujący sposób: duża część (bo aż 39 osób) opowiedziała się za stanowiskiem, iż sprzyja to pomniejszeniu komfortu pracy, 10 osób uważa, że komfort nie ulegnie zmianie, a tylko jedna osoba nie poparła stanowiska, według którego komfort pracy wzrośnie.

Zgodnie z uzyskanymi wynikami 44 osoby podjęłyby pracę w miejscu, gdzie zobowiązane byłyby do podpisania zgody na pełne monitorowanie swojej pracy. 40 ankietowanych nie miałoby nic przeciwko poddaniu kontroli swojego służbowego komputera.

Wśród wszystkich pytanych nie było nawet jednej osoby, która by bez sprzeciwu poddała się przeszukaniu.

Interpretacja wyników

Z wyników uzyskanych po przeprowadzeniu ankiety oraz po zbadaniu związku pomiędzy poszczególnymi pytaniami testem chi-kwadrat można stwierdzić, że istnieje związek między odpowiedziami na pytania: 9 i 20, a także 9 i 10.

Pracownicy, którzy nie zgadzają się na monitorowanie bez ich zgody, równocześnie zgadzają się na taką kontrolę za zgodą i uważają, że patologie w firmie będą istnieć niezależnie od zastosowanych środków mających im przeciwdziałać. Jest to bardzo ważne stwierdzenie. Pokazuje, jak bardzo badani pracownicy zwracają uwagę na to, czy kontrola w firmie jest czymś, na co nie mają wpływu i o czym nie wiedzą, czy jest to zjawisko, na które mają wpływ i posiadają wiedzę o środku służącym kontroli. Moglibyśmy pokusić się o wniosek, że skoro aż 40 na 50 (pytanie 10) badanych zgodziłoby się na monitoring prowadzony za ich zgodą, a 49 nie zgodziłoby się na monitoring bez ich zgody, to

dla pracownika nie ma znaczenia, czy istnieje, czy nie istnieje kontrola. Znaczenie ma to, czy pracodawca informuje pracownika o tym, że w firmie stosowana jest kontrola.

Testowi chi-kwadrat poddano także pary pytań: 6 i 17, 5 i 17, 10 i 18, 13 i 14,7 i 8, 5 i 14. W tym przypadku wykazano, że powyższe pary pytań nie pozostają ze sobą w żadnym związku.

Wnioski końcowe

Wśród pracowników przeprowadzone badanie było różnie komentowane. Większość jednak jest zdania, że w żadnej firmie, większej czy mniejszej, pracownik nie stanowi jakiegokolwiek zagrożenia dla bezpieczeństwa firmy/przedsiębiorstwa/instytucji.

Pracownicy chętnie wyrażają zgodę na wprowadzanie i stosowanie przez pracodawcę środków kontroli, takich jak monitoring, podsłuch czy też inne środki służące realizacji celu, jakim jest bezpieczeństwo firmy. Pracownicy ci jednak kategorycznie sprzeciwiają się, aby taka forma kontroli funkcjonowała w zakładzie pracy bez ich wiedzy.

Spora część ankietowanych nie miałaby nic przeciwko podjęciu pracy, która opatrzona byłaby w wymóg złożenia przez nich uprzedniej pisemnej zgody na poddanie ich pełnej kontroli przez pracodawcę.

Z rezerwą podchodzą jednak pracownicy do takiej metody kontroli, która przekraczałaby dopuszczalny (akceptowany ze względów czysto racjonalnych w kręgach pracowniczych) stopień ingerencji w ich sferę prywatności. Z wyraźną dezaprobatą spotkała się taka metoda kontroli jak na przykład przeszukanie w celu ochrony mienia.

Zdaniem badanych jednym z ewentualnych skutków, jakich można się spodziewać ze względu na fakt kontrolowania pracowników, jest zmniejszenie się komfortu pracy, co jednak nie musi być równoznaczne ze spadkiem ich efektywności.

W opinii ankietowanych zaufanie, którym obdarzają się współpracownicy, nie pozostanie na tym samym poziomie, a ulegnie zdecydowanemu zmniejszeniu.

Jak wynika z badania, każdy pracobiorca priorytetowo traktuje zaufanie, jakim został obdarzony przez swojego pracodawcę. Pracodawca

musi zatem bardzo ostrożnie dobierać stosowane przez siebie środki kontroli, tak aby nie doprowadziły do radykalnej zmiany stosunków między nim a kontrolowanym pracownikiem.

Kluczowy wpływ na prawomyślność, lojalność zatrudnionych ma każda, nawet najmniejsza deformacja relacji typu pracodawca–pracownik.

W interesie pracodawcy leży to, aby zastosowane sposoby nadzoru nie miały negatywnego wpływu na efektywność oraz wydajność pracy. Powinien on liczyć się ze zdaniem współpracowników i co najważniejsze: nie stosować zabezpieczeń wbrew ich woli.

Co ciekawe, pracodawcy małych i średnich firm, którzy zapoznali się z powyższą ankietą, twierdzili, że unikają zatrudniania pracowników co do których mają wątpliwości, czy będą lojalni. Zdają sobie jednak sprawę z tego, że coraz trudniej jest sprawdzić od razu lojalność i uczciwość człowieka, którego zatrudniają. Pracodawcy dużych firm i przedsiębiorstw uważają, że kontrola pracowników jest dla nich niezbędnym elementem sprawnego działania firmy, którą prowadzą. W większym zakładzie pracy pracodawca może nawet nigdy nie zetknąć się z pracownikiem osobiście, dlatego zależy mu, aby ktoś „za niego" sprawdził, czy w zakładzie pracy występują jakieś patologie (kradzieże, fałszowanie danych itp.).

Pracownikom dużych zakładów pracy trudniej jest stworzyć relacje ze sobą, jeszcze trudniej z pracodawcą.

Co ma zrobić pracodawca, jeśli chce, aby, mimo że pracownik nie ma z nim bezpośredniego kontaktu, poczuł, że pracodawca, zatrudniając go, zaufał mu i nie będzie wkraczał nadmiernie w sferę jego prywatności, kontrolując go? Rozwiązaniem jest uprzedzenie pracownika o występującej w zakładzie pracy kontroli i zaznajomienie go ze sposobem tej kontroli. Pracownik, który nie będzie pewien sposobu działania środka kontroli, będzie z mniejszą uwagą skupiał się na pracy, ponieważ może koncentrować się na tym, czy to, co robi, jest już czymś, za co dostanie naganę od pracodawcy, czy jest to działanie, na które pracodawca zezwala. Rzecz jasna, nie mówimy tutaj o oczywistych dla pracowników wykroczeniach, których się dopuszczają, ale o niejasnych czasami dla pracownika wymaganiach pracodawcy.

Takie rozwiązanie nie zaniży poziomu zaufania i lojalności pracowników firmy, przedsiębiorstwa, a pracodawcy umożliwi sprawowanie dalszej kontroli nad miejscem pracy.

Dawid Czupik, Bartłomiej Gonciarz, Mateusz Mucha, Maciej Pabisz

Wykorzystanie poligrafu w biznesie prywatnym

Celem pracy była analiza wykorzystania badań poligraficznych na użytek biznesu prywatnego w Polsce. Cel ten udało się zrealizować tylko częściowo, gdyż firmy wykonujące badania obejmują tajemnicą informacje dotyczące klientów, nie ujawniają żadnych liczb dotyczących przeprowadzonych badań. W tej sytuacji jedyną możliwą metodą sprawdzenia skali zjawiska było przeprowadzenie rozmów z ekspertami, którzy zresztą zastrzegli sobie anonimowość.

Istnienie związku między przeżyciami a zmianami fizjologicznymi w organizmie ludzkim zauważane było od bardzo dawna. Już w starożytności próbowano łączyć uczucia z pewnymi narządami i tak np. gniew umiejscawiano w wątrobie, uczucia bardziej wzniosłe w sercu. Rozwój na przełomie XIX i XX w. takich dziedzin naukowych, jak psychologia, fizjologia spowodował, iż problem związku psychofizycznego coraz częściej próbowano zbadać empirycznie. Psychologowie posługujący się metodami eksperymentalnymi zaczęli rejestrować zmiany pracy narządów wewnętrznych pod wpływem przeżywanych emocji, w szczególności zwracając uwagę na fakt występowania takich zmian przy kłamstwie i innych zachowaniach nieszczerych. Efektem tych prac było skonstruowanie urządzenia pozwalającego na ujawnienie i rejestrowanie śladów pamięciowych oraz emocjonalnych, czyli poligrafu. Analiza zapisu tego urządzenia pozwala na wykrycie zachowań nieszczerych u badanego. Stąd tzw. „wykrywacz kłamstw" znalazł zastosowanie w takich dziedzinach, gdzie konieczne było zbadanie prawdomówności, zwłaszcza w kryminalistyce, działalności wywiadowczej. Dość szybko zalety tej metody dostrzegli prywatni przedsiębiorcy i badania poligraficzne są stosowane w biznesie już od lat 30., po raz pierwszy zastosowano je wobec pracowników jednego

z banków w Chicago. Skuteczności tej metody dowodzi jeden z pierwszych przypadków użycia poligrafu do badań lojalności pracowników, który miał miejsce w 1946 r. na rzecz The Manhattan District of Corps of Engineers, producenta bomby atomowej. Przebadano wówczas 690 pracowników. Pięciu z nich miało obiekcje przed przystąpieniem do testu, jednak gdy wyjaśniono im, że pytania nie będą dotyczyły życia prywatnego, ich wątpliwości ustąpiły i zgodzili się na udział w testach. Przeprowadzone badania przyczyniły się do wykrycia kilku przypadków kradzieży, ujawniania informacji poufnych niepowołanym osobom. Odnotowano również przypadki, gdy na wieść o zamiarze przeprowadzenia testów poligraficznych skradzione rzeczy zostały zwrócone przed inwentaryzacją. W 1953 r. program testów poligraficznych został przerwany przez Atomic Energy Connission z powodu, jak podano: „tylko marginalnego wzrostu poziomu bezpieczeństwa". Wkrótce jednak okazało się, iż było to bardzo złe posunięcie, gdyż podczas inwentaryzacji przeprowadzonej w 1984 r. stwierdzono brak 1,710 funtów uranu.

W Polsce metoda ta stosowana była od lat 70., ale powszechnie wykorzystuje się ją dopiero po przemianach społeczno-gospodarczych po roku 1989.

Można przypuszczać, że wykonuje się od kilku do kilkudziesięciu badań miesięcznie, jest to mała liczba w stosunku do sytuacji, gdzie poligraf znalazłby potencjalne zastosowanie. Jako przyczyny tego zjawiska należy wymienić:

- niską świadomość skuteczności tej metody. Pracodawcy z reguły nie posiadają wiedzy na ten temat i budują swoją opinię o poligrafie w oparciu o panujące stereotypy i mity rozpowszechniane nierzadko w środkach masowego przekazu. Niemały wpływ na rzadkie sięganie po wykrywacz kłamstw ma negatywna opinia części środowiska naukowego, podważająca skuteczność i zasadność tej metody w licznych publikacjach;
- ponadto dość negatywne nastawienie w środowisku prawniczym, objawiające się m.in. sceptycznym podejściem sądów do wyników badania poligraficznego jako dowodu;

- pracodawcy bardzo często nie porównują ewentualnych strat wynikających z zatrudnienia nieodpowiednich ludzi z kosztami badań;
- duże znaczenie ma też działalność osób świadczących usługi z zakresu badań poligraficznych, które nie posiadają odpowiednich kwalifikacji w tej dziedzinie, przez co zaniżają poziom świadczonych usług i wydatnie przyczyniają się do wytworzenia negatywnej atmosfery wobec tej metody. Osoby te mogą swobodnie działać na rynku, gdyż nie jest to działalność w żaden sposób koncesjonowana i w zasadzie każdy posiadający odpowiedni sprzęt może bez przeszkód się nią zajmować. Niejako próbą przeciwdziałania temu zjawisku jest wydawanie przez Polski Związek Poligraferów certyfikatów, które stanowią jedynie certyfikaty jakościowe, jednak ich uzyskanie nie stanowi warunku koniecznego do działalności w tej branży.

Działające na polskim rynku firmy i instytucje, chcąc zabezpieczyć się przed stratami, starają się budować poczucie lojalności względem zatrudnionych osób, podczas gdy pierwszoplanowym problemem pozostaje ich kontrola. Bierze się to stąd, iż elementem bądź czynnikiem, który przynosi firmie najwięcej strat, jest jej pracownik – działający samodzielnie lub w zmowie z kimś z zewnątrz. Badanie poligraficzne pozwala na odpowiednie ukierunkowanie wersji przedmiotowych i podmiotowych konkretnych rozważań istotnych dla dobra (głównie bezpieczeństwa) danej instytucji lub firmy. Wykazuje się bowiem związki emocjonalne badanego z wiedzą na temat danego zdarzenia. Wydaje się, że żadna inna metoda nie jest w stanie tak dokładnie określić czynnika, który miał wpływ na straty w danej instytucji.

Spośród trzech sytuacji, w których możliwe jest zastosowanie poligrafu, pracodawcy najczęściej sięgają po tę metodę w przypadku wystąpienia zdarzenia generującego straty, pozostałe rodzaje badań, czyli: badania przedzatrudnieniowe i okresowe badanie lojalności personelu są wykorzystywane sporadycznie, co jest wynikiem braku odpowiednich nawyków u pracodawców.

Poligraficzne badania przedzatrudnieniowe kandydatów na pracowników są szybką i stosunkowo tanią metodą sprawdzenia ich wiarygod-

ności i predyspozycji. Każda firma może sama według swoich kryteriów określić wzorzec pracownika, jaki jest potrzebny na dane stanowisko, często przez stworzenie katalogu cech niepożądanych. Badanie ma na celu wykrycie niekompetentnych kandydatów w przedsiębiorstwie, których działalność może powodować finansowe i materialne straty.

Jeżeli chodzi o okresową kontrolę lojalności, to jest to forma badania celowa wobec osób mających wysoki stopień służbowej samodzielności. Wynika to stąd, iż gdyby osoby takie podjęły działania na szkodę firmy, to szkoda taka mogłaby zostać ujawniona dopiero po długim czasie, gdy straty osiągną już poważne rozmiary. Kolejną przesłanką przemawiającą za celowością tych badań jest dostęp tych osób do szczególnie ważnych tajemnic przedsiębiorstwa – kwestia „szczelności" takich osób ma bowiem istotne znaczenie. Badanie tego rodzaju proponuje się pracownikom, wobec których nie ma konkretnych podejrzeń, testy zaś mają charakter czysto zapobiegawczy. Motywacją do poddania się tego rodzaju badaniom powinna być współodpowiedzialność za losy firmy.

Badania przeprowadzane w przypadku zaistnienia konkretnego zdarzenia dotyczą przede wszystkim:

- kradzieży (według danych z USA kradzieże pracownicze powodują rocznie straty w wysokości ok. 120 mld dolarów (brak danych w Polsce na ten temat);
- włamania, ponieważ zdarza się często, że sprawcy mają „swojego" wewnątrz firmy, który ułatwia im dokonanie przestępstwa;
- fałszerstwa lub oszustwa. Badania przeprowadzone przez znaną międzynarodową kancelarię biegłych księgowych Ernest & Young wykazały, że ponad połowę nadużyć wykryto przypadkowo, a 3/4 z nich dokonali pracownicy;
- korupcji w firmie, np. przy wyborze kooperanta;
- ujawnienia tajemnic firmy;
- zagubienia ważnych dokumentów, wartościowych przedmiotów – nieraz warto sprawdzić, czy to faktycznie przypadkowa utrata;
- utrzymywania przez pracowników kontaktów z konkurencją;
- nałogów, szantażu itp.

Wykorzystanie testu określonego typu jest wyłączną decyzją operatora. Możliwość wyboru testu niejednokrotnie jest ograniczona okolicznościami badanej sprawy, preferencjami realizującego badanie i jego wiedzą. Najczęściej stosowaną techniką jest technika pytań kontrolnych Reida w postaci klasycznej, czyli raczej przestarzałej, oraz testy szczytowego napięcia. Testy te wzajemnie się uzupełniają i nie stanowią dla siebie konkurencji, można je stosować łącznie lub pojedynczo. W przypadku badań mających wyeliminować osoby z kręgu podejrzanych stosuje się wyłącznie testy szczytowego napięcia. Nie znaleźliśmy informacji, aby stosowane były testy zleconego kłamstwa techniki Backstersa ani bardzo bliskiego mu ideowo testu kłamstwa prawdopodobnego (testy typu PLT, DLT).

Przedsiębiorcy, którzy decydują się skorzystać z poligrafu, z reguły kierują się motywami ekonomicznymi, gdyż straty powodowane przez nielojalnych pracowników opiewają niejednokrotnie na duże sumy. Również chęć zachowania prestiżu firmy oraz to, że przestępstwa pospolite w miejscu pracy, takie jak np. drobne kradzieże, psują atmosferę i są uciążliwe dla reszty personelu i mogą prowadzić do powstania napięć wpływających na obniżenie wydajności pracy, stają się coraz częściej przyczynami przeprowadzanych badań poligraficznych.

Krąg badanych określa pracodawca, operator może jedynie sugerować zakres. Ponadto każda osoba uczestnicząca w badaniu musi wyrazić na nie zgodę, a zadawane pytania nie mogą dotyczyć prawnie chronionych sfer życia prywatnego. W tej kwestii duże znaczenie odgrywa dopracowanie treści oświadczenia, jakie podpisuje osoba wyrażająca zgodę, co pozwala na uniknięcie roszczeń z tytułu niewłaściwego wykorzystania wyników badania przez pracodawcę. Pracownicy są uprzedzani o terminie badania i jednocześnie zostają poinformowani o warunkach, jakie muszą zachować, np. o zakazie spożywania alkoholu, zażywania leków uspokajających itp. Przed przystąpieniem do badań przeprowadza się rozmowę na okoliczności mogące mieć znaczenie w trakcie badań, między innymi co do stanu zdrowia. Następnie zapoznaje się taką osobę z istotą badania poligraficznego oraz pytaniami, jakie będą zadawane.

To, jak pracodawca wykorzysta wiedzę, którą uzyska w wyniku badania, zależy wyłącznie od niego. Dość często uzyskana wiedza staje się podstawą skierowania sprawy do organów ścigania, gdyż zgłoszenie przestępstwa niejednokrotnie jest jednym z warunków uzyskania odszkodowania. Jednakże ani wynik badania, ani odmowa poddania się mu nie mogą stanowić samodzielnej podstawy do zwolnienia pracownika. Musi ono być poparte innymi dowodami.

Obecnie można zaobserwować wzrost liczby wykonywanych badań. Jest to wynikiem dużej skuteczności tej metody, co przekonuje biznesmenów. Osoby, które są pozytywnie doświadczone, bardzo chętnie wykorzystują ponownie poligraf w swojej działalności, często polecając tę metodę swoim kontrahentom lub partnerom biznesowym. Polskie prawo pracy nie reguluje jednoznacznie tej kwestii, stąd stosowanie poligrafu opiera się głównie na zasadzie, że co nie jest zabronione przez prawo, to jest dozwolone. Warto w tej kwestii wziąć przykład z rozwiązań, jakie stosowane są w USA, tam najwięcej badań, bo ok. 80%, jest wykonywanych na potrzeby prywatnego przemysłu i handlu. Większość amerykańskich firm bankowych, handlowych i przemysłowych korzysta z badań poligraficznych przy przyjmowaniu pracowników na bardziej odpowiedzialne stanowiska do pracy oraz z tzw. okresowych kontroli uczciwości zatrudnionego personelu. Coraz szersze zastosowanie poligrafu zaczęło godzić w amerykańskie poczucie wolności jednostki. W związku z tym wiele organizacji pracowniczych zaczęło ostrą kampanię przeciwko badaniom poligraficznym prowadzonym przy zatrudnieniu. Wynikiem tej kampanii prowadzonej głównie w latach 60. było wprowadzenie przez część stanów przepisów regulujących tę kwestię. Przepisy te określają, w jakich sytuacjach i w jakim zakresie pracodawca może żądać od pracownika poddania się badaniu poligraficznemu.

27 grudnia 1988 r. Kongres uchwalił ustawę regulującą kwestie użycia poligrafu w biznesie prywatnym na terenie USA; jej pełna nazwa brzmi: Employee Polygraph Protection Act (EPPA). EPPA dotyczy większości przedsiębiorców prywatnych, nie obejmuje swoim zakresem organizacji rządowych (zarówno federalnych, jak i lokalnych), w przypadku tych jednostek kwestię użycia poligrafu regulują oddzielne ustawy.

Przed wejściem w życie EPPA prawo regulowało jedynie użycie poligrafu w sprawach karnych oraz przez agencje rządowe. W miarę tego jak metoda ta stawała się coraz bardziej popularna, coraz więcej pracodawców decydowało się na jej użycie, w związku z tym zaczęto podnosić kwestie, iż należy uregulować prawnie zasady użycia poligrafu na rzecz pracodawców prywatnych.

Ustawa ta stanowi generalny zakaz przeprowadzania badań poligraficznych na rzecz pracodawców prywatnych, jednakże od tej reguły EPPA przewiduje kilka wyjątków, gdy użycie „wykrywacza kłamstw" w stosunku do pracowników lub przyszłych pracowników jest dozwolone. Zakaz ustanowiony na mocy tego aktu normatywnego podyktowany został głównie chęcią ochrony praw pracowników przed nadużyciami ze strony pracodawców. Równie ważnym czynnikiem była debata, która w owym czasie toczyła się w USA, dotycząca wiarygodności i dokładności poligrafu. Znamienne jest tu zdanie, jakie wypowiedział Richard Nixon w związku z dochodzeniem prowadzonym w sprawie wycieku informacji z Białego Domu: „Nie wiem za wiele o poligrafie, nie wiem, jak dokładny jest, ale wiem, że wywołuje on przerażenie u ludzi". Zdanie to uwidacznia, jakie odczucia wywoływała u sporej grupy osób ta metoda, brak wiedzy na ten temat wzbudzał obawy i nieufność.

Ustawa, definiując pojęcie *lie detector,* określa jego zakres, zaliczając do niego oprócz poligrafu również inne urządzenia służące do wykrywania nieszczerości u badanego, takie jak np. analizatory głosu.

EPPA ma zastosowanie w stosunku do wszystkich pracowników zatrudnionych lub pośrednio działających w interesie pracodawcy w sektorze prywatnym. W przypadku badań przedzatrudnieniowych odnosi się ona również do ewentualnych pracowników. Ustawa stanowi szereg wymogów formalnych, które muszą być spełnione, aby badanie było legalne:

1) Pracodawca jest zobowiązany przesłać pracownikom wykaz praw przysługujących im na podstawie EPPA. Dokument ten przygotowany jest przez Urząd Pracy (Departament of Labour). Ponadto ustawa nakłada obowiązek przechowywania przez pracodawcę określonych dokumentów mających związek z przeprowadzaniem badań poligraficznych w zakładzie pracy.

2) Poligrafer przeprowadzający testy musi posiadać aktualną licencję (obowiązującą w miejscu przeprowadzania testu), ponadto musi posiadać profesjonalne ubezpieczenie lub złożyć 50 000 dolarów kaucji celem zabezpieczenia ewentualnych roszczeń ze strony pracowników.

3) Przede wszystkim musi zachodzić jedna z enumeratywnie wymienionych w ustawie sytuacji, które stanowią wyjątek od ogólnego zakazu przeprowadzania testów poligraficznych. Są to następujące sytuacje:

a) wyjątek taki zachodzi, gdy toczy się postępowanie w konkretnej sprawie, która spowodowała stratę ekonomiczną lub inny uszczerbek majątkowy dla firmy. Do sytuacji takich możemy zaliczyć:

- kradzież,
- malwersację,
- przywłaszczenie,
- szpiegostwo przemysłowe,
- sabotaż.

Toczące się postępowanie musi dotyczyć konkretnego zdarzenia już stwierdzonego. Pracodawca nie może zarządzić testów poligraficznych mających na celu sprawdzenie, czy w ogóle kiedykolwiek miała miejsce jakaś kradzież w firmie, gdyż badanie takie nie spełniałoby znamion ustawowo określonych jako wyjątek w EPPA. Zgodnie z prawem pracodawca musi wykazać, iż pracownik, który ma być poddany testom na „wykrywaczu kłamstw", miał dostęp do danej rzeczy i istnieją uzasadnione podejrzenia, że mógł mieć związek z określoną sprawą;

b) drugi wyjątek, jaki ustawa stanowi od ogólnego zakazu, odnosi się do firm zajmujących się ochroną mienia. W przypadku tych firm dozwolone są również badania przedzatrudnieniowe;

c) kolejny wyjątek ustanowiony został w przypadku firm posiadających licencję na wytwarzanie, dystrybucję, przechowywanie substancji psychotropowych – tu również dopuszczone są badania przedzatrudnieniowe.

Ze specyficzną sytuacją mamy do czynienia, gdy w związku z przestępstwem pracowniczym organy ścigania prowadzą postępowanie karne i w ramach tego postępowania zarządzone są badania poligraficzne pracowników. Przyjmuje się, że do czasu, gdy pracodawca zachowuje

jedynie bierną postawę, np. ograniczając się do udzielenia pracownikom czasu wolnego od pracy w celu poddania się badaniu poligraficznemu prowadzonemu przez policję, EPPA nie ma zastosowania. W wyżej wymienionych przypadkach użycie poligrafu regulowane jest przez ustawy odrębne.

Prawa egzaminowanego wynikające z EPPA:

1. Pracownik ma prawo do pisemnej informacji o czasie i miejscu przeprowadzenia testu. Pismo to dodatkowo musi zawierać:

- dane o naturze przeprowadzanego testu oraz podstawie, na jakiej jest przeprowadzany;
- jasną informację, iż uczestnictwo w nim nie stanowi warunku dalszego zatrudnienia;
- informację, że test nie może zawierać pytań, które wcześniej nie zostały z egzaminowanym omówione;
- pouczenie dla egzaminowanego, iż wszystko, co oświadczy, może być użyte przeciwko niemu jako dodatkowy wspomagający dowód;
- pouczenie o środkach prawnych, jakie przysługują egzaminowanemu w przypadku naruszenia jego praw;
- informacje o tym, w jaki sposób pracodawca może wykorzystać wynik testu oraz w jakich okolicznościach może on być ujawniony i komu;
- ewentualne poinformowanie badanego, że przebieg testu jest utrwalany za pomocą urządzeń audiowizualnych, takich jak np. kamery.

2. Pracownik ma prawo skontaktować się z adwokatem lub przedstawicielem związków zawodowych.

Egzaminator przed przystąpieniem do testu musi poinformować raz jeszcze badanego o jego prawach. Egzaminowany może w każdej chwili przerwać test zarówno przed jego rozpoczęciem jak i w trakcie. Poligrafer nie może zadawać pytań poniżających ani też dotyczących poglądów politycznych, religii, kwestii rasowych, zachowań seksualnych. Pracodawca nie może poddawać testom osób, które posiadają zaświadczenie lekarskie, iż stres wywołany testem mógłby wywołać u nich uszczerbek na zdrowiu.

Dozwolone na podstawie EPPA jest ujawnianie wyników następującym osobom:

1. Egzaminowany lub osoba przez niego upoważniona.
2. Pracodawca.
3. Sąd, agencje rządowe, mediator na podstawie zarządzenia sądu.
4. Urząd Pracy lub jego upoważnieni przedstawiciele.

Jeżeli w wyniku testu zostaną uzyskane informacje o popełnieniu przestępstwa, mogą one być ujawnione organom ścigania bez występowania o zgodę do sądu. Poligrafer przeprowadzający badanie może również pokazać jego wyniki, bez ujawniania tożsamości badanego, innemu poligraferowi w celu konsultacji.

Za naruszenie praw pracowniczych chronionych przez EPPA pracodawca ponosi odpowiedzialność na gruncie cywilnym. Ustawa ta zabrania zmuszania pracowników do poddania się badaniu poligraficznemu, zakazuje również jakiejkolwiek dyskryminacji osób, które odmówiły lub też wynik ich testu wykazał nieszczerość. Wynik badania poligraficznego nie może być jedyną podstawą, na jakiej opiera się decyzja pracodawcy o zwolnieniu pracownika, musi on być poparty innymi dowodami.

Uregulowanie prawne przyczyniło się do wzrostu poziomu świadczonych usług, gdyż ujednolicono szkolenie i podniesiono jego poziom.

W Stanach Zjednoczonych badania poligraficzne przedzatrudnieniowe są bardzo popularne, zwłaszcza w różnego rodzaju agencjach policyjnych szukających nowych pracowników. Tłumaczy się to tym, iż badanie takie pozwala na wyjawienie informacji, jakich nie dałoby się dowieść w inny sposób (inną metodą selekcji). Kolejnym argumentem przemawiającym za wyższością badań poligraficznych nad innymi metodami w poszukiwaniu kadr pracowniczych jest fakt, iż pozwalają one ustalić bardzo dokładne informacje o kandydatach. Dzięki temu pracodawca unika ryzyka zatrudnienia niepożądanego pracownika. Badania te umożliwiają dodatkowo samym kandydatom uczciwe zakończenie procesu selekcji na dane stanowisko. Natomiast pracodawca może być pewien, że zatrudnia „wysokiej jakości" pracowników nadających się

najlepiej do danej pracy spośród wszystkich kandydatów. 90% agencji, które przeprowadzały badania przedzatrudnieniowe, deklaruje pewność, że dzięki nim zatrudniły odpowiednich pracowników. Według nich takie metody, jak: testy psychologiczne, wywiady osobiste i wiele innych są znacznie mniej użyteczne aniżeli badanie poligrafem. Wreszcie ostatnią korzyścią, którą wskazały omawiane instytucje, jest to, iż dzięki badaniom wychodzi na jaw kryminalna przeszłość kandydatów: chodzi o przestępstwa przez nich popełnione, które nie zostały wykryte przez organy ścigania. Przestępstwa, które najczęściej są ujawniane podczas badań, to: gwałty, napady z bronią w ręku, włamania, podpalenia i wiele innych.

Podsumowując rozważania na temat wykorzystania poligrafu w „polskim biznesie prywatnym", należy stwierdzić, iż nie jest to najpopularniejsza z metod wykorzystywanych do selekcji bądź kontroli pracowników. Wpływa na to z pewnością fakt, iż kwestie dotyczące poligrafu w stosunkach pracy nie są w prawie polskim w żaden sposób uregulowane: kodeks pracy „nie zna" tej metody. Pracodawcy podchodzą więc do „wykrywacza kłamstw" raczej z dystansem, obawiając się, by jego użycie nie wywołało ujemnych skutków dla nich i ich firm. Dodatkowo „niechęć do poligrafu" potęgują liczne artykuły bądź komentarze znanych osób wywodzących się ze środowiska naukowego i prawniczego, które nie mogą przekonać się do skuteczności tej metody.

Pracodawcy, jeżeli sięgają po poligraf, robią to w ostateczności, gdy w ich firmie doszło już do przestępstwa i należy je wykryć. Często jednak może być już za późno, by znaleźć winowajcę, bądź straty są tak ogromne, że firma musi upaść. Warto w tym momencie się zastanowić, czy nie byłoby korzystniej zacząć przeprowadzać badania przedzatrudnieniowe i okresowo kontrolować lojalność pracowników za pomocą poligrafu, by nie doprowadzić do wspomnianych wyżej sytuacji. Lepiej profilaktycznie kontrolować, co dzieje się w naszej firmie, i w ten sposób budować wokół niej dobrą atmosferę, niż musieć stosować bardziej restrykcyjne środki, takie jak dyscyplinarne zwolnienia nieuczciwych pracowników, czy też zmniejszanie produkcji na skutek strat przez nich spowodowanych.

Zacieśnienie współpracy pomiędzy środowiskami biznesowymi a Stowarzyszeniem Poligraferów Polskich oraz regulacja prawna dotycząca wykorzystania poligrafu w stosunku do pracowników z pewnością przyczyniłyby się do rozpowszechnienia tej metody w podnoszeniu bezpieczeństwa firmy oraz do pełniejszego wykorzystania jej zalet.

Anna Huzior, Małgorzata Nyc

Przestępczość wśród pracowników dużych centrów handlowych

Wstęp do zagadnienia

Bezpieczeństwo biznesu to temat obejmujący wiele zagadnień, ponieważ biznes można rozumieć szeroko, od prowadzenia banku z wielomilionowym kapitałem aż po skromne gospodarstwo rolne, czyli generalnie jako działalność nastawioną na zysk. Prowadzenie działalności gospodarczej, również takiej jak sklepy wielkopowierzchniowe, wiąże się z pewnymi zagrożeniami, które można podzielić na:

a) zewnętrzne (konkurenci na rynku, klienci, nieuczciwi dostawcy i kontrahenci),

b) wewnętrzne (pracownicy, menedżerowie).

Tematem tej pracy są zagrożenia wewnętrzne, jakimi są „przestępstwa pracownicze". Problem ten zostanie ogólnie zarysowany i zilustrowany przykładami z praktyki.

Na wstępie należałoby zadać pytanie: „Czym jest przestępczość pracownicza?". Odpowiedź na nie nie jest prosta, ponieważ ani kodeks karny, ani kodeks pracy, ani też doktryna nie definiują tego pojęcia. Terminu „przestępczość pracownicza" nie powinniśmy definiować jako przestępstwa w rozumieniu kodeksu karnego popełnianego przez osobę będącą pracownikiem. Przestępstwo w świetle prawa karnego to czyn zabroniony pod groźbą kary przez ustawę, bezprawny, zawiniony i społecznie szkodliwy w stopniu wyższym niż znikomy, a nie każdy czyn popełniany przez pracownika na szkodę pracodawcy wszystkie te znamiona wyczerpuje. Najlepiej zagadnienie będące przedmiotem tej pracy opisuje anglojęzyczny termin *corporate fraud* (firmowe oszustwo, nieuczciwość). Ze względu jednak na brak wyczerpującego odpowied-

nika w języku polskim będziemy korzystać z terminu „przestępczość pracownicza", traktując go oczywiście w sposób pomocniczy.

„Przestępstwo pracownicze" może być dokonane zarówno w formie działania, jak i zaniechania. Po stronie pracownika zawsze występuje element winy, a stroną poszkodowaną (bardzo często materialnie) jest pracodawca. Trzeba również pamiętać, że nie wszystkie czyny popełnione na szkodę pracodawcy są bezprawne, jak np. „kradzież czasu" czy wykorzystywanie sprzętu pracodawcy do prywatnych celów, niewłaściwe zabezpieczanie towarów przez pracowników poszczególnych działów, wystawienie na półkę drogiego sprzętu RTV/AGD, zwłaszcza małych rozmiarów, jest niedopełnieniem obowiązków pracowniczych i stanowi „zachętę" dla potencjalnych złodziei – nieuczciwych klientów (straty z tytułu braku zabezpieczenia towarów są znaczne).

„Przestępstwo pracownicze" może mieć postać:
- kradzieży,
- kradzieży z włamaniem,
- przywłaszczenia mienia,
- nieodpowiedniego prowadzenia dokumentacji,
- podrabiania znaków identyfikacyjnych,
- „sprzedaży" informacji konkurencji,
- podrobienia dokumentu,
- nielegalnego wypełnienia podpisanego dokumentu,
- wyłudzenia odszkodowania,
- inną, niewyczerpującą znamion przestępstwa według kodeksu karnego.

Najczęściej popełnianym przestępstwem w centrach handlowych jest kradzież; należy do niej zaliczyć także konsumpcję towarów bez zapłaty. W magazynach, chłodniach, toaletach pracowniczych pozostawiane są opakowania po zjedzonych bądź wypitych towarach. Znajdowane są opakowania po czekoladach, batonach, gumach do żucia. Na polu kradzieży pracownicy wykazują się daleko idącą pomysłowością, np. alkohol przelewany jest do butelek po wodzie mineralnej i odpowiednio oznaczony kupowany przez pracowników marketów za cenę wody mineralnej, mimo iż butelka zawiera o wiele cenniejszą ciecz.

Często zdarza się, że kasjerzy nie kasują całego towaru osobom podstawionym, członkom rodziny lub że pracownicy wynoszą towar ukryty w odzieży, w bieliźnie. Zaskakująco niewiele odnotowuje się przypadków kradzieży z włamaniem. W ciągu roku są to pojedyncze przypadki, ponieważ drogie artykuły (np. RTV/AGD) są zamykane w magazynach w specjalnych boksach. Tam właśnie usiłuje się dostać sprawca, ale klucze do tych magazynków posiada ochrona i wydaje towar na halę sprzedaży za pokwitowaniem pracownikowi danego działu.

Wszystkie „przestępstwa pracownicze" możemy podzielić dychotomicznie ze względu na częstotliwość ich popełniania. Możemy wyróżnić przestępstwa:

- jednorazowe, np. zniszczenia, kradzieże towarów lub pieniędzy (zazwyczaj dopuszczający się ich pracownik spontanicznie wykorzystuje nadarzającą się okazję. Pojedyncze przestępstwa należą do rzadkości i nie powodują dużych strat),
- powtarzające się, np. fałszowanie dokumentacji, kradzieże z kont, wynoszenie towaru o małych gabarytach w odzieży podczas opuszczania miejsca pracy i obiektu (powodują największe straty materialne, ważnym ich elementem jest zatajenie działania, są przestępstwem trudnym do wykrycia, powodującym znaczne straty).

„Przestępstwa pracownicze", zwłaszcza te popełniane długofalowo, powtarzające się, z reguły nie są łatwe do wykrycia. Dzieje się tak dlatego, ponieważ ważnym elementem powodzenia takich czynów jest ich zakonspirowanie. W przypadku jednorazowego „przestępstwa", zwłaszcza polegającego na zniszczeniu mienia, sprawa ma się nieco odmiennie. Generalnie wbrew powszechnie panującemu wśród kadry zarządzającej przekonaniu większość „przestępstw pracowniczych" nie jest wykrywana podczas kontroli przeprowadzanych przez zarząd ani w toku audytu zewnętrznego. Jak podaje Michael Comer w książce *Corporate fraud*, większość przestępstw pracowniczych wychodzi na jaw przez przypadek[1]. Procentowa zależność wygląda następująco:

- 51% – przypadek,
- 19% – audyt zewnętrzny,

[1] M. I. Comer, *Corporate fraud,* 3rd edition, 1998 r.

- 10% – kontrole zarządu,
- 20% – inne.

Najczęstsze działania pracodawców prowadzące do „wyłowienia" nieuczciwych pracowników to: codzienne kontrole pracowników na posterunkach ochrony, zabezpieczanie towarów w miejscach niewidocznych i bez wiedzy pracowników danego marketu, zadziałanie systemu alarmowego w trakcie kontroli. Również audyt dokumentacji stanowi źródło wiedzy o przestępstwach. Problem niskiej wykrywalności pomoże zilustrować nam fakt, iż w 2005 roku w jednym z wrocławskich hipermarketów ujęto 31 osób, a do połowy 2006 roku ujawniono tylko 6 kradzieży pracowniczych na kwotę 455,79 PLN.

Bardzo ciężko jest określić, jakie rzeczywiste straty ponoszą przedsiębiorstwa. Przyjmuje się, że straty te wynoszą od 2 do 5% całkowitego obrotu. W przypadku dużych centrów handlowych jest to jeszcze bardziej utrudnione, ponieważ przyjmuje się w nich próg strat dopuszczalnych. Jego wysokość stanowi tajemnicę handlową, stąd trudno wnioskować, na ile straty są dotkliwe. Kilka liczb uzyskanych z działu ochrony jednego z wrocławskich hipermarketów pomoże zilustrować skalę zjawiska w 2005 roku.

Łączna wartość odzyskanego towaru wyniosła 15935,62 PLN (w tym między innymi: 2 pracowników ujęto na kradzieży płyt DVD o wartości 560 PLN, pracownicy skarbca i kas przywłaszczyli bony towarowe, pracownik punktu obsługi klienta ukradł 2 banknoty po 200 PLN, kasjer dokonał kradzieży towaru o wartości 965 PLN, ujawniono kradzież pieniędzy w kwocie 636 PLN przez 2 pracowników punktu obsługi klienta, magazynier dokonał kradzieży perfum o wartości 29 PLN, 2 pracowników działu mięsnego „przemetkowało" schab na kości – straty 259 PLN, 2 pracowników piekarni dokonało kradzieży odtwarzaczy DVD o wartości 181 PLN).

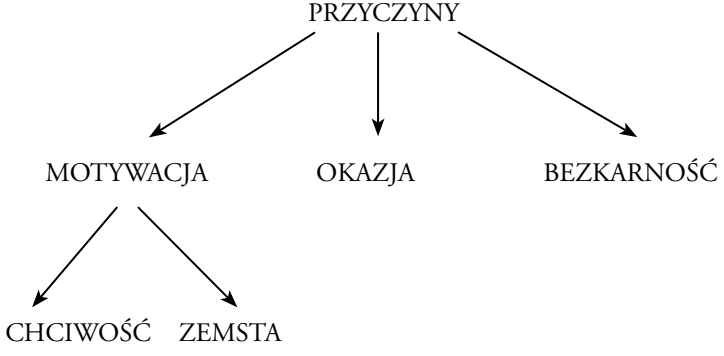
Warto zwrócić również uwagę, jakie straty powoduje prowadzenie rozmów prywatnych z telefonów służbowych. Mimo że pojedyncza, kilkuminutowa rozmowa pracownika w porównaniu z obrotami sklepu jest „kroplą w oceanie", to jej permanentne nadużywanie może kosztować pracodawcę nawet kilka tysięcy złotych.

Największe straty powodują przestępstwa dokonywane przez kasjerów pozostających w porozumieniu i związku przestępczym z inną osobą lub osobami. Jeden z zanotowanych przypadków w pewnym markecie dotyczył towaru o wartości ponad 5000 PLN.

Mimo że przytoczone kwoty nie są zatrważające, warto zwrócić uwagę, że ze względu na nieuczciwość pracowników w Stanach Zjednoczonych ok. 30% przedsiębiorstw ulega likwidacji.

„Przestępstwa pracownicze" popełniane są przez pracowników wszystkich szczebli, jednakże najczęściej są to: pracownicy fizyczni, w tym kasjerzy, magazynierzy, sprzedawcy, czyli pracownicy na podstawowych stanowiskach, rzadziej kierownicy działów (pojedyncze przypadki w ciągu 2, 3 lat). Charakteryzując osoby popełniające „przestępstwa pracownicze", można zauważyć, że w większości są to mężczyźni i wbrew powszechnemu przekonaniu ani wiek, ani krótki staż pracy w danym miejscu nie mają znacznego wpływu na skłonność do popełniania przestępstw pracowniczych (odnotowano kilka przypadków dokonania kradzieży przez pracowników ze stażem pracy dłuższym niż 7 lat). Często są to osoby uzależnione od alkoholu (czasem też od narkotyków), ryzykanci, osoby lubiące życie na wysokim poziomie, a wiecznie cierpiące na brak gotówki.

Przyczyny popełniania „przestępstw pracowniczych" są różne. Obrazowo przedstawiono je na poniższym schemacie.



Źródło: opracowanie własne.

Zaistnienie sprzyjającej okazji jest nieodzownym warunkiem popełniania zwłaszcza jednorazowych, spontanicznych przestępstw. Powiedzenie „okazja czyni złodzieja" znajduje tu pełne zastosowanie. Oczywiście wielce krzywdzące byłoby stwierdzenie, że każdy wykorzysta nadarzającą się okazję. Wszystko zależy od stopnia uczciwości. Przez uczciwość należy rozumieć sprawiedliwość i prostolinijność w sposobie zachowania, wypowiedziach, prawość, prawdomówność, wolność od oszustwa, szacunek dla człowieka i jego własności. Wyróżnia się uczciwość moralną, czyli podświadomą, wynikającą z poczucia odpowiedzialności i szacunku, oraz uczciwość warunkową będącą jedynie rezultatem strachu o konsekwencje bycia złapanym. Na ile jesteśmy uczciwi?

- 25% ludzi kłamie i oszukuje,
- 25% nigdy nie zachowuje się nieuczciwie,
- 50% może zachować się nieuczciwie albo uczciwie, zależnie od okoliczności i okazji.

Trzeba też dodać, że nie każdy pracownik będzie w równie dużym stopniu „kuszony" przez nadarzające się okazje. O wiele więcej będzie ich miała osoba mająca dostęp do informacji, środków, aktywów, dokumentów czy systemu komputerowego. Oczywiście będą to pracownicy obdarzeni większym zaufaniem lub mający dłuższy staż. Tu widzimy, jak ważne byłoby kontrolowanie przeszłości potencjalnych pracowników, bo wielu strat można by po prostu uniknąć. Należy też zwracać uwagę na wszelkie symptomy mogące świadczyć o nieuczciwości pracownika, a mogą to być: podwyższenie stopy życiowej, częsty udział w imprezach alkoholowych, palenie drogich papierosów, braki w danym towarze wychwytywane przez ochronę, znajdowanie opakowań po towarze w magazynach lub innych pomieszczeniach socjalno-administracyjnych.

Kolejną przyczyną jest motywacja. Motywów sprawca może mieć wiele, jednym z nich może być chciwość. Jest ona najczęstszą przyczyną popełniania przestępstw przeciwko mieniu, również „przestępstw pracowniczych". Pracownicy bardzo często „dorabiają" sobie w ten sposób do zbyt niskiego (przynajmniej wg nich) wynagrodzenia. Poza tym, powtarzając teorię Mertona, przestępstwo jest jedną z dróg do zdobycia prestiżu, pieniędzy, zwłaszcza gdy społecznie akceptowane sposoby ich

uzyskania są dla pracownika nieosiągalne. Ryzyko oszustwa pracowniczego wzrasta, gdy pracownik napotyka na uczciwej drodze do awansu i wyższego wynagrodzenia bariery, których nie może przekroczyć. Mogą to być wiek, płeć, brak kwalifikacji, narodowość, zarezerwowanie „lepszych" stanowisk dla członków rodziny (w przypadku przedsiębiorstwa rodzinnego), a nawet palenie tytoniu.

Drugim najczęstszym motywem obok chciwości jest chęć zemsty. Jest ona często podawana jako usprawiedliwienie dla przestępstw popełnianych przez pracowników na szkodę pracodawcy. Może to być zemsta za niską płacę, złe traktowanie, niedocenianie lub odsuwanie od awansu. Z tego motywu zazwyczaj popełniane są przestępstwa jednorazowe, spontaniczne, polegające na niszczeniu mienia.

Również brak obawy zostania złapanym często popycha do popełniania przestępstw, również tych pracowniczych. Jak już było wspomniane, są one rzadko wykrywane, rzadko więc sprawca jest ukarany czy napiętnowany. Często też problem przestępstwa pracownika rozwiązuje się „wewnętrznie". Przestępstwo takie nie jest zgłaszane organom ścigania (aby nie nagłaśniać sprawy), a z pracownikiem rozwiązuje się umowę w trybie natychmiastowym, a tymczasem najbardziej odstraszającym czynnikiem przed popełnieniem „przestępstwa pracowniczego" byłby przykład ujęcia pracownika i wyprowadzania go z marketu skutego kajdankami przez policję. Jest to zgodne z koncepcją, że najbardziej odstrasza nie tyle kara wysoka, ile szybka i nieuchronna. Bardzo często też „przymyka się oko" na pewne kryminogenne zachowania pracowników, pewien stopień nieuczciwości jest tolerowany, tworząc poczucie bezkarności. A należy pamiętać, że nie ma czegoś takiego jak „małe oszustwo", bo już wkrótce może nastąpić jego eskalacja.

Po zarysowaniu problemu „przestępczości pracowniczej" należy przyjrzeć się zabiegom prewencyjnym, jakie podejmują właściciele hipermarketów. W każdym sklepie wielkopowierzchniowym jest wdrożona wewnętrzna procedura prowadząca do zmniejszenia tego rodzaju incydentów. Bramy i drzwi obiektu pozostają zamknięte i są pod ochroną. Towar wwożony i wywożony (sprzedawany) jest kontrolowany zarówno przez ochronę, jak i system elektronicznych bramek

aktywacyjnych, które reagują na jawne bądź ukryte zabezpieczenia doczepiane do drogich towarów. Gabloty są zamykane. Działa również system ochrony fizycznej, w tym detektywi sklepowi, których zadaniem jest kontrola nie tylko klientów. Pracownicy poddawani są procedurom kontroli i nadzoru. Nie wolno im wnosić na teren sklepu (poza szatnię) pieniędzy, papierosów itp. towarów. Przy wyjściu do domu podlegają oni podwójnej kontroli. Podobnym zabiegom kontrolnym podlegają również pracownicy ochrony. W niektórych hipermarketach pracowników ochrony kontroluje dyrektor lub osoba przez niego upoważniona.

System elektroniczny sprawdzany jest na bieżąco. Sprawność bramek reagujących na magnetyczne zabezpieczenia kontroluje się dwa razy dziennie. Na bieżąco wymieniane jest również ustawienie kamer, tak aby mieć wgląd w miejsca, które uważa się za szczególnie zagrożone (np. te, gdzie znajduje się najwięcej pustych opakowań po spożytych towarach). Jednak bardzo rzadko jest zmieniany cały system.

Jak widać, na zapewnienie bezpieczeństwa przeznacza się wiele starań i duże nakłady finansowe. Co do zasady ochrona w obiektach handlowych traktowana jest na równi z działem handlowym i znajduje się w centrum zainteresowania dyrekcji. To właśnie dyrektor jest przede wszystkim odpowiedzialny za system bezpieczeństwa mienia. Większość z tych zabiegów jednak ma na celu zapobiegnięcie szkodom, jakie powoduje nieuczciwość klientów, dokonywane przez nich kradzieże, czyli działania z zewnątrz. Trzeba jednak pamiętać i to miała niniejsza praca podkreślić, że istnieje jeszcze inne zagrożenie, często o wiele większe, bo nieuświadomione i o wiele bardziej zakonspirowane – działanie nieuczciwego pracownika, które jak widać nie jest zjawiskiem marginalnym. Uderza ono w słaby punkt pracodawcy, bo wykorzystuje to, że pracodawca nie spodziewa się ataku albo lekceważy jego syndromy lub już zaistniałe przypadki. Dlatego bardzo ważne jest, aby zdać sobie sprawę z istnienia zagrożeń wewnętrznych i podjąć konieczne kroki, aby im przeciwdziałać (od szkolenia dla kadry zarządzającej aż po bardziej skrupulatny dobór kandydatów do pracy). Świadomość i zapobieganie (nawet przy dużych nakładach, jakie za sobą pociąga) jest wciąż bardziej opłacalne niż pokrywanie późniejszych strat.

Varia

Agnieszka Korotusz

Molestowanie seksualne i przemoc w miejscu pracy

Definicje molestowania seksualnego stworzono w celu zminimalizowania zjawiska molestowania i dyskryminacji kobiet w miejscu pracy. Podstawę definicji stworzyła United Stated Equal Employement Opportunity Commission (EEOC), według której molestowanie seksualne to „wszelkie niechciane nagabywanie na tle seksualnym, prośby o współżycie seksualne lub jakiekolwiek inne prośby o charakterze seksualnym, jeżeli podporządkowanie się im lub ich odrzucenie może bezpośrednio wpłynąć na status zawodowy lub jakość wykonywanej pracy przez nagabywaną osobę lub może wytworzyć wokół tej osoby wrogą atmosferę w miejscu pracy". Osobą molestowaną może być zarówno kobieta, jak i mężczyzna, jednak statystyki potwierdzają, że to kobiety najczęściej bywają ofiarami molestowania, zwłaszcza seksualnego. Osobą molestującą może być natomiast przełożony ofiary, pełnomocnik pracodawcy (zmieniłabym na przedstawiciela pracodawcy), kierownik innego działu, osoba niezatrudniona. Ofiara nie musi być osobą molestowaną, ale może być nią każdy, na kogo wpływa uwłaczające zachowanie (ofiara wtórna). Bezprawne molestowanie seksualne może nie powodować ekonomicznych strat dla przedsiębiorstwa w postaci straconych dni pracy, pieniędzy na rekonwalescencję ofiary, z drugiej strony może skończyć się zwolnieniem z pracy pracownika molestowanego. I tak się dzieje w większości przypadków. Zachowanie sprawcy musi być niepożądane. Aby mówić o molestowaniu, wymagany jest opór wobec sprawcy, inaczej mówiąc, ofiara musi wyrazić swój sprzeciw. Jak pisze Jarosław Warylewski: „Opór to przejaw braku zgody ofiary na zachowanie sprawcy i musi być on dostatecznie uzewnętrzniony". Trzeba podkreślić, iż przyjęło się błędnie uważać, że sprzeciw powinien przyjąć formę oporu fizycznego. Jednakże w niektórych sytuacjach opór

ten mógłby narazić ofiarę na jeszcze większe cierpienia, dlatego wystarczającym przejawem braku zgody powinien być sprzeciw werbalny, który ponadto jest wymagany zwłaszcza w takich sytuacjach jak zmuszanie ofiary do wysłuchiwania „nieprzystojnych propozycji" bądź znoszenia czy oglądania nieprzyzwoitych gestów. W tych sytuacjach opór fizyczny nie jest konieczny. Wyróżnia się dwa typy molestowania seksualnego: „coś za coś" i „wrogie środowisko". Molestowanie typu „coś za coś" (*quid pro quo*) występuje w przypadku, gdy podporządkowanie się lub odrzucenie seksualnych żądań pracodawcy wpływa na zatrudnienie, awans, utrzymanie pracy, degradację. Jest to groźba zmierzająca do pokonania oporu pokrzywdzonego i wystarczająco ukazująca ekonomiczne skutki molestowania seksualnego, gdyż chociażby pojedyncze seksualne napieranie może składać się na molestowanie seksualne, jeżeli jest połączone z przyznaniem lub odmową korzyści związanych z zatrudnieniem. Natomiast molestowanie typu „wrogie środowisko" (*hostile environment*), jak pisze dr hab. UŚ Eugenia Mandal, to niechciane, niepożądane przez osobę zainteresowanie seksualne lub ofensywne czy wrogie zachowania bezpośrednio skierowane pod jej adresem lub wobec jej płci, które przyczyniają się u niej do szkód, krzywd i obniżają efektywność pracy. Wrogie środowisko może być tworzone przez pracowników, klientów, a składa się z powtarzających żądań o seksualną przysługę, „nieprzystojnych pytań", wulgaryzmów, uwłaczających gestów, występowania przedmiotów o charakterze seksualnym (kalendarzy, zdjęć, czasopism). Istnieją dwa warunki, które powodują, iż pracodawcy są odpowiedzialni za wrogie środowisko. Pierwszy pracodawca wiedział lub powinien wiedzieć o molestowaniu, drugi pracodawca nie podjął właściwego działania zapobiegającego molestowaniu. Przypadki, w których pracodawca wiedział o molestowaniu, dotyczą m.in. zaistniałych wcześniej skarg na kierownictwo, molestowania otwarcie praktykowanego wśród pracowników. W niektórych przypadkach sądy USA stosują Reasonable Woman Standard, aby zdefiniowały pojęcie molestowania seksualnego, dlatego że kobiety częściej bywają ofiarami molestowania seksualnego niż mężczyźni i są w stanie wskazać, które formy „łagodniejszego" molestowania mogą być wstępem do bardziej

brutalnych zachowań. Mężczyźni, jako że rzadziej bywają ofiarami molestowania, inaczej postrzegają to zjawisko. Stąd sądy powinny spojrzeć na sprawę z punktu widzenia ofiary. Odmianami tych dwóch form molestowania są sytuacje, w których pracownicy, którzy nie są celem molestowania, tracą możliwość awansów w pracy na korzyść osób mniej wykwalifikowanych, ale godzących się na molestowanie (*quid pro quo third – party sexual harassement*), oraz sytuacje, w których pracownicy niemolestowani muszą pracować w atmosferze, w której molestowanie jest rozpowszechnione (*hostile environment third – party sexual harassement*). Konsekwencją stawiania na uprzywilejowanej pozycji osób molestowanych jest pogorszenie jakości wykonywanej pracy przez pozostałych pracowników, którzy w wyniku nieprzyjemnych warunków pracy rezygnują z niej. Według Unii Europejskiej molestowanie seksualne to „wszelkie formy niechcianego – werbalnego, niewerbalnego lub fizycznego-zachowania o charakterze seksualnym, którego celem lub skutkiem jest pogwałcenie godności osoby, zwłaszcza poprzez zastraszanie, wrogość, upodlanie, poniżanie lub obrażanie". W Polsce natomiast definicja molestowania pojawiła się stosunkowo niedawno w art. 18^{3a}§6 Kodeksu Pracy, mówiącym o dyskryminacji ze względu na płeć, na którą składa się każde nieakceptowane zachowanie o charakterze seksualnym lub odnoszące się do płci pracownika, którego celem lub skutkiem jest naruszenie godności lub poniżenie albo upokorzenie pracownika; na zachowanie to mogą się składać fizyczne, werbalne lub pozawerbalne elementy. Wcześniej definicję molestowania sformułowała Parlamentarna Grupa Kobiet, według której molestowaniem seksualnym jest nieakceptowane zachowanie o podłożu seksualnym, naruszające godność osoby molestowanej lub wywołujące atmosferę zastraszenia, upokorzenia lub wrogości, w szczególności gdy akceptacja takiego zachowania lub jej brak będzie stanowić podstawę decyzji dotyczącej osoby molestowanej. Jak widać, molestowanie seksualne może przybierać różne formy. Począwszy od najmniej drastycznych, molestowanie może polegać na gapieniu się na części ciała kobiety, komentarzach, żartach, gestach upokarzających seksualną naturę, pokazywaniu obrazków lub przedmiotów o charakterze seksualnym (*unwanted sexual attention*), do

coraz bardziej odrażających (nieakceptowanych) form, do których można zaliczyć niechciane dotykanie, szczypnięcia, chwytania, fizyczne seksualne ataki oraz rozpowszechnianie pornografii w miejscu pracy. Coraz więcej przypadków molestowania w Polsce wychodzi na jaw. Jednakże przestępstwa tego rodzaju to przestępstwa ścigane na wniosek, dlatego niewiele z nich zostaje ujawnionych przed sądem. Z jednej strony osoby molestowane niechętnie mówią o tym, co je spotkało, poruszanie tematu molestowania jest dla nich zbyt bolesne, z drugiej strony – pojawiają się trudności z udowodnieniem winy sprawcy, gdyż ani ofiara, ani ewentualni świadkowie nie są skłonni do mówienia z obawy przed utratą pracy. Trzeba również podkreślić, że ofiara przestępstwa seksualnego nie może skorzystać z bezpłatnej pomocy prawnej, która zapewniana jest jednak sprawcy przestępstwa. Ponadto, nawet gdy dochodzenie w sprawie zostanie wszczęte, z reguły trwa ono kilka miesięcy. W czasie tak długotrwałego postępowania ofiara przemocy narażona jest na powtórną wiktymizację. Pierwszy raz ofiara zostaje pokrzywdzona w momencie popełnienia przestępstwa, następnie może doznawać wielu upokorzeń i naruszeń swych praw zarówno w kontaktach z organami ścigania, jak i ze sprawcą. I tu pojawia się kolejny problem. W ciągu ostatnich kilkudziesięciu lat prokuratura była dosyć negatywnie nastawiona do ofiar przestępstw na tle seksualnym, zjawisko molestowania seksualnego wiązała z prywatnością, intymnością ofiary i nie wkraczała w nie bez pozwolenia ofiary. W latach dziewięćdziesiątych Centrum Praw Kobiet przeprowadziło sondaż wśród policjantów i prokuratorów, by zbadać ich nastawienie do ofiar przestępstw na tle seksualnym. Jedno z ciekawszych pytań, które zostało zadane w obu grupach zawodowych, brzmiało: Czy zdarza się, że dopuszczający się zgwałcenia mężczyźni działają w przekonaniu, że ich zachowanie jest sprzeczne z wolą kobiety? „Tak" odpowiedziało 57% prokuratorów oraz 64% policjantów. Ponadto decyzje sądów bywają zaskakujące, np. warszawski Sąd Pracy odmówił wypłaty milionowego zadośćuczynienia za molestowanie w pracy, gdyż stwierdził, że ofiara nie udowodniła faktu doznania krzywdy i traumy z powodu tego wydarzenia, natomiast sąd wrocławski, który sądził Zbigniewa L., byłego dyrektora jednego z wrocław-

skich teatrów, za molestowanie podległych mu pracownic, umorzył postępowanie ze względu na niewielką szkodliwość czynu. Jeszcze inny sąd uznał, że obmacywanie przez spodnie nie jest molestowaniem. Wspomnieć można jeszcze o umorzeniu postępowania przez prokuraturę rejonową, która stwierdziła, że dotykanie gołych pleców i górnej części pośladków nie jest molestowaniem, podobnie pocałowanie w szyję, przyciągnięcie do siebie czy nawet uchwycenie za krocze przez spodnie nie stanowi innej czynności seksualnej w znaczeniu prawnym.

Odpowiedzialność karna i przykłady molestowania seksualnego w środowisku pracy w Polsce

Warty przytoczenia jest przepis 199 Kodeksu Karnego, który mówi: „kto, przez nadużycie stosunku zależności lub wykorzystania krytycznego położenia, doprowadza inną osobę do obcowania płciowego lub do poddania się innej czynności seksualnej albo do wykonania takiej czynności, podlega karze pozbawienia wolności do lat 3". Takiej karze powinien podlegać między innymi kierownik nocnej zmiany w fabryce Frito Lay mieszczącej się w Grodzisku Mazowieckim, w której 8 pracownic straciło pracę. Kobiety wcześniej nie rozmawiały na ten temat, gdyż bały się, że staną się obiektem plotek albo stracą pracę. Po tym jak sprawa stała się głośna, dyrekcja grodziskiego zakładu postanowiła je zwolnić, zarzucając im kradzieże i nieobecności w pracy. Molestowanie tych pań polegało między innymi na kładzeniu ręki na ich kolanach i przesuwaniu w stronę majtek. Kolejnym przykładem na istnienie zjawiska molestowania w pracy jest skazanie 10 grudnia 2004 w Dzierżeniowie 10 mężczyzn za molestowanie pracownicy w fabryce Bielaw w Bielawie. Przez ponad rok mężczyźni wykorzystywali seksualnie pracownicę. Godziła się ona na to ze względu na groźbę utraty pracy. Szef pracownicy zmuszał ją do stosunków seksualnych raz w tygodniu, w zakładzie, zawsze w godzinach pracy. Wzywał ją do swojego biura lub magazynu. Gdy sprawa trafiła do prokuratury, kierownik zwolnił kobietę. Również w służbie zdrowia, w której odnotowuje się najwięcej przypadków użycia przemocy przez podopiecznych względem personelu, zdarzają się przypadki molestowania seksualnego, wspomnę tylko o chirurgu dziecięcym, dyrektorze Pogotowia Ratunkowego, który

przez ponad dwa lata wykorzystywał młode i dojrzałe pielęgniarki, salowe, sprzątaczki. Groził im pogorszeniem sytuacji materialnej, utratą pracy, jeśli będą mu się opierać. Doktor został skazany na rok i 4 miesiące w zawieszeniu na 4 lata. Mimo że odnotowuje się coraz więcej przypadków molestowania seksualnego w miejscu pracy w Polsce, to jest to jednak problem w znacznej części ukryty, o którym się nie mówi, a nawet unika się rozmowy związanej z tym zagadnieniem. Problem tym trudniejszy do zidentyfikowania i udowodnienia, gdyż molestowanie odbywa się zazwyczaj bez świadków i jest to przestępstwo godzące w wolność człowieka w zakresie najbardziej intymnej sfery jego życia. Kobieta ma prawo do ochrony swojej wolności seksualnej rozumianej nie tylko jako wolność „od czegoś", w tej sytuacji od niechcianego nagabywania, wszelkich nacisków ograniczających jej prawo do dysponowania swoim ciałem w sferze stosunków seksualnych, a także wolności „do czegoś" przejawiającej się w nakazie uszanowania prawa do seksualnego samostanowienia. Odpowiednie byłoby m.in. wprowadzenie przepisów, które w sposób realny zabezpieczałyby prawa osób molestowanych, wskazane byłoby również wprowadzenie legalnych definicji szantażu seksualnego, wrogiego środowiska i innych zjawisk. Trzeba również podkreślić, że polska literatura w kwestii molestowania seksualnego w miejscu pracy jest skromna, podobnie jeśli chodzi o orzecznictwo polskich sądów.

Przemoc w środowisku pracy (na podstawie badań w Stanach Zjednoczonych)

Obecnie stosuje się o wiele więcej przemocy niż w latach ubiegłych. FBI's Uniform Crime Reports wykazało, że w ciągu prawie 40 lat liczba przestępstw z użyciem przemocy wzrosła o 350%. Przywykliśmy do wiązania przemocy z gangami panującymi w „zurbanizowanych gettach", osobami handlującymi narkotykami, rodzinami patologicznymi, ale nie z miejscem pracy, z pracownikami. Biorąc pod uwagę chociażby ataki na Word Trade Center (1993, 2001) i Oklahomę (1995), bardziej skupiamy się na zwalczaniu przemocy z zewnątrz, pomijając ukrytą, na co dzień stosowaną przemoc wewnątrz przedsiębiorstwa. Z drugiej strony wydarzenia takie jak ataki, bombardowania, ostrzeliwania, które

nie zdarzają się na co dzień, powodują odwrócenie uwagi od sytuacji zachodzących wewnątrz organizacji, powodujących nie tylko fizyczne i psychiczne rany u pracownika, ale narażających również przedsiębiorstwo na straty finansowe, osłabienie produkcji i moralności w miejscu pracy, a także mogących prowadzić do cięższych nadużyć. Przestępstwa ukryte przypominają swoim charakterem nagłą i destrukcyjną naturę min lądowych. Zazwyczaj są niezauważalne, dopóki jedna z nich nie zostanie zdetonowana i nie zmieni miejsca pracy w niepewne, niezabezpieczone pole minowe. Eksplozja może spowodować rany cielesne, jak i doprowadzić do jeszcze bardziej niebezpiecznych sytuacji. Mimo to kierownictwo, pracownicy, ofiary bardzo często ignorują „miny lądowe". Przemoc w pracy może pochodzić z zewnętrznego i wewnętrznego źródła. Przestępcy, terroryści, zawiedzeni klienci mogą skierować swoją agresję w kierunku pracowników, mienia przedsiębiorstwa. Corocznie w latach 1992–1998 w USA dochodziło w godzinach pracy do 959 zabójstw, 23 235 ataków bez skutków śmiertelnych powodujących straty. W latach 1992–1996 National Crime Victim Survey (NCVS) oszacowało, że każdego roku dochodziło do 396 000 pobić, 84 000 kradzieży i 51 000 gwałtów i seksualnych ataków.

Słownik synonimów definiuje przemoc jako: 1. przymus, presja, nacisk, zmuszanie, siła; 2. przewaga; 3. prześladowanie, ucisk, tyrania, gnębienie, dyskryminacja, okupacja. Używane jest również pojęcie „agresja". Europejska Agencja Bezpieczeństwa i Zdrowia Publicznego uważa, że akty agresji lub przemocy mogą mieć formę nieprzyzwoitych zachowań charakteryzujących się brakiem szacunku dla innych, fizycznej lub słownej agresji – zamiaru zadania bólu oraz napaści – zamiaru skrzywdzenia innej osoby. Zdefiniowanie, czym jest przemoc w miejscu pracy, nasuwa dyskusje. Niektórzy chcieliby, aby definicja ta obejmowała język i działania, które powodują, że osoba czuje się niekomfortowo w miejscu pracy, inni, groźby i molestowanie. Wszyscy jednak uważają, że na pojęcie przemocy w miejscu pracy składają się wszelkie rany cielesne wyrządzone przez jedną osobę drugiej. Zatem przemoc w miejscu pracy to akt przemocy zawierający fizyczne ataki (napaści) i groźby ataków skierowane bezpośrednio do osoby w pracy lub na służ-

bie. Amerykańscy socjolodzy dokonali klasyfikacji aktów przemocy na: molestowanie, groźby, ataki fizyczne.

Zaobserwować można, że płeć pracownika wpływa na rodzaj stosowanej przemocy. Mężczyźni są bardziej narażeni na bycie ofiarami ekstremalnych form przemocy: morderstw, kradzieży, pobić, natomiast kobiety zwykle bywają ofiarami niechcianych seksualnych zachowań. Badania potwierdzają, że kobiety są ofiarami lżejszych form przemocy, narażone są bardziej na uderzenia, kopnięcia itp. Analizy NCVS przeprowadzone w latach 1987–1996 wykazały, że mężczyźni częściej atakowani są przez nieznane osoby, natomiast kobiety prawdopodobnie znają swoich oprawców. The National Violence Against Women Survey pokazała, że kobiety najczęściej bywają ofiarami przemocy o charakterze seksualnym stosowanej przez współpracowników. Szczególnie są one narażone na ataki ze strony partnerów (męża, byłego męża, chłopaka, byłego chłopaka), co jest przyczyną 1/6 zabójstw kobiet w USA (stan na 1992) i 13 000 konsekwencji z zachowaniem życia (stan na 1993 r.). Kobiety stanowią prawie 50% siły roboczej. Jednak zatrudnione są na niższych stanowiskach niż mężczyźni, mniej płatnych. To podporządkowanie sprawia, że są one bardziej podatne na odczuwanie przemocy. Predyktorzy przemocy (predyktor, z ang. *predictor* – pojęcie używane w psychologii, koncentrujące się na zbudowaniu sylwetki pracownika potencjalnie gwałtownego) preferują jako swoje ofiary kobiety na niższych stanowiskach, uważając je za słabsze, niższe rangą, podwładne. Te, które są młode i niezamężne, bywają w najgorszej sytuacji, łatwiejsze do zdominowania stają się równie łatwym celem.

NIOSH (1980–1992) objęło badaniem osoby w wieku od 16 do 93 lat. Największa liczba zabójstw wydarzyła się wśród pracowników w wieku 25–34 lat, podczas gdy procent zabójstw w miejscu pracy wzrósł wraz z wiekiem. Największe ryzyko zabójstw dotyczy pracowników w wieku 65 lat i wzwyż. W okresie 13 lat większość zabójstw w pracy popełniona była przy użyciu broni palnej (76%).

W zależności od okoliczności przemoc może pochodzić od niezadowolonego klienta, pacjenta, współpracownika, pracownika, pracodawcy, byłego partnera (np. byłego męża).

Metoda stosowania przemocy wyróżnia popełnianie aktów przemocy bez użycia narzędzi, jak na przykład popychanie na ścianę, przewrócenie na podłogę, kopanie, bicie, ściskanie, szczypanie, gryzienie oraz stosowanie przemocy z zastosowaniem różnych narzędzi, np. noży, broni palnej.

NIOSH wykazało, że zabójstwa w pracy stały się drugą po wypadkach samochodowych przyczyną śmierci osób w społeczeństwie amerykańskim, natomiast National Crime Victimization Survey wykazał, że blisko milion ludzi jest atakowanych w czasie pracy lub służby każdego roku; stanowi to 15% wszystkich aktów przemocy doświadczanej przez amerykańskich rezydentów powyżej lat 12. 75% wszystkich zabójstw w miejscu pracy w roku1993 było powiązanych z kradzieżami, natomiast ogólnie zabójstwa te stanowią 9% wszystkich zabójstw popełnianych w Stanach Zjednoczonych. National Traumatic Occupational Fatalities (NTOF) Surveillance System wskazał, że 9 937 zabójstw w miejscu pracy zostało popełnionych w latach od 1980 do 1992 roku. Na początku lat osiemdziesiątych liczba zabójstw uległa zmniejszeniu, jednakże w 1990 zaczęła wzrastać, powodując, że zabójstwa w pracy stały się drugą przyczyną zgonów wśród mężczyzn, natomiast główną przyczyną wśród pracujących kobiet. Większość żeńskich ofiar pracowała w sektorze sprzedaży detalicznej (46%) i w sektorze usług (22%). Większość ofiar męskich była zatrudniona przy sprzedaży detalicznej (36%) w sektorze usług (16%) oraz w administracji publicznej (11%), transporcie/komunikacji (11%). Według Europejskiej Agencji Bezpieczeństwa i Zdrowia w Pracy najbardziej narażonym na przemoc jest sektor usług, a w szczególności osoby zatrudnione w zakładach opieki zdrowotnej (pielęgniarki, sanitariusze, lekarze, zwłaszcza na nocnych zmianach), szkolnictwie, transporcie, sprzedaży detalicznej, cateringu i sektorze finansowym. W ostatnich latach oszacowano w Stanach Zjednoczonych, że pracownicy służby zdrowia są narażeni na szesnastokrotnie większe

ryzyko przemocy niż pracownicy innych sektorów, w Wielkiej Brytanii prawie 40% pracowników Narodowej Służby Zdrowia (NHS) było poniżanych w 1998, w Australii dwóch na trzech pracowników sektora zdrowotnego doświadczyło fizycznej lub psychicznej przemocy w 2001 roku. Według BLS Annual Survey of Occupational Injuries and Illnesses (ASOII) największa liczba aktów przemocy w roku 1992 dotyczyła sektora usług (zwłaszcza w domach opieki zdrowotnej, w zakładach opieki społecznej, szpitalach) i sprzedaży detalicznej (sklepy spożywcze, restauracje, bary).

Ostrzały albo eksplozje bomb prezentują dramatyczne, bezpośrednie i poważne problemy, które muszą być zdecydowanie i niezwłocznie rozpoznane. Konsekwencje „min lądowych" mogą wydawać się mniej bolesne, jednakże często okazują się fatalne dla ofiar przestępstw w miejscu pracy. Interwencja kierownictwa jest często bezplanowa z powodu niepewności, czy podjąć akcję i jaki ma ona mieć charakter. Zwłoka albo niewłaściwe odpowiedzi mogą okazać się gorsze w skutkach niż niepodjęcie żadnego działania. „Miny lądowe" mogą nie pozostawiać żadnych blizn, z drugiej zaś strony mogą doprowadzić do głębokich, emocjonalnych i psychologicznych ran. Ofiary mogą cierpieć na bezsenność, odczuwać ciągłe napięcie, nerwowość, złość, zastraszenie, niskie poczucie własnej godności, depresję, niepokój, odseparowanie, pourazowe zaburzenie stresowe. Prawie 1/3 ofiar ukrywa swoje leczenie psychologiczne, a prawie 20% odchodzi z pracy, przenosi się lub jest zwalniana. Powtarzające się „miny lądowe" mogą doprowadzić do niszczycielskich strat finansowych, obniżenia produktywności (wydajności), serii pracowniczych/kierowniczych konfliktów. We wszystkich większych organizacjach są one ukryte. Pytanie, jak je znaleźć, zanim zostaną zdetonowane. Zbyt dużo organizacji nie wykorzystuje możliwości sprawdzenia kryminalnej historii swoich kandydatów, co daje możliwość szybkiego wychwycenia agresji w początkowej fazie. Pozornie nieszkodliwe, mniejsze albo wydarzające się raz na jakiś czas mogą doprowadzić do bardziej agresywnych form przemocy. Mimo polityki stanowej dla przeciwieństwa, wielu pracowników, jak i ich przełożonych

nie poczuwa się do informowania o „minach lądowych". Strach, ryzyko utraty pracy, zemsta współpracowników zniechęcają ofiary molestowania do zgłaszania tych zdarzeń. Ataki współpracowników, partnerów, są często spostrzegane jako żenujące zachowania należące do prywatnych spraw ofiary. Nie ma oficjalnego rejestru „min lądowych". Trzeba je znaleźć, badając pracownika, szanując jednocześnie jego wrażliwość i osobistą naturę.

Najbardziej narażone na przemoc są osoby osamotnione w pracy, młodzi, dobrze wykształceni pracownicy, którzy mogą stanowić zagrożenie dla przełożonych m.in. o ustalonej pozycji zawodowej, osoby wyróżniające się od pozostałych chociażby pod względem poglądów politycznych, nietypowym strojem, osoby sumiennie i bardzo dobrze wykonujące swoją pracę. Wzrost przemocy mogą powodować także takie czynniki, jak praca w obszarach o wysokiej przestępczości, w godzinach nocnych, związana z publiczną wypłatą pieniędzy, indywidualna lub w małych zespołach, związana z ochroną mienia o wysokiej wartości.

W celu zminimalizowania przemocy w środowisku pracy Europejska Agencja Bezpieczeństwa i Zdrowia Publicznego zaleca m.in. wprowadzenie fizycznych środków ochrony, takich jak: zamki, osłony, zainstalowanie systemu kamer monitorujących, odpowiedniego oświetlenia, lepszej organizacji pracy związanej z regularnym usuwaniem ze stanowisk pracy gotówki i cennych przedmiotów; korzystanie z rozwiązań bezgotówkowych oraz szkolenia i informowania personelu w zakresie rozpoznawania niedopuszczalnych zachowań oraz wczesnych zachowań agresji.

Bibliografia

European Agency for Safety and Heath at Work, „Factsheet" 2002, No 24: *Violence at work*.

Gay Anderson D., Westneat S. and Reed D., *Workplace Violence against Female Long- haul Truckers*, „Security Journal" 2005, 18 (2), 31–38.

Kenny J.F., *Workplace Violence and the Hidden Land Mines: A Comparision of Genre Victimization*, „Security Journal" 2005, 18 (1), 55–56.

Kędzia B.B., Kowalewski S., *Przemoc – nowy „czynnik ryzyka zawodowego" w środowisku pracy*, Centralny Instytut Ochrony Zdrowia, „Bezpieczeństwo Pracy" 2002, nr 1.

Kędzia B.B., Kowalewski S., *Przemoc – nowy „czynnik ryzyka zawodowego" w środowisku pracy*, „Bezpieczeństwo Pracy. Nauka i Praktyka" 2002, nr 1 (366).

Kobiety w Polsce w latach 90., Raport Centrum Praw Kobiet, Warszawa 2000.

Kodeks karny. Część szczególna, t. 1, Komentarz do art. 117–221 kk, red. A. Wąsek, wyd. 2, Warszawa 2004 („Duże Komentarze Becka").

Kodeks karny. Część szczególna, t. 2, Komentarz do art. 117–221 kk, red. A. Zoll, wyd. 2, Kraków 2006 („Komentarze Zakamycza").

Mandal E., *Molestowanie seksualne w miejscu pracy*, „Czasopismo Psychologiczne" 2001, t. 7, nr 1.

Słownik synonimów, red. Z. Kurzowa, Warszawa 2006.

The National Institute for Occupational Safety and Health, dane statystyczne organizacji dostępne na: http://www.cdc.gov/niosh.

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny.

Warylewski J., *Molestowanie seksualne w miejscu pracy*, Sopot 1999.

Monika Suchodaj

Poczucie bezpieczeństwa właścicieli gospodarstw rolnych

Celem moich badań było uzyskanie obrazu poglądów właścicieli gospodarstw rolnych na niektóre kwestie dotyczące bezpieczeństwa tych gospodarstw. Badaniu w formie ankiety poddałam 33 średniotowarowe gospodarstwa w powiecie staszowskim. Przedstawię jedynie najważniejsze spostrzeżenia wynikające z przeprowadzonego pilotażu.

Poziom przestępczości na wsiach jest niski, zatem rolnicy nie zabezpieczają swoich gospodarstw przed ewentualną kradzieżą lub włamaniem. Jest to także zbyt kosztowne w porównaniu z ich dochodami. Poza tym wieś jest miejscem, w którym żadne informacje nie są anonimowe, wszystko jest rozpowszechniane, zatem miejscowi drobni przestępcy nie mogą liczyć na powodzenie. Zdarzają się jednak dość liczne przypadki kradzieży sprzętu rolniczego, którego miejsce przechowywania znają tylko najbliżsi sąsiedzi. Daje to dużo do myślenia. Dlatego też trudno powiedzieć, kto stwarza większe zagrożenie, okoliczni mieszkańcy czy działający przestępcy z zewnątrz. Gospodarze rolni sądzą, że mogą liczyć jedynie na siebie, działania policji w zgłaszanych sprawach okazują się bowiem nieskuteczne, gdyż ich zdaniem rzadko kiedy policja rzetelnie przeprowadza śledztwa i dochodzenia. Istnienie takiego przekonania jednoznacznie potwierdziły moje badania.

Natomiast duży problem stanowi tzw. przestępczość ukryta (pośrednia). Według przeprowadzonych badań aż 22 z 33 osób nie wierzy w uczciwość pracowników Agencji Restrukturyzacji i Modernizacji Rolnictwa. Uważają oni, że jest ona instytucją skorumpowaną, uniemożliwiającą korzystanie z dostępnych dla rolników dotacji i pomocy, zatrudniającą wielu niepotrzebnych pracowników. Ponadto badani

przeze mnie właściciele przedsiębiorstw rolnych są przeświadczeni, że generalnie funkcjonowanie urzędów administracji publicznej w opinii tych, którzy załatwiali w nich jakieś sprawy, jest raczej kiepskie. Około połowa badanych stwierdziła również, że władze gminy nie współpracują z mieszkańcami przy rozwiązywaniu problemów lokalnych, albo przynajmniej nie spotkali się bezpośrednio z jakąkolwiek formą współpracy, albo też informacja o tego typu działaniach jest niedostateczna.

Innym zagrożeniem dla przedsiębiorstw rolnych są częste tzw. oszustwa towarowe w rolnictwie. Rolnicy uważają, że np. nawozy sztuczne i środki ochrony roślin są fałszowane, mają znacznie niższą jakość, niż wynika to z opisu na opakowaniu. Podobnie jest z nasionami roślin uprawnych, które często są albo słabej jakości, podatne na choroby, albo jest ich mniej, niż podaje informacja na opakowaniu. Według badanych tego rodzaju oszustw towarowych jest mnóstwo. Jako przykład podam sytuację, w której zamiast deklarowanych 1000 sztuk nasion w jednym opakowaniu było ich z reguły 960–970, co przy cenie 1 zł za sztukę nasiona daje złodziejowi wysokie zyski.

Paradoksem jest fakt, że mimo przekonania o tak licznych oszustwach towarowych w rolnictwie większość przedsiębiorców nie stara się uzyskać informacji o potencjalnym partnerze przed podjęciem kontaktów handlowych. Jest to nieco inne zagadnienie, ale świadczy o lekceważeniu istotnego zagrożenia. Zasięganie informacji o partnerach handlowych np. w wywiadowniach gospodarczych czy w innych, podobnych źródłach praktycznie się nie zdarza.

Bardzo ważnym, a przede wszystkim powszechnie znanym zjawiskiem jest bezrobocie. Bezrobocie na wsi stanowi jeden z najtrudniejszych problemów społeczno-gospodarczych, choć sprawa ocen tego zjawiska jest skomplikowana. Kobiety w przeprowadzonych przeze mnie ankietach w 100% odpowiedziały, że bezrobocie na wsi jest duże. Natomiast bardziej ostrożniejsi byli mężczyźni i nie wszyscy odpowiadali, że jest duże, gdyż według nich, jeżeli nie ma kogo zatrudnić do pracy, to bezrobocie nie istnieje. Związek między poglądami na natężenie bezrobocia a płcią badanych osób okazał się statystycznie istotny. W społeczności wiejskiej występuje głównie bezrobocie utajone. Obja-

wia się ono tym, że ludzie zrezygnowali z poszukiwania pracy z powodu nieskuteczności swoich usiłowań. Przyczynia się do tego również niskie wykształcenie. Mężczyźni mają przeważnie wykształcenie zawodowe, u kobiet jest ono nieco wyższe, gdyż prawie połowa kobiet posiada już wykształcenie średnie. Nie jest to wynik satysfakcjonujący, a jeszcze bardziej niepokoi to, że większość badanych osób uznało swoje kwalifikacje za wystarczające, a mniej za częściowo wystarczające. W okresie gwałtownego rozwoju technologii kwestia wykształcenia powinna być sprawą szczególnie ważną, dlatego zatrważające jest zarówno niskie wykształcenie ludności wiejskiej, jak i to, że nie odczuwają potrzeby podnoszenia swoich kwalifikacji. Najwyższa pośród grup demograficznych stopa bezrobocia występuje wśród młodzieży kończącej naukę. Łatwo zauważyć, że właśnie ludzie tej grupy wiekowej popełniają największą liczbę przestępstw, co spowodowane jest brakiem źródeł utrzymania. Główną cechą obszarów wiejskich jest monofunkcyjność gospodarki opartej na małych i średnich przedsiębiorstwach rolnych.

Ludność wiejska zakłada niewielkie, rodzinne przedsiębiorstwa nastawione na produkcję roślin uprawnych, z których stara się utrzymać całe rodziny. Stanowią one niemal połowę ogólnej liczby małych i średnich przedsiębiorstw. Jednak postępujące procesy globalizacji i integracji gospodarki światowej stwarzają coraz trudniejsze warunki do działania drobnym przedsiębiorcom. Gospodarstwa rolne w Polsce cechuje słabość techniczna, technologiczna i informatyczna. Do najważniejszych ograniczeń rozwojowych zaliczyć należy przede wszystkim brak stabilizacji cen, utrudniony dostęp do kredytów bankowych, które i tak są bardzo drogie, a również rozdrobnienie struktury handlu detalicznego i infrastruktury hurtowej hamujące budowę zintegrowanych łańcuchów dostaw. Istnieje także niski poziom koncentracji i charakterystyczna dla polskiego rolnika niewielka skłonność do wspólnego działania. Dlatego nic dziwnego, że 30 z 33 osób badanych na pytanie, czy chciałyby skorzystać z porad rzetelnych doradców do spraw produkcji rolnej, odpowiedziały – tak. Pozostałe 3 osoby, które nie zadeklarowały zamiaru skorzystania z porad, uważają, że nie istnieją rzetelni, uczciwi doradcy.

Wśród producentów rolnych panuje silne przekonanie, że mimo występowania tak ogromnego bezrobocia na wsi niestety nie ma chętnych do pracy. Ciekawe jest, że ludzie w większości uważają, że zatrudnianie cudzoziemców jest korzystniejsze ekonomicznie niż zatrudnianie mieszkańców okolicy, jednak zatrudniają ich bardzo rzadko. Być może spowodowane jest to brakiem warunków niezbędnych do zakwaterowania pracownika. Większość tych drobnych przedsiębiorstw radzi sobie z brakiem dobrego pracownika na tzw. zasadzie wzajemnej samopomocy. Uważa się także, iż cudzoziemcy stwarzają mniejsze zagrożenie dla bezpieczeństwa gospodarstwa niż mieszkańcy okolicy.

Rzeczywistość gospodarcza nie jest oceniana przez rolników jako korzystna. Większość właścicieli ocenia obecną sytuację jako sprzyjającą wprowadzeniu zmian we własnym gospodarstwie, a także, że obecne warunki sprzyjają podejmowaniu działalności nowego rodzaju. Osąd taki wydaje się optymistyczny, gdyż takie postrzeganie rzeczywistości gospodarczej może stymulować podejmowanie aktywności nowego typu. Okazało się jednak, że niewielki procent badanych osób w ciągu ostatnich lat podjęło działalność nowego typu. Podstawową przyczyną tak małej przedsiębiorczości badanych osób okazał się brak pieniędzy, brak odwagi, brak przykładu, ale również przyzwyczajenie się do takiego stanu, jaki istnieje i brak nadziei na poprawę. W grę wchodzi również trwałość podstawowych wartości uznawanych w kulturach wiejskich: ziemia, praca, rodzina. Odejście od tak silnie zakorzenionej wartości, jaką jest praca na roli, jest bardzo trudnym procesem. Dlatego też tak wiele osób decyduje się na formę przedsiębiorczości związaną z produkcją rolną.

Wnioski końcowe:

1. Mimo wyraźnie lepszej niż w miastach sytuacji kryminologicznej terenów rolniczych poczucie bezpieczeństwa rolników jest dość niskie, choć ma to przyczyny raczej socjalne niż inne.

2. Wyraźny wzrost przestępczości i słabnące poczucie bezpieczeństwa, ujawniające się na co dzień, nie dotarły jeszcze do prywatnych średnich gospodarstw rolnych w stopniu znacznym.

3. Zdarzające się dość rzadko włamania na teren przedsiębiorstwa czy zniszczenia lub zabranie środków i sprzętu są spowodowane pijaństwem i zawiścią ludzi, a także próbą bezprawnego wzbogacenia się.

4. Bezrobocie rodzi oceny paradoksalne – mimo wysokich wskaźników notorycznie zgłaszany jest brak rąk do pracy.

5. Powszechne jest przekonanie, iż instytucje powołane do wsparcia rolnika, są skorumpowane (np. ARiMR), a inne, jak Policja – nieskuteczne.

6. Ze względów ekonomicznych nowoczesne środki bezpieczeństwa biznesu są całkowicie badanej przeze mnie grupie rolników niedostępne, od dawna potrzebna jest modernizacja przedsiębiorstw rolnych oraz wielofunkcyjny rozwój wsi.

7. Mimo formalnie istniejących instytucji doradztwa w zakresie przedsiębiorczości w gospodarstwach rolnych, właściciele tych przedsiębiorstw nie mają pojęcia o ich istnieniu. Zadaniem takich instytucji jest wspieranie małej i średniej przedsiębiorczości w udzielaniu konsultacji i porad z zakresu działalności gospodarczej, przygotowanie wniosków kredytowych, prowadzenie szkoleń z organizacji i zarządzania własnym przedsiębiorstwem rolnym, inwestowania, zaplecza konkurencyjnej bazy surowcowej; niestety faktycznie takowe nie istnieją.

Magdalena Słota

Narkotyki w polskich przedsiębiorstwach

Cel badania

Współcześnie narkomania stała się jednym z problemów, z jakimi boryka się społeczeństwo. Jest wiele przyczyn sięgania po środki odurzające. Brak akceptacji, narastające tempo życia, wymagania stawiane uczniom i studentom, a także pracownikom mogą ich skłonić do sięgnięcia po narkotyki, które chwilowo pozwalają odsunąć myśli o nieprzyjemnych sytuacjach, dają możliwość psychicznej ucieczki od rzeczywistości. Niestety na krótko i za wysoką cenę.

Problem ten jest rozpowszechniony głównie wśród ludzi młodych, co jest przedmiotem licznych badań[1]. Jednak (przynajmniej w Polsce) nie mówi się o jego występowaniu w grupie ludzi starszych pracujących zawodowo. Celem moich badań było ustalenie, jak przedsiębiorcy zareagowaliby na wystąpienie takiego problemu, jakie są ich poglądy na zażywanie narkotyków, czy są przygotowani na pojawienie się takiego problemu.

Należy zwrócić uwagę, że do grupy narkotyków zaliczamy nie tylko popularne substancje syntetyczne, takie jak amfetamina, kokaina czy naturalne – liście konopi indyjskich[2], ale także tytoń i alkohol, które należą do legalnych środków odurzających[3].

---

[1] www.narkomania.gov.pl/epidemiologia.htm.

[2] Opis działania tych i innych substancji zob. w: W. Wanat, *Odlot donikąd. Narkotyki i narkomania*, Warszawa 2004.

[3] Badanie jednak ich nie uwzględnia.

Metoda badania

Badanie przeprowadzone za pomocą anonimowej ankiety objęło przedsiębiorstwa różnych regionów Polski, których zakłady różniły się zarówno pod względem liczby zatrudnionych pracowników, lokalizacji miejsca pracy, jak i branży. Dzięki temu można było uzyskać w miarę obiektywne wyniki. Jednak spośród wszystkich testowanych zakładów większość znajduje się na terenie województwa śląskiego, które ze względu na swój rozwój przemysłowy i wysokie zaludnienie wydało mi się bardzo atrakcyjne do przeprowadzenia takiego badania.

Część pierwsza ankiety składająca się z czterech pytań pozwoliła na podzielenie przedsiębiorców na grupy, odpowiednio według płci, rodzaju wykształcenia, stażu pracy i lokalizacji przedsiębiorstwa. Druga część składała się z dziewięciu pytań, z kilkoma możliwymi odpowiedziami jednokrotnego wyboru. W przypadku nieudzielenia odpowiedzi bądź zakreślenia więcej niż jednej odpowiedzi[4] została ona uznana za nieważną. Poniżej zamieszczono ww. ankietę:

ANKIETA
NARKOTYKI W MIEJSCU PRACY

Prosimy o podanie kilku podstawowych informacji o sobie, dane te posłużą wyłącznie do celów naukowych. Ankieta jest całkowicie anonimowa.

A. PŁEĆ:
- ❑ kobieta,
- ❑ mężczyzna.

B. WYKSZTAŁCENIE:
- ❑ podstawowe,
- ❑ zawodowe,
- ❑ średnie,
- ❑ wyższe.

[4] Nie dotyczy pytania 1.

C. OGÓLNY STAŻ PRACY:
- ❑ do 5 lat,
- ❑ 5–10 lat,
- ❑ 10–15 lat,
- ❑ 20 lat i więcej.

D. LOKALIZACJA MIEJSCA PRACY:
- ❑ wieś,
- ❑ miasto 20–50 tys. mieszkańców,
- ❑ miasto 50–100 tys. mieszkańców,
- ❑ miasto 100–200 tys. mieszkańców,
- ❑ miasto powyżej 200 tys. mieszkańców.

1. Do jakiej dziedziny zalicza się Pana/Pani miejsce pracy?
- ❑ służba zdrowia,
- ❑ nauka/ szkolnictwo,
- ❑ handel,
- ❑ budownictwo,
- ❑ bankowość/ubezpieczenia,
- ❑ administracja,
- ❑ transport,
- ❑ turystyka,
- ❑ usługi,
- ❑ rzemiosło,
- ❑ telekomunikacja/informatyka,
- ❑ energetyka,
- ❑ górnictwo,
- ❑ hutnictwo,
- ❑ marketing/reklama,
- ❑ służby mundurowe,
- ❑ inne.

2. Czy uważa Pan/Pani, że problem narkotyków występuje w Pana/Pani miejscu pracy?
- ❑ tak,
- ❑ nie.

Jeśli TAK, to czy uważa Pan/Pani, że problem ten jest:

- ❑ duży,
- ❑ raczej duży,
- ❑ raczej niewielki,
- ❑ niewielki.

3. Czy jeśli obserwuje Pan/Pani ten problem, to w jakiej grupie pracowników on występuje?
- ❑ osób pracujących fizycznie,
- ❑ osób pracujących umysłowo,
- ❑ w obu ww. grupach w podobnym nasileniu.

4. Co zdaniem Pana/Pani jest przyczyną korzystania z narkotyków?
- ❑ problemy osobiste,
- ❑ problemy w miejscu pracy,
- ❑ inne.

5. Czy sądzi Pan/Pani, że narkotyki pozwalają rozwiązywać problemy zawodowe?
- ❑ tak,
- ❑ nie,
- ❑ czasami.

6. Czy w Pana/Pani miejscu pracy wystąpił kiedyś problem wynikający z zażywania środków odurzających przez pracowników?
- ❑ tak,
- ❑ nie.

Jeśli TAK, czy usiłowano na drodze służbowej wyjaśnić, skąd ten problem się pojawił?
- ❑ tak,
- ❑ nie.

Czy próbowano udzielić pomocy osobie, której ten problem dotyczył?
- ❑ tak,
- ❑ nie.

7. Czy sądzi Pan/Pani, że zażywanie narkotyków pozytywnie wpływa na efektywność pracy?
- ❑ tak,

- ❑ nie,
- ❑ nie mam zdania.

Czy może ono mieć wpływ na zachowanie wobec innych współpracowników?

- ❑ tak,
- ❑ nie,
- ❑ nie mam zdania.

8. Czy sądzi Pan/Pani, że osoby zażywające narkotyki w pracy powinny:

- ❑ zostać zwolnione dyscyplinarnie (niezależnie od odpowiedzialności karnej),
- ❑ zostać skierowane na leczenie i zwolnione,
- ❑ zostać skierowane na leczenie i otrzymać bezpłatny urlop,
- ❑ nie mam zdania.

9. Czy sądzi Pan/Pani, że powinny być organizowane szkolenia pracowników mające na celu ochronę przed skutkami narkomanii?

- ❑ tak,
- ❑ nie,
- ❑ nie mam zdania.

Wyniki

Ankietowani przedsiębiorcy mają w 71,4% wykształcenie wyższe, w 28,6% – średnie. Są to głównie mężczyźni (67,9%). Najwięcej przedsiębiorstw znajduje się w miastach, których liczba mieszkańców wynosi od 20 do 50 tysięcy (50%). Mniej liczną grupę stanowili przedsiębiorcy ze wsi oraz dużych miast o liczbie mieszkańców powyżej 200 tys. (ok. 18%); 100–200 tys. mieszkańców (10,7%), a najmniejszy odsetek to przedsiębiorcy z miast, których liczba ludności wynosi od 50 do 100 tys. mieszkańców (3,5%). Staż pracy ankietowanych w ok. 54% wynosi powyżej 20 lat; około 18% ankietowanych pracuje zawodowo od 5 do 10 lat. Staż pozostałej grupy przedsiębiorców (kategoria do 5 lat oraz 10–15 lat) wynosi 14,3%.

W toku badań, za pomocą testu χ^2 (poziom istotności wynosił α=0,05; próg zależności: 3,841) testowałam 20 hipotez zerowych:

$\mathbf{H_0^1}$ – Nie ma związku pomiędzy występowaniem narkotyków w przedsiębiorstwie a miejscem jego lokalizacji.

$\mathbf{H_0^2}$ – Nie ma związku między płcią ankietowanych a tym, w jakiej ich zdaniem grupie narkotyki występują.

$\mathbf{H_0^3}$ – Nie ma związku między stażem przedsiębiorców a ich poglądem na to, w jakiej grupie pracowników występują narkotyki.

$\mathbf{H_0^4}$ – Nie ma związku pomiędzy płcią przedsiębiorców a ich poglądem na to, jaka jest przyczyna korzystania z narkotyków.

$\mathbf{H_0^5}$ – Nie ma związku między wielkością miasta, gdzie przedsiębiorstwo się znajduje, a poglądem ankietowanych na to, jaka jest przyczyna korzystania z narkotyków.

$\mathbf{H_0^6}$ – Nie ma związku między stażem przedsiębiorców a ich poglądem na to, czy narkotyki pozwalają rozwiązywać problemy zawodowe.

$\mathbf{H_0^7}$ – Nie ma związku między wystąpieniem problemu z narkotykami w przedsiębiorstwie a jego lokalizacją.

$\mathbf{H_0^8}$ – Nie ma związku między poglądem przedsiębiorców na to, czy narkotyki wpływają na efektywność pracy, a ich płcią.

$\mathbf{H_0^9}$ – Nie ma związku między poglądem przedsiębiorców na to, czy narkotyki wpływają na efektywność pracy, a ich stażem.

$\mathbf{H_0^{10}}$ – Nie ma związku między poglądem przedsiębiorców na to, czy narkotyki wpływają na efektywność pracy, a lokalizacją przedsiębiorstwa.

$\mathbf{H_0^{11}}$ – Nie ma związku między płcią przedsiębiorców a ich zdaniem na temat, czy zażywanie narkotyków wpływa na zachowanie wobec innych współpracowników.

$\mathbf{H_0}^{12}$ – Nie ma związku między stażem przedsiębiorców a ich zdaniem na to, czy zażywanie narkotyków wpływa na zachowanie wobec innych współpracowników.

$\mathbf{H_0}^{13}$ – Nie ma związku między lokalizacją przedsiębiorstwa a zdaniem przedsiębiorców na to, czy zażywanie narkotyków wpływa na zachowanie wobec innych współpracowników.

$\mathbf{H_0}^{14}$ – Nie ma związku między płcią przedsiębiorców a ich próbą wyjaśnienia na drodze służbowej, skąd pojawił się problem zażywania narkotyków.

$\mathbf{H_0}^{15}$ – Nie ma związku między stażem przedsiębiorców a ich próbą wyjaśnienia na drodze służbowej, skąd pojawił się problem zażywania narkotyków.

$\mathbf{H_0}^{16}$ – Nie ma związku pomiędzy płcią przedsiębiorców a prawdopodobnym sposobem ich postępowania wobec pracowników, którzy mają problem z narkotykami.

$\mathbf{H_0}^{17}$ – Nie ma związku pomiędzy wykształceniem przedsiębiorców a prawdopodobnym sposobem ich postępowania wobec pracowników, którzy mają problem z narkotykami.

$\mathbf{H_0}^{18}$ – Nie ma związku pomiędzy lokalizacją przedsiębiorstwa a prawdopodobnym sposobem postępowania przedsiębiorcy wobec pracowników, którzy mają problem z narkotykami.

$\mathbf{H_0}^{19}$ – Nie ma związku pomiędzy stażem przedsiębiorców a ich chęcią organizowania szkoleń pracowników, mających na celu ochronę przed skutkami narkomanii.

$\mathbf{H_0}^{20}$ – Nie ma związku pomiędzy lokalizacją przedsiębiorstwa a chęcią przedsiębiorców do organizowania pracownikom szkoleń, mających na celu ochronę przed skutkami narkomanii.

W trzech przypadkach stwierdziłam brak podstaw do ich odrzucenia, tym samym wykazując następujące, statystycznie istotne zależności. Zatem *Istnieje związek między stażem przedsiębiorców a ich poglądem na to, czy narkotyki pozwalają rozwiązywać problemy zawodowe.*

Przedsiębiorcy, których staż pracy wynosi powyżej 10 lat, zgodnie odpowiadają, że narkotyki nie rozwiązują problemów zawodowych, co daje powody do zadowolenia, jednak 25% z przedsiębiorców, których staż pracy jest mniejszy niż 10 lat, twierdzi, że środki odurzające czasami mogą pomóc w rozwiązywaniu tychże problemów. Należy zwrócić uwagę na fakt, że rozpowszechnienie narkotyków nastąpiło w ciągu ostatnich kilku lat. Można przypuszczać, że pogląd ten wynika z prawdopodobnej styczności młodszego pokolenia przedsiębiorców z narkotykami. Jednak należy pamiętać, co już wcześniej nadmieniłam, że w sytuacjach trudnych narkotyki przynoszą chwilową „ulgę", a ich permanentne zażywanie prowadzi do nałogu. Dlatego warto pomyśleć np. o szkoleniach mających na celu ochronę przed skutkami narkomanii (chęć ich organizacji deklaruje 75% ankietowanych). Profilaktyka bowiem może zabezpieczyć zarówno przedsiębiorców, jak i pracowników przed uzależnieniem.

Istnieje związek między płcią przedsiębiorców a prawdopodobnym sposobem ich postępowania wobec pracowników, którzy mają problem z narkotykami.

75% ankietowanych mężczyzn zwolniłoby pracownika, który zażywa środki odurzające. Mniej rygorystyczne pod tym względem okazały się kobiety, które skierowałyby taką osobę na urlop w celu wyleczenia się z nałogu (80%).

Ważne jest odpowiednie postąpienie z pracownikiem, który zażywa narkotyki. Zwolnienie z pracy może u takiej osoby wywołać uczucie odrzucenia, co spowoduje pogłębienie się nałogu, a nie podjęcie próby leczenia. Najlepszym sposobem pomocy jest rozmowa, najlepiej z psychologiem; wyjaśnienie, co skłoniło pracownika do sięgnięcia po środki

odurzające. Stanowcza próba skierowania takiej osoby na leczenie bez uprzedniej konwersacji może zakończyć się fiaskiem. Osoba uzależniona odbiera to jako atak na siebie, przy tym najczęściej tłumacząc się, że ten nałóg jej nie dotyczy. Prawdopodobnie zacznie się wtedy buntować. Psycholodzy przyznają, że w niektórych przypadkach takie osoby muszą „zejść na dno", aby zrozumieć konsekwencje zażywania środków odurzających.

Prywatnie przedsiębiorcy twierdzą, że skierowanie osoby na leczenie jest lepszym rozwiązaniem, zwłaszcza jeśli mają zaufanie do pracownika i jeśli pracownik sprawdza się w przedsiębiorstwie.

Istnieje związek pomiędzy płcią przedsiębiorców a ich poglądem na to, że zażywanie narkotyków ma wpływ na zachowanie wobec innych współpracowników.

Ankietowane kobiety zgodnie opowiadają się za tym, że narkotyki wpływają na zachowanie się osoby wobec innych współpracowników, natomiast zdaniem 35% mężczyzn takiego wpływu na zachowanie wobec innych nie ma.

Wpływ środków odurzających na zachowanie człowieka jest uzależniony od rodzaju narkotyku. Na przykład marihuana według specjalistów wprowadza w stan zadowolenia, jednak powoduje obniżoną zdolność ruchową, w przeciwieństwie do amfetaminy lub LSD, które wprowadzają w stan euforii i pobudzają zdolności psychofizyczne. Ecstasy powoduje poczucie silnej więzi z otoczeniem i empatię w stosunku do innych. Jednak każdy z ww. środków oprócz pozornie „pozytywnych" efektów działania może wywoływać stany depresyjne oraz niepokój mogący przerodzić się w panikę, a także spowodować agresję wobec innych. Dlatego też nie zawsze, aczkolwiek często, mogą mieć wpływ na zachowanie wobec osób trzecich, z czym nasi przedsiębiorcy powinni się liczyć.

Podsumowanie wyników

Wśród ankietowanych przedsiębiorców 100% uważa, że w ich firmach nie występuje problem zażywania narkotyków, a tylko 7% ankietowanych przyznało, że taki problem wystąpił. Można by przypuszczać, że środki odurzające, mimo że w dzisiejszych czasach tak bardzo rozpowszechnione, nie są popularne w miejscach pracy w Polsce albo że pracodawcy nie są świadomi możliwości ich zażywania przez pracowników. Przy coraz większej konkurencji na rynku pracy nie można sobie pozwolić na utratę zaufania pracodawcy. Patrząc jednak na drugą stronę medalu: osoby, które nie są wystarczająco odporne na stres i narastające tempo pracy, coraz częściej będą sięgać po środki wspomagające.

Ankietowani przedsiębiorcy boją się wyraźnie o bezpieczeństwo swoje i swoich pracowników, opowiadając się w 75% za przeprowadzeniem szkoleń mających na celu ochronę przed skutkami narkomanii, co oczywiście bardzo cieszy. Jednak musieliby prawdopodobnie zadbać o ich organizację na własną rękę, ponieważ władze państwa na dzień dzisiejszy nie dostrzegają potrzeby szkolenia ich w zakresie zapobiegania i rozprzestrzeniania się narkomanii w przedsiębiorstwach. Możemy mieć tylko nadzieję, że potrzeba programowego szkolenia, dostarczania wiadomości o szkodliwości narkotyków przyczyni się do dostrzeżenia problemu, co wpłynie na powiększenie się liczby placówek zajmujących się walką z narkomanią, nie tylko wśród młodzieży.

Na koniec trzeba zaznaczyć, że anonimowa ankieta, którą posłużyłam się do przeprowadzania badania, nie do końca obiektywnie przedstawia sytuację, jaka panuje w tychże zakładach. Każdy przedsiębiorca chce zadbać o reputację swojej firmy, bardzo często ukrywając, co tak naprawdę się w niej dzieje. Z drugiej strony dyrektorzy, menedżerowie nie zawsze wiedzą, co do ukrycia mają ich podwładni. Na przykład wiadomo mi z anonimowego źródła, że zdarzały się przypadki wykradania zarekwirowanych wcześniej narkotyków przez pracowników służb mundurowych. Proceder ten zdarza się w wielu placówkach w całej Polsce. Ciężko jednak zbadać, jak szeroka jest jego skala. Spytałam również psychologa, który anonimowo za pomocą poczty elektronicznej udzie-

la porad w sprawach narkomanii, czy zgłaszały się do niego o pomoc osoby pracujące zawodowo. Odpowiedział, że zdarzały się takie przypadki, niestety „nie ma systematycznych danych, które odpowiadałyby na pytanie, jaka jest skala zjawiska polegającego na braniu narkotyków w związku z funkcjonowaniem zawodowym.

Są przesłanki wskazujące, że istnieje związek między braniem speedów (np. amfetaminy) w celu zwiększenia efektywności funkcjonowania zawodowego. Mówi się, że zjawisko to dotyczy młodych ambitnych pracowników nastawionych na robienie kariery zawodowej. Amfetamina zwiększa ich wydolność i umożliwia intensywniejszą pracę. Jednak brak danych, które umożliwiłyby oszacowanie rozmiarów tego zjawiska".

Tak więc możemy mieć nadzieję, że badania nad problemem występowania narkotyków w polskich przedsiębiorstwach będą kontynuowane. Warto zbadać jego skalę i w porę reagować, by zapobiec jego poszerzaniu. Moje badanie, choć pilotażowe, może skłoni innych do kontynuowania prac w tej dziedzinie. Co prawda media przestrzegają rodziców, żeby uczulali swoje pociechy na zagrożenia wynikające z zażywania środków odurzających, ale co zrobić w wypadku, gdy to nie dziecko, lecz rodzic je zażywa?

Źródła

Strony internetowe

www.narkotyki.gov.pl.
www.narkotyki.com.pl.
www.narkotyki.esculap.pl.

Anna Konik

Próba charakterystyki działalności agencji detektywistycznych

Niniejsza praca jest jedynie próbą scharakteryzowania działalności detektywistycznej na terenie Polski. Rynek usług detektywistycznych jest bowiem bardzo specyficzny i jakakolwiek próba jego eksploracji jest zadaniem bardzo trudnym. Wynika to z czynników, jakie go ukształtowały. Przede wszystkim jest to poziom rozwoju i ustrój gospodarczy naszego państwa, z drugiej strony uregulowania prawne dotyczące prowadzenia działalności detektywistycznej i zdobywania licencji detektywa. Początkowy brak ustawy i niedoskonałość obecnej Ustawy o usługach detektywistycznych[1] przyczyniły się do wykreowania rynku bardzo hermetycznego i zróżnicowanego. Agencje chcące się na nim utrzymać uległy pewnej specjalizacji, z drugiej strony powstała szara strefa, w której funkcjonują agencje zajmujące się działaniami często zupełnie sprzecznymi z ustawą.

Obecnie nie tylko nagminne staje się obchodzenie przez detektywów przepisów ustawy, ale także jej rażące łamanie. Oczywiście żaden detektyw nie przyzna się jawnie do takich praktyk, stąd niemożliwe staje się rzetelne zapoznanie z działalnością detektywistyczną na rynku krajowym. Nie bez znaczenia dla obecnego stanu rzeczy pozostają uwarunkowania historyczne. Przede wszystkim dlatego, iż detektywi to głównie osoby nie tylko wychowane przez poprzedni system, ale także w dużej mierze pracujące w organach go tworzących. Jeden z detektywów, z którym miałam przyjemność prowadzić rozmowę, podkreślił, iż niemożliwe byłoby, aby ktoś niepracujący np. w policji mógł z powodzeniem świadczyć usługi detektywistyczne. Kolejny detektyw

[1] Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych, Dz.U. z 2002 r., nr 12, poz. 110.

na pytanie o definicje odpowiedział, iż „detektyw jest to policjant na emeryturze". W zestawieniu z faktem, iż dopiero w 2006 r. pierwsze osoby, które nie miały nic wspólnego z ubiegłym systemem, odchodzą w stan spoczynku (po 15 latach służby), wnioski nasuwają się same. Ponadto uwarunkowania gospodarcze mają niebagatelne znaczenie, swoboda działalności gospodarczej przyczyniła się bowiem nie tylko do możliwości otwarcia własnej działalności, ale także do powstania zapotrzebowania na usługi detektywistyczne. Dodatkowym bodźcem stał się wzrost znaczenia informacji głównego towaru, jakim obracają detektywi, stąd tak istotna jest konieczność bardzo precyzyjnego ustalenia dopuszczalnego sposobu ich zdobywania i przetwarzania. Rozwój rynku i sektora prywatnego w gospodarce pociągnął za sobą konieczność powstania odpowiednika wywiadu państwowego działającego dla osób prywatnych, agencje detektywistyczne oraz wywiadownie gospodarcze są odpowiedzią na to zapotrzebowanie.

Trudno obecnie określić, ile takich licencji zostało wydanych ze względu na brak konieczności prowadzenia ewidencji, jednakże w roku 1997 NIK po kontroli podał do informacji następującą tabelę:

Tabela 1. Liczba koncesji wydawana w zakresie ochrony

Lata	Ochrona osób	Ochrona mienia	Usługi detektywistyczne	Ochrona osób i mienia	Ochrona osób i usług detektyw.	Ochrona mienia i usług detektyw.	Ochrona sób mienia i usług detektyw.	Razem
1	2	3	4	5	6	7	8	9
1998–1993	12	2358	118	1020	17	218	1573	5316
1994	4	354	23	248	–	35	135	799
1995	5	330	21	269	–	16	102	743
od 31.05.1996 r.	1	136	5	116	2	7	52	319
Ogółem	22	3178	167	1653	19	276	1862	7177

Wydano zatem około 2324 koncesje dla podmiotów, które mogły świadczyć usługi detektywistyczne, przy czym 639 spośród wszystkich koncesji nie zostało odebranych, natomiast 279 zostało cofniętych lub wygasło. NIK niestety nie podaje, ile z tych koncesji zostało utraconych przez podmioty świadczące usługi detektywistyczne. Przyjmuje się zatem, iż w tym okresie wykorzystywanych było około 1500 koncesji na działalność detektywistyczną.

Chcąc scharakteryzować usługi detektywistyczne, należy najpierw wyjaśnić samo pojęcie „detektywa". Etymologicznie słowo pochodzi od łacińskiego *detectio*, co oznacza odkryć, wyjawić[2], ponadto za detektywa uznaje się osobę, która prowadzi śledztwo metodami niejawnymi. Obecnie obowiązująca ustawa mówi jedynie, iż detektyw to osoba wykonująca swoją działalność na podstawie licencji. Brak legalnej definicji licencji jest zrozumiały, zwłaszcza że ustawodawca określa jej wygląd oraz warunki, jakie musi spełnić detektyw, aby ją uzyskać, natomiast wiadomo, że licencja to zezwolenie na wykonywanie określonej działalności czy podejmowanie określonych działań w ramach wyznaczonych przez ustawodawcę. Oczywiste jest, iż w naszych dywagacjach na temat usług detektywistycznych będziemy opierać się głównie na obecnie obowiązującej ustawie, rozmowach z detektywami i badaniach przeprowadzonych na nich, w tym na raporcie NIK z 1996 r., który w świetle ankiety przeprowadzonej wśród detektywów okazuje się nadal aktualny.

Zacznijmy od samej ustawy. Powstała ona dopiero w 2001 r., czyli prawie 12 lat po powstaniu pierwszych agencji detektywistycznych, do tego czasu działalność ta była jedynie uregulowana przez Ustawę z 23.12.1988 r. o działalności gospodarczej, Dz.U. nr 101, poz. 1178 ze zm. Były to przepisy bardzo ogólne pozostawiające duży zakres uznania administracyjnego Ministerstwu Spraw Wewnętrznych i Administracji, to ono bowiem ustalało kryterium przyznawania licencji na usługi detektywistyczne. Nie dziwi zatem, iż najbardziej odpowiednie do prowadzenia działalności detektywistycznej według ministerstwa były osoby związane z resortem spraw wewnętrznych oraz byli żołnierze. Raport Najwyższej Izby Kontroli z 1996 r. dotyczący nadzoru nad niepań-

[2] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1988, s. 117.

stwowymi formacjami uzbrojonymi ujawnił szereg nieprawidłowości w funkcjonowaniu agencji detektywistycznych – począwszy od stanu zatrudnienia w agencjach, a skończywszy na ich działalności.

Przede wszystkim okazało się, iż agencje zatrudniały osoby nieprzygotowane do wykonywania powierzonych im zadań pod względem psychicznym i posiadanych umiejętności, a także osoby karane uprzednio za przestępstwa umyślne. Ponadto agencje te działały na podstawie indywidualnych regulaminów wewnętrznych. Bardzo często naśladowały swym działaniem i organizacją wyspecjalizowane organy państwowe, na przykład policję, przez używanie środków technicznych umożliwiających wykonanie tajnego nadzoru, śledzenia lub pilnowania kogoś lub czegoś. Dodatkowo przed wejściem w życie obecnie obowiązującej ustawy agencje same ustalały wzór licencji i jednolitego umundurowania, ponownie sięgając do wzorów wykorzystywanych przez organy państwowe. W legitymacji jednej z agencji zawarta była formuła o udzielaniu wszelakiej pomocy jej właścicielowi przy prowadzeniu czynności służbowych[3]. Z drugiej strony wykazano, iż rzetelna ocena stanu zatrudnienia w agencjach była w tamtych czasach niemożliwa. Brak było bowiem odpowiedniej ewidencji tych podmiotów czy prowadzenia statystyk, ponadto wielu detektywów nawet w chwili obecnej prowadzi swoją działalność bez wymaganej koncesji. Nie powinny zatem nikogo dziwić wnioski po kontroli NIK-u, iż konieczne jest wprowadzenie w życie ustawy regulującej dokładnie sposób i kryterium uzyskiwania licencji, a także gwarantującej prawidłowe wykonywanie działalności detektywistycznej oraz możliwość skutecznego prowadzenia nadzoru nad nią ze strony organów administracji państwowej w interesie obywateli i państwa.

Dlatego też przyspieszono prace nad obecnie obowiązującą ustawą, która zakwalifikowała usługi detektywistyczne do tak zwanej działalności regulowanej, co oznacza w praktyce, iż na wykonywanie działalności w zakresie świadczenia usług detektywistycznych wymaga obowiązkowego wpisu do rejestru działalności detektywistycznej prowadzonego

[3] Informacja zawarta w Raporcie Najwyższej Izby Kontroli „o wynikach nadzoru organów administracji państwowej nad niepaństwowymi formacjami uzbrojonymi" z 1997 r. Nr ewid. 29/97/P96028/DON.

przez Ministra Spraw Wewnętrznych i Administracji[4]. Ponadto, aby zostać wpisanym do rejestru, detektyw musi uzyskać licencję. Przy czym wpis do rejestru ma charakter deklaratoryjny i konieczny, ponieważ nabycie uprawnienia do prowadzenia działalności detektywistycznej następuje *ex lege*, po spełnieniu przez przedsiębiorcę warunków określonych w art. 15 ustawy:

„Przedsiębiorca może wykonywać działalność, o której mowa w art. 3, jeżeli: 1) posiada licencję:

a) przedsiębiorca lub ustanowiony przez niego pełnomocnik – w przypadku przedsiębiorcy będącego osobą fizyczną,

b) co najmniej jedna osoba uprawniona do reprezentowania przedsiębiorcy lub pełnomocnik ustanowiony przez przedsiębiorcę do kierowania działalnością detektywistyczną – w przypadku przedsiębiorcy niebędącego osobą fizyczną;

2) nie jest wpisany do rejestru dłużników niewypłacalnych Krajowego Rejestru Sądowego;

3) osoby nieposiadające licencji, wchodzące w skład organu zarządzającego przedsiębiorcy oraz ustanowieni przez ten organ prokurenci oraz przedsiębiorca będący osobą fizyczną nie byli karani za przestępstwa umyślne lub umyślne przestępstwa skarbowe; 4) zawarł umowę ubezpieczenia, o której mowa w art. 24 ust. 1"[5].

Natomiast art. 2 tejże ustawy określa pojęcie usług detektywistycznych i wskazuje przesłanki mające określić daną usługę jako detektywistyczną, jest to przede wszystkim charakter tej czynności, czyli „czynności polegające na uzyskiwaniu, przetwarzaniu i przekazywaniu informacji o osobach, przedmiotach i zdarzeniach"[6], wykonywanie jej na podstawie umowy ze zleceniodawcą, „umowa o świadczenie usług detektywistycznych". Przy czym umowa ta ma charakter cywilnoprawny, jest ukierunkowana na podjęcie określonych działań, a nie konkretny rezultat, oraz realizowana jest w formie i zakresie niezastrzeżonym dla organów i instytucji państwowych na mocy odrębnych przepisów.

[4] Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych, Dz.U. z 2002 r. nr 12, poz. 110.

[5] *Ibidem*.

[6] *Ibidem*.

Są to czynności operacyjno-rozpoznawcze, których przeprowadzenie przez inne osoby w innych okolicznościach jest przestępstwem, natomiast gdy wykonywane jest przez funkcjonariusza publicznego, mamy do czynienia z kontratypem działania w ramach uprawnień i obowiązków. Chociaż określenie to przysparza wielu problemów, ponieważ wymaga znajomości tajnych rozporządzeń czy niejawnych regulaminów wewnętrznych, w których to zawarte są zastrzeżenia odnośnie do formy wykonywania niektórych działań. Zanim jednak rozpocznie się działalność detektywistyczną, należy uzyskać licencję, a w tym celu złożyć egzamin, który jest bardzo trudny i szczegółowy, zwłaszcza w deklaracjach programowych. Obejmuje on problematykę Konstytucyjną RP, przepisy dotyczące Policji, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, a także ochrony danych osobowych, ochrony informacji niejawnych, prawa cywilnego i karnego, kryminalistyki, kryminologii, wiktymologii i psychologii sądowej. Co jednak podkreślają sami egzaminatorzy, dotyczy on za małej liczby uprawnień i obowiązków przyszłych detektywów.

W obecnej chwili dziwić może niedoskonałość ustawy, która dodatkowo była motywowana raportem NIK. Z drugiej strony wiemy, że specyfika usług detektywistycznych i konkurencja istniejąca na rynku tych usług wymuszają postępowanie na granicy prawa. Najprostszym przykładem są płatni informatorzy w postaci funkcjonariuszy policji czy pracowników administracji.

Weźmy jedno z najprostszych zleceń, jakim jest ustalenie adresu dłużnika, można by go śledzić, czego jasno nie zabrania ustawa, ale szybciej, łatwiej, a przede wszystkim taniej jest zapytać „zaprzyjaźnionego" policjanta. Powszechne jest zatem, z czym detektywi się nie kryją, korzystanie z danych dostępnych jedynie policji, czego jasno zabrania ustawa. Jednakże obecny stan rzeczy nie powinien nikogo dziwić. Spójrzmy bowiem na początek lat dziewięćdziesiątych, kiedy to powstały pierwsze agencje detektywistyczne. Ustawa niejasno precyzowała, kto może uzyskać taką koncesję, mówiąc jedynie, iż powinna być to osoba posiadająca odpowiednie kwalifikacje, dlatego też najczęściej byli to dawni funkcjonariusze policji, straży przemysłowych oraz miejskich.

Nie dziwi zatem ich skłonność do sięgania po środki zastrzeżone tylko dla organów państwowych. Czy patrząc z drugiej strony: korzystanie przez organy państwowe z usług prywatnych detektywów. Sejmowa komisja do spraw badania działań tajnych służb ujawniła, że zdarzało się, iż detektywi wbrew zakazowi art. 2 ust. 26[7], który mówi, iż „Zleceniodawcą czynności, o których mowa w ust. 1 pkt. 6, nie mogą być organy prowadzące lub nadzorujące postępowania w tych sprawach". Wykonywali zadania powierzone im przez organy państwowe, np. prowadząc działalność na rzecz MSW. Nie to jest jednak dziwne, bo państwo w celu zachowania wewnętrznego bezpieczeństwa obywateli może korzystać z różnych, mniej lub bardziej oficjalnych środków. Dziwi jednak to, iż przez ustawę zabrania sobie takiej możliwości. Uzasadnienia takiego stanu rzeczy można jedynie szukać w fakcie, iż państwo dysponuje formacjami, które mają znacznie szersze uprawnienia w zakresie przetwarzania i zdobywania informacji, jednakże nie zawsze jest możliwe wykorzystywanie tych źródeł ze względu na konieczność formalizacji zleceń im powierzanych.

Detektywa można bowiem wynająć zupełnie nieoficjalnie, np. wystarczy, aby nie zachował on pisemnej formy umowy ze zleceniodawcą, co jest bardzo często stosowane przez detektywów. Usługa zostaje wykonana bez zawierania odpowiedniej umowy oraz wypisywania faktury po zakończeniu zlecenia. Taki proceder jest nagminnie stosowany przez agencje, ułatwia go fakt, iż bardzo często takie agencje zajmują się jeszcze fizyczną ochroną mienia, te usługi są ewidencjonowane i w dokumentacji stanowią główny dochód agencji. Jak jest w rzeczywistości, wiedzą tylko sami detektywi.

Przyczyny takiego stanu rzeczy są dwie. Po pierwsze, są to zlecenia nielegalne, których wykonywanie wiąże się z naruszeniem prawa i oczywiste jest, że takie usługi nigdy nie będą ewidencjonowane, po drugie, zleceniodawca często nie chce, aby w jakichkolwiek dokumentach było zapisane jego zlecenie. Powody mogą być różne: nie tylko działanie poza prawem, ale także zwykłe unikanie płacenia podatku, w efekcie duża część, o ile nie większość usług jest dokonywana nieoficjalnie, a co

[7] *Ibidem*.

za tym idzie – nielegalnie. Paradoksalnie w ten sposób państwo samo generuje działalność *de facto* przestępczą, do której żaden detektyw w oficjalnej ankiecie się nie przyzna. Dlatego też usługi, do jakich przyznają się detektywi, mieszczą się w katalogu zawartym w ustawie, który jak wiadomo, nie jest zamknięty.

Spójrzmy jednak na zlecenia mieszczące się w katalogu ustawowym. Na tym polu podstawowym atutem agencji detektywistycznych jest przekonanie klientów, iż działają one szybciej i skuteczniej niż ograny państwowe, a także w przypadku osób prawnych – chęć załatwienia sprawy wewnątrz firmy. Żadna firma bowiem nie chce się przyznać, iż jest okradana przez swoich pracowników, a także często nie wierzy, iż policja w toku rutynowego postępowania odnajdzie skradzione mienie. Podobnie ma się sprawa z tak zwaną windykacją długów, zajmuje się nią znaczna część detektywów, w myśl prawa mogą oni jedynie gromadzić informacje odnośnie do dłużnika, wtedy gdy zleceniodawca posiada wyrok z klauzulą wykonalności. Jednakże samą windykacją agencja detektywistyczna nie może się zajmować, dziwić zatem może, że znaczna część detektywów zaznaczyła w przeprowadzonej przeze mnie ankiecie, iż się nią zajmuje.

Ankieta ta została rozesłana do wybranych agencji na terenie całego kraju. Spośród tych, które odpowiedziały, 71% to firmy działające na rynku od 6 do 18 lat. Najczęściej są to firmy o ogólnopolskim zakresie działalności zatrudniające do 7 detektywów. Główną formą ich promocji są kontakty osobiste, książki teleadresowe i Internet. Klienci to w 86% osoby fizyczne. Natomiast spośród osób prawnych 45% to spółki prawa handlowego i instytucje, ale zdarzają się też przedsiębiorstwa państwowe i ubezpieczyciele. Wykazała ona ponadto, iż:

1. Zlecenia najczęściej dotyczą:

- spraw rodzinnych i małżeńskich 57%,
- zobowiązań majątkowych,
- ustalania składników majątkowych,
- wywiadu środowiskowego.

2. Najrzadziej są to zlecenia dotyczące:

- poszukiwań osób zaginionych (50% zajmuje się tym wyjątkowo),

- badania zachowania okresu karencji przez byłych pracowników (57% zajmuje się tymi sprawami wyjątkowo),
- badania szkód zgłaszanych ubezpieczycielom (53% zajmuje się takimi sprawami wyjątkowo).

Brak zależności pomiędzy wynikami wykazany za pomocą testu hi kwadrat potwierdza tezę wskazaną przez NIK w 1997 r., iż usługi detektywistyczne od początku ich powstania uległy znacznej specjalizacji. Z jednej strony bowiem są to agencje funkcjonujące przy granicach kraju zajmujące się głównie poszukiwaniem skradzionych samochodów, z drugiej strony to agencje funkcjonujące wewnątrz kraju, które zajmują się raczej zdolnością płatniczą czy sprawami rodzinnymi. Dla nich poszukiwanie zagubionego mienia wydaje się nieetyczne ze względu na znikomą wykrywalność i koszty, jakie musiałby ponieść potencjalny klient. Istnieje też kilka agencji zajmujących się weryfikacją prawdziwości szkód zgłaszanych ubezpieczycielom. W rozmowach, które przeprowadziłam z detektywami, poinformowano mnie, iż z reguły odmawiają oni przyjmowania takich zleceń ze względu na niekorzystne warunki, jakie proponują zakłady ubezpieczeniowe. Przejawem specjalizacji są także tak zwane wywiadownie gospodarcze, przed 2002 r. zaliczane do usług detektywistycznych, obecnie tylko wtedy gdy dostarczają informacji, których klient nie mógłby znaleźć sam, które nie są ogólnodostępne. Są to firmy zajmujące się zdobywaniem informacji odnośnie do zdolności płatniczych, wykonywania zobowiązań majątkowych i wiarygodności podmiotów w sprawach wynikających ze stosunków gospodarczych[8]. Nie będę jednak poświęcać większej uwagi wywiadowniom gospodarczym ze względu na ich niewielką liczbę w Polsce oraz działalność nie zawsze związaną z usługami detektywistycznymi.

Na zakończenie pragnę zauważyć, iż rynek usług detektywistycznych jeszcze długo pozostanie niezbadany ze względu na swoją specyfikę oraz nieudolne działania organów legislacyjnych, brak należytej kontroli bowiem zawsze powoduje powstanie szarej strefy. Ponadto niejasne są także powiązania zależności pomiędzy samymi firmami świadczącymi usługi detektywistyczne. Niemalże każdy z detektywów ma

[8] G. Gozdór, *Usługi detektywistyczne. Komentarz*, Warszawa 2006.

coś, jak to się zwykło mówić na sumieniu, świadczą o tym chociażby ostatnio wykryte nieprawidłowości w działaniach najsłynniejszych polskich detektywów. Jednakże trudno w obecnej sytuacji szukać winnych – niedoskonałość ustawy stwarza tylko możliwości, które są wykorzystywane przez nieuczciwych pracowników agencji, a których potem nie bardzo ma kto i nie bardzo da się wykryć. Nie dziwi zatem, że państwo zamiast sprzymierzeńca wygenerowało działalność *de facto* przestępczą.