# Wywiad i kontrwywiad gospodarczy

Jerzy Wojciech Wójcik

# Wywiad i kontrwywiad gospodarczy

WSZECHNICA POLSKA
Szkoła Wyższa w Warszawie

Redakcja wydawnicza
Bogumił Paszkiewicz

Projekt graficzny i typograficzny
Krystyna Bukowczyk



**ISBN 978-83-89-077-31-8**

Nakład 100 egz.

**WSZECHNICA POLSKA**
**Szkoła Wyższa w Warszawie**

Pałac Kultury i Nauki
00-901 Warszawa, pl. Defilad 1
Infolinia: 0 801 033 101
rekrutacja@wszechnicapolska.edu.pl

**www.wszechnicapolska.edu.pl**

# Spis treści

# Wprowadzenie

Omawiając problematykę wywiadu gospodarczego należy mieć na uwadze jego interdyscyplinarny, a szczególnie kryminologiczny, kryminalistyczny i prawny charakter. Powszechnie uważa się, że niezbędne jest badanie wiarygodności partnera transakcyjnego, a podstawę wymiany gospodarczej stanowi szeroko pojmowane zagadnienie informacji, która obok kapitału jest jednym z najważniejszych warunków realizacji planowanych celów przedsiębiorstwa. Zatem zasób posiadanych informacji, a szczególnie informacji chronionych, jest zagadnieniem węzłowym zarówno w zawieranych transakcjach, jak i w ochronie tajemnicy przedsiębiorstwa, tym bardziej, że minęły już czasy mylenia wywiadu gospodarczego ze szpiegostwem gospodarczym. Zasadne jest zatem określenie, że wywiad gospodarczy to procedura związana z wymianą informacji pomiędzy przedsiębiorstwem a jego otoczeniem biznesowym, w którym przewiduje się istotne korzyści dla przedsiębiorstwa. Mając na względzie obszerność i złożoność problematyki wywiadu i kontrwywiadu gospodarczego autor dokonał wnikliwej i wyczerpującej analizy skomplikowanych procedur bezpieczeństwa i wymiany informacji.

W dobie współczesnych osiągnięć gospodarczych należy mieć na uwadze aktywnie rozwijającą się przedsiębiorczość na tle prawa konkurencji. Wywiad gospodarczy grupuje szereg istotnych zagadnień z zakresu prawa i finansów, a szczególnie zarządzania, ekonomii, socjologii, psychologii, informatyki, a także etyki biznesu.

Podstawą działania wywiadu gospodarczego jest dokładne i kuteczne rozpoznanie nie tylko otoczenia, lecz przede wszystkim konkurencji. Jest to warunek powodzenia w planowanym rozwoju przedsiębiorstwa lub w jego restrukturyzacji. Znajomość tych zagadnień, na tle dynamicznych zmian społeczno-ekonomicznych, oraz zarządzanie strategiczne powinny gwarantować sukcesy przedsiębiorstwa.

Istotne znaczenie w powstaniu niniejszej pracy wywarło zainteresowanie tematyką wywiadu i kontrwywiadu gospodarczego w ramach zorganizowanej przez Wszechnicę Polską Szkołę Wyższą w Warszawie i Fundację Instytut Wywiadu Gospodarczego w Krakowie ogólnopolskiej konferencji naukowej pn. Wywiad i kontrwywiad w teorii i praktyce biznesu, która odbyła się 25 maja 2017 roku w Warszawie[1].

Wybrane zagadnienia informacji, jej pozyskiwania i wpływu na stan wiedzy, a także jej znaczenie jako produktu strategicznego w zarządzaniu przedsiębiorstwem oraz powszechność manipulowania informacją, a także jej asymetrii, to wstępne zagadnienia zawarte w rozdziale pierwszym. Znaczenie informacji jest przedmiotem obszernej literatury. Uporządkowania pojęć tego terminu podjął się prof. M. Kwieciński. Określa on, że informacja musi spełniać wymogi wysokiej jakości, a w szczególności: selekcji, aktualności, dokładności, pewności, jednoznaczności, operatywności, pełności, a także użyteczności i wiarygodności.

1 http:www.google.pl sprawozdanie z ogólnopolskieej konferencji naukowej wywiad i kontrwywiad w teorii i praktyce biznesu(dostęp10.02.2018)

W rozdziale drugim omówiono zagadnienia dotyczące wybranych tajemnic zawodowych, a szczególnie tajemnicy przedsiębiorstwa, jej ekonomicznego znaczenia, czynów nieuczciwej konkurencji oraz zasad odpowiedzialności karnej za jej stosowanie.

Przedmiotem rozważań w trzecim rozdziale są zagadnienia dotyczące manipulowania informacją na tle rozpoznanych i osądzonych przestępstw gospodarczych, a szczególnie fałszerstw dokumentów tożsamości na tle przestępczości bankowej oraz przestępczego wykorzystania cyberprzestrzeni dla potrzeb biznesowych.

Zagadnienia obejmujące genezę i rozwój wywiadu gospodarczego oraz jego rozpoznawcze znaczenie dla potrzeb transakcji gospodarczych, kierunki jego rozwoju oraz definicję jako zagadnienia ponadnarodowego, omówiono w rozdziale czwartym. Uwzględniono również wybrane rozpoznane zagrożenia i *modus operandi* przestępczości bankowej przy udziale podstępnej działalności „słupów".

Powszechnie wiadomo, że postęp technologiczny jest istotnym bodźcem dla szpiegostwa gospodarczego, jak również handlu informacjami strategicznymi. Niektóre z rozpoznanych tego typu spraw w Europie i na Dalekim Wschodzie przynosi analiza zawarta w rozdziale piątym.

W kolejnych rozdziałach znajdziemy analizę powszechnie stosowanych metod działania w ramach wywiadu gospodarczego, jego rodzaje, techniki i zakres, łącznie z grą operacyjną i dezinformacją.

Praktyczne znaczenie mają zasady opracowywania koncepcji działania jednostki wywiadu gospodarczego oraz ochrony kontrwywiadowczej w przedsiębiorstwie, a także projekty badawcze rynku i klienta biznesowego na tle etyki wywiadowcy gospodarczego; są one przedstawione w rozdziale ósmym.

Podstawowe regulacje prawne dotyczące omawianych zagadnień, a szczególnie ochrony informacji związanych z prowadzeniem dzia-łalności gospodarczej, zawarto w rozdziale dziewiątym. Natomiast rozdział dziesiąty przynosi podsumowanie omawianych zagadnień w zakresie prawnych aspektów ochrony informacji związanych z pro-wadzeniem działalności gospodarczej i bezpieczeństwem biznesu.

W opracowaniu ujęto cytowaną bibliografię dotyczącą: literatury przedmiotu, wykazu aktów prawa krajowego oraz wykazu cytowanych pozycji netografii.

# Rozdział 1

# Informacja a wiedza

## 1. Pojęcie i zakres informacji

Współcześnie obserwujemy systematycznie narastające zapotrzebowanie na informacje, niezbędne dla potrzeb podejmowania decyzji strategicznych w rodzinie, przedsiębiorstwie, państwie.

Mając informację, a przynajmniej łatwy dostęp do niej, zespół wywiadu gospodarczego może prowadzić badania, opracowywać analizy oraz podejmować racjonalne decyzje. Otrzymuje bowiem materiał do przeanalizowania, wnioskowania i zarządzania. W dodat-ku może odpowiednio wcześnie podjąć działania zapobiegające pow--staniu sytuacji kryzysowej.

W dobie ery informacji, wraz z upowszechnieniem się dostępu do informacji oraz zwiększeniem szybkości jej przepływu, informacja nabiera coraz większego znaczenia w codziennym życiu.

Subiektywność informacji niejednokrotnie sprawia, że jej wartość jest różna w zależności od odbiorcy i jego dotychczasowej wiedzy. Powoduje to problem w ocenie zarówno przydatności, jak i wartości analizy uzyskanych informacji.

Informacja, która stanowi etap pośredni w tworzeniu wiedzy, jest niezbędna przy podejmowaniu każdej decyzji. W aktualnym napływie informacji, w sytuacji ich zalewu czy szumu często wyodrębnienie istotnych informacji stanowić może poważny problem. Zatem istotną umiejętnością jest właściwe zebranie i analizowanie informacji istotnych, możliwie jak najdokładniejszych, które będą kluczowe w podejmowaniu decyzji dotyczących określonych przedsięwzięć, zarówno na rzecz wywiadu gospodarczego jak i w ramach działań kontrwywiadu gospodarczego.

Termin informacja najogólniej oznacza właściwość badanych obiektów, relację między elementami zbiorów obiektów, której istotą jest zmniejszanie niepewności (nieokreśloności)[2]. Inne definicje to, przykładowo:

- informacja to wiadomość, nowina[3];
- informacja oznacza element wiedzy przekazywanej za pomocą języka lub innego kodu i stanowi czynnik zmniejszający stopień niewiedzy o jakimś zjawisku, umożliwiający człowiekowi polepszenie znajomości otoczenia i sprawniejsze przeprowadzenie celowego działania[4];

2 http://pl.wikipedia.org/wiki/Informacja(dostęp18.06.2010.
3 W. Kopaliński (red.) *Słownik języka polskiego*, Warszawa 1985, s. 188.
4 B. Dunaj(red.) *Słownik współczesny języka polskiego,* Warszawa 1998, s. 320.

- informacją jest wiadomość lub określona suma wiadomości o sytuacjach, stanach rzeczy, wydarzeniach i osobach. Może być przedstawiona w formie pisemnej, fonicznej, wizualnej i każdej innej możliwej do odbioru przy pomocy zmysłów[5];
- w języku potocznym informacja to *wiadomość, komunikat, wskazówka, pouczenie*[6];
- informacja to: *każdy czynnik, dzięki któremu człowiek lub urządzenia automatyczne mogą przeprowadzić bardziej sprawne, celowe działanie; powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, pouczenie; komórka w urzędzie udzielająca informacji*[7].

Informacja dla współczesnego społeczeństwa ma szczególne znaczenie w wielu aspektach, a zwłaszcza w kontekście obywatelskiego prawa do informacji. Oznacza to, że każdy obywatel ma prawo do rzetelnej, zweryfikowanej, aktualnej informacji, potrzebnej mu do życia i funkcjonowania w społeczeństwie i państwie. Dostęp do informacji ułatwia informatyzacja i cyfryzacja, a przede wszystkim systemy informacyjne, które określa się jako struktury posiadające wiele poziomów. Umożliwiają one użytkownikowi na przetwarzanie, za pomocą procedur i modeli, informacji wejściowych w wyjściowe. Są one najczęściej obsługiwane poprzez system informatyczny, który jest wydzieloną, skomputeryzowaną, częścią systemu informacyjnego[8]. Komputeryzacja systemów informacyjnych odgrywa istotną rolę w sprawności działania systemu zarządzania. Przykładowo, stosując kryterium poziomu zaawansowania technicznego, wyróżniono cztery generacje systemów informatycznych: transakcyjne, informowania kierownictwa, wspomagania decyzji oraz ekspertowe.

System informacyjny pozwala użytkownikowi na transformowanie określonych informacji, czyli wejście na pożądane informacje oraz wyjście za pomocą odpowiednich procedur i modeli. System informacyjny ma kluczowe znaczenie w administracji publicznej, a także w gromadzeniu wiedzy, nauce, biznesie i zarządzaniu wiedzą, gdyż jest to proces technologiczny, który realizuje co najmniej jedną z następujących funkcji:

- generowanie (produkcja) informacji,
- gromadzenie (zbieranie) informacji,
- przechowywanie (pamiętanie, magazynowanie, archiwizacja) informacji,
- przekazywanie (transmisja) informacji,
- przetwarzanie (przekształcanie, transformacja) informacji,
- udostępnianie (upowszechnianie) informacji,
- interpretacja (translacja na język użytkownika) informacji,
- wykorzystanie (użytkowanie ) informacji[9].
- Informacja składa się z danych. Natomiast dane rozumie się jako całość tego, co może być przetwarzane z użyciem umysłu w celu uzyskania informacji[10].

W pewnych sytuacjach przekaźnikiem informacji staje się plotka. Zdarza się bowiem, że niektóre informacje przekazywane są nieoficjalnie, nie zawsze polegają na prawdzie, a niekiedy są kłamliwe czy złośliwe. Plotka jest definiowana w słow-

5 B. Michalski, *Prawo dziennikarza do informacji,* Kraków 1974, s. 9-10.
6 M. Szymczak (red.), *Słownik języka polskiego,* t. 1, Warszawa 1988, s. 788.
7 Leksykon PWN, Warszawa 1972, s. 444.
8 J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Warszawa 2005, s. 18.
9 J. Oleński, *Ekonomika informacji. Metody,* Warszawa 2003, s. 39.
10 S. Galata*, Strategiczne zarządzanie organizacjami. Wiedza, intuicja, strategie, etyka,* Warszawa 2004, s. 59.

nikach językowych jako niesprawdzona lub kłamliwa pogłoska, powodująca utratę dobrego wizerunku osoby, której dotyczy. Powszechnie uważa się, że plotka jest synonimem pogłoski, która jest definiowana jako rozpowszechnianie niepewnych, niesprawdzonych wiadomości. Natomiast w naukach społecznych plotkowanie jest definiowane m. in. jako:

1. negatywne, złośliwe, płytkie obmawianie nieobecnych osób,
2. wymiana oceniających informacji o nieobecnej osobie,
3. proces wymiany informacji o nieobecnych osobach o zabarwieniu oceniającym, pomiędzy bliskimi sobie osobami.

Według Wikipedii plotkowanie od pogłoski odróżnia się treścią. Zazwyczaj plotka dotyczy ludzi, natomiast pogłoska dotyczy raczej zdarzeń i może dotyczyć ludzi. Pogłoska i plotka różnią się również wiarygodnością. Pogłoska zazwyczaj jest prawdziwa, natomiast plotka jest w dużej mierze produktem fantazji wysnutej z wątłych poszlak, zależnej od indywidualnych zainteresowań, dowolnie rozbudowywanych w ogólniejszą pozorną informację. Pomimo swej negatywnej reputacji plotkowanie pełni wiele pożytecznych funkcji, do których zalicza się: funkcję wpływu społecznego, funkcję informacyjną, funkcję podtrzymywania więzi oraz funkcję rozrywkową[11].

Podziały i klasyfikacje informacji, na tle różnych kryteriów warte są przytoczenia. Wydaje się, że podstawowe i najpopularniejsze rodzaje informacji to:

- faktograficzna – odwzorowuje wyróżnione stany obiektów w ramach danej obserwacji (obiekty, ich cechy i ich wartości, relacje oraz czas);
- techniczna – jest to taka informacja faktograficzna, która odnosi się do obiektów technicznych (np. wyrób, surowiec, maszyna), ich cech, takich jak waga, zużycie, kolor, kształt, itp.;
- techniczno-ekonomiczna – jest to taka informacja faktograficzna, której obiektami są obiekty techniczne, ale ich cechami są charakterystyki ekonomiczne, np. cena, koszt wytworzenia, itp.[12];
- ekonomiczno-społeczna – może mieć charakter albo mikro- albo makroekonomiczny. W pierwszym przypadku jej odniesieniem jest mikroekonomiczny obraz przedsiębiorstwa (np. zysk, sprzedaż w danym okresie, zadanie inwestycyjne, oprocentowanie lokat i kredytów, itp.). W drugim przypadku informacja odnosi się np. do gospodarki narodowej (np. stopa inflacji, stopy procentowe banku centralnego, itp.);
- jednostkowa – dotyczy konkretnego faktu techniczno-ekonomicznego (np. konkretnej transakcji, osoby, itp.);

11 http://pl.wikipedia.org/wiki/Plotka(21.04.2015).

12 Wyróżnić można niezwykle ważne dla przedsiębiorstwa rodzaje informacji techniczno-ekonomicznych, a przykładowo:
   a. normy techniczno-ekonomiczne występujące najczęściej w formie wskaźników normatywnych opartych na technologicznych charakterystykach danego wyrobu, czy usługi;
   b. taryfy, np. taryfy kolejowe, stawki celne, stawki płac odnoszące się do konkretnych wyrobów, usług, czy pracowników;
   c. statystyczne wskaźniki techniczno-ekonomiczne, np. wynikowy statystyczny wskaźnik zużycia cementu i kruszywa na wyprodukowanie jednego metra sześciennego betonu, z uwzględnieniem strat w produkcji, transporcie w konkretnym przedsiębiorstwie;
   d. statystyczne dane techniczno-ekonomiczne, czyli statystyczne informacje techniczno-ekonomiczne odnoszące się do podmiotów gospodarczych jako obiektów informacji faktograficznej. Szerzej: J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Warszawa 2006, s. 153.

- zagregowana – opisuje zagregowane zbiory jednorodnych obiektów jednostkowych (np. liczba wytworzonych samochodów w danym czasie) lub ilość takich obiektów mających wspólną cechę (np. liczba sprzedanych samochodów określonej marki). Możliwe jest również opisywanie zjawisk w określonym systemie np. wzrost dobrobytu wyrażony jako zysk na zatrudnionego[13].

Dodając do tej klasyfikacji grunt prawny uzyskamy rodzaje informacji w formie jawnej i chronionej. Ma to istotne znaczenie z punktu widzenia możliwości operacyjnych, czyli uzyskiwania, przekazywania i wykorzystywania informacji.

Można wyróżnić dwa podstawowe punkty widzenia informacji:

1. obiektywny – informacja oznacza pewną właściwość fizyczną lub strukturalną obiektów (układów, systemów), przy czym jest kwestią dyskusyjną czy wszelkich obiektów, czy jedynie systemów samoregulujących się (w tym organizmów żywych),
2. subiektywny – informacja istnieje jedynie względem pewnego podmiotu, najczęściej rozumianego jako umysł, gdyż jedynie umysł jest w stanie nadać elementom rzeczywistości znaczenie (sens) i wykorzystać je do własnych celów [14].

Źródłem najbardziej cennych informacji są wszystkie ośrodki, w których powstają informacje w pierwotnej formie. Informacjami są wszelkie dane o świecie zewnętrznym, które uzyskujemy albo przez bezpośrednie poznanie zmysłowe albo przez odbiór podawanego przez inne osoby opisu jakiegoś stanu rzeczy lub zjawisk[15]. Tak rozumiana informacja ma swoje źródło, do których zalicza się: osoby, rzeczy, miejsca, zjawiska i zdarzenia, następstwa zdarzeń, zwłaszcza ślady, dokumenty, zwłoki, a także czynności operacyjno-rozpoznawcze. Mogą one również być zdobywane poprzez zasadzkę, wypad, poszukiwanie, przechwytywanie i namierzanie źródeł promieniowania elektromagnetycznego.

Praktyczne zasoby informacji dzielą się na trzy grupy, tj.: informację pierwotną, wtórną i retrospektywną, a przykładowo:

Informacja pierwotna powstaje przez wszelkiego rodzaju udokumentowane działania indywidualne lub zbiorowe, badania naukowe, a także przez eksperymenty własne.

Informacja wtórna pochodzi z gromadzenia materiałów ze źródeł wewnętrznych i zewnętrznych. Składają się na nią publikacje specjalistyczne firm, banków, fundacji gospodarczych, ogłoszeń, katalogów, cenników, sprawozdań statystycznych, raportów finansowych, innych dokumentów oraz raportów wywiadowni gospodarczych.

Informacja retrospektywna wywodzi się ze źródeł pierwotnych i wtórnych, które odnoszą się do przeszłości, a znajdują się w archiwach i posiadają w wielu przypadkach wartość użytkową[16].

Zatem przez informację należy rozumieć wszelkie dane zawarte w różnorodnych formach jak np.: tekst, obraz, dźwięk, liczby czy zapach, otrzymywane drogą bezpośrednią czy pośrednią, działają na zmysły odbiorcy, dzięki którym można przeprowadzić bardziej sprawne celowe przedsięwzięcia.

13 Szerzej*:* P. Dziekański*, Informacja jako dobro ekonomiczne będące źródłem przewagi konkurencyjnej* www.ur.edu.pl/file/16795/28.pdf(2.06.2014) oraz W. Flakiewicz*, Systemy informacyjne w zarządzaniu,* Warszawa 2002, s. 28.

14 Szerzej: http://pl.wikipedia.org/wiki/Informacja(18.01.2012).

15 T. Hanusek, *Kryminalistyka. Zarys wykładu*, Kraków 1998, s. 72.

16 A. Wierzbicki, *Informacja jako zasób – wpływ na stosunki społeczne i gospodarcze w krajach rozwiniętych*, "Gospodarka Narodowa" 1996, nr 12, s. 66.

Każda informacja charakteryzuje się swoją rangą i związanym z nią ewentualnym zakresem ochrony i dostępności. Określa się to jako poziom bezpieczeństwa informacji, który związany jest przede wszystkim z zajmowanym stanowiskiem, zakresem obowiązków i poziomem zaufania. Dokument z klauzulą „poufne" może być przeznaczony przez autora jedynie dla określonego gremium, np.: „tylko zarząd" (ang. *CEO only*), „tylko dyrekcja" (*executives only*), „do użytku wewnętrznego" (*company confidential*). Stosowana jest również klauzula „ogólnie dostępne" (*public*).

W konkluzji stwierdzić należy, że informacja jest niezbędnym instrumentem zarówno politycznego, jak i społecznego, a także ekonomicznego i kulturowego działania. W aspektach gospodarczych jest również narzędziem pracy porównywalnym ze środkami produkcji, transportu czy konsumpcji. Bez informacji wszelka działalność, np.: produkcyjna, usługowa, bankowa, naukowo-badawcza - byłaby istotnie ograniczona. Zatem jednym z decydujących czynników o ekonomicznym sukcesie przedsiębiorstwa staje się dostęp do światowych zasobów informacji oraz możliwość i umiejętność ich wykorzystania. Coraz powszechniej podstawowym narzędziem tego dostępu stają się sieci informatyczne. Nie jest to jednak cywilizacja informatyczna, (która tak powinna być określana zdaniem wielu informatyków), lecz jest to cywilizacja informacyjna[17].

Elementami równie istotnymi jak zbieranie informacji jest właściwe zorganizowanie ich obiegu i gromadzenia. Przykładowo, o sukcesie i efektywności działań w walce z przestępczością, jak i na polu walki decyduje, która ze stron będzie dysponowała większą liczbą aktualnych informacji o przeciwniku, metodach, jakimi się posługuje oraz siłach i środkach, jakie może zastosować.

## 2. Dostęp do informacji publicznej

We współczesnych społeczeństwach zorganizowanych w struktury państwowe obywatelskie prawo człowieka do informacji wynika i jest realizowane bezpośrednio z prawa człowieka do prawdy. Obywatelskie prawo do informacji oznacza, że „każdy obywatel ma prawo do rzetelnej, weryfikowalnej aktualnej informacji, potrzebnej mu do życia i funkcjonowania w społeczeństwie i państwie". Wynika z tego fakt, że „Dla każdego społeczeństwa, dla każdego systemu politycznego i ekonomicznego istnieje określony zakres informacji, jaki jest niezbędny obywatelom, aby mogli świadomie w pełny sposób korzystać z innych praw człowieka i praw obywatelskich"[18].

Z powyższej tezy wynika, że w społeczeństwach demokratycznych na państwie ciąży odpowiedzialność za realizację prawa obywatela do informacji oraz budowa infrastruktury informacyjnej rozumianej jako kompleks norm informacyjnych, instytucji, organizacji i systemów informacyjnych, których zadaniem jest m.in.: gromadzenie, przechowywanie i udostępnianie potrzebnej informacji.

Prawo dostępu do informacji publicznej spełnia niezwykle ważną rolę, albowiem:

1. umożliwia współdziałanie obywateli z władzą przy wykonywaniu zadań publicznych,
2. umożliwia współdecydowanie w zakresie celów wydatkowania funduszy publicznych,
3. stwarza możliwość aktywności obywatelskiej,

17 A. Wierzbicki: *Informacja jako zasób: wpływ na stosunki społeczne i gospodarcze w krajach rozwiniętych* „Gospodarka Narodowa" 1996 nr 12.

18 J. Olesiński, *Ekonomika informacji. Metody,* Warszawa 2003, s. 19.

4. stwarza możliwość prowadzenia kontroli obywatelskiej, kontroli działania władzy oraz wykonywania przez nią procedur prawnych.

Realizacja tych zadań w Rzeczypospolitej Polskiej jest zagwarantowana konstytucyjnie. Na podstawie art. 61 ust. 1 Konstytucji RP obywatel ma prawo do uzyskiwania informacji o działalności:

1. organów władzy publicznej oraz osób pełniących funkcje publiczne,
2. organów samorządu gospodarczego i zawodowego,
3. innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

Prawo do uzyskiwania informacji publicznej obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku łub obrazu.

W Konstytucji RP znajdziemy również pierwsze ograniczenia dotyczące udostępniania informacji. Na podstawie art. 61 ust. 3 informacji publicznej nie udostępnia się, ze względu na określone w ustawach:

1. ochronę wolności i praw innych osób i podmiotów gospodarczych,
2. ochronę porządku publicznego i bezpieczeństwa państwowego,
3. ochronę ważnego interesu gospodarczego państwa.

W ostatnich latach dostęp do informacji został bez wątpienia ułatwiony w wyniku osiągnięć technologii informatycznej. A poszukiwanie informacji i uzyskanie jej jest bez porównania łatwiejsze niż kiedyś. Do niedawna odbiorca informacji był niejako skazany na pakiety informacyjne, które zostały dlań przygotowane. Współcześnie – w dobie interaktywności źródeł informacji – sami odbiorcy tworzą dla siebie takie pakiety, złożone z kategorii informacji, których uzyskaniem są zainteresowani. Niezmiernie istotnym zagadnieniem jest również faktyczny dostęp do informacji. Powszechnie wiadomo, że główną zasadą demokracji uczestniczącej jest udział ludzi w procesie podejmowania decyzji, które mają wpływ na ich życie. Ma to również wpływ na przyjmowanie przez społeczeństwo racjonalnej postawy i podejmowanie racjonalnych działań i decyzji zarówno w wymiarze indywidualnym, czy ogólnospołecznym, publicznym, jak np. w formie aktu wyborczego[19].

Jednakże problemem staje się kwestia poszukiwania pożądanej informacji w powszechnym szumie informacyjnym, a także jej racjonalnego wykorzystania i zrozumienia. Pamiętać należy o umiejętności pozwalającej na wyłonienie wartościowego źródła informacji. Zagadnienie to wiąże się z manipulowaniem informacją, stosowaniem dezinformacji i technik socjotechnicznych. Ponadto, informacja nie jest tożsama z wiedzą[20].

Zasadą prawną jest, iż wszystko co dotyczy funkcjonowania państwa i jego organów jest informacją publiczną i powinno być udostępniane. Istnieje jednak wiele przesłanek, w wyraźnie prawem określonych przypadkach, że informacja publiczna nie może być udostępniona ze względu na ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.

19 J. Naisbitt, *Megatrendy,* Warszawa 1997, s. 197.

20 Szerzej: G. Sartori, *Teoria demokracji,* Warszawa 1998, s. 135.

Prawo do informacji publicznej podlega także ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorstwa oraz ze względu na wyłączenie jej jawności z powołaniem się na ochronę danych osobowych, czy prawo do prywatności oraz tajemnice inną niż państwowa, służbowa, skarbowa, statystyczna, czy inna np. o charakterze zawodowym.

Można zatem określić, że powyższe aspekty dotyczą zarówno jawnego, prawnie gwarantowanego dostępu do informacji publicznej, jak i ograniczeń prawnych w tym zakresie. Zatem prawo dostępu do informacji publicznej nie ma charakteru bezwzględnego i podlega licznym ograniczeniom zawartym we właściwych ustawach. Podobne ograniczenia dostępu do informacji zawierają ustawodawstwa innych krajów.

Zagadnienie dostępu i niektórych ograniczeń do informacji publicznej reguluje ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej[21]. Tematyka ta mieści się m.in. w ramach prawa karnego gospodarczego, a ogólnie zagadnienie to jest miernikiem poziomu współczesnej demokracji i społeczeństwa obywatelskiego.

Niezwykle istotne są uwarunkowania w zakresie respektowania ograniczeń w dostępie do informacji, które występują w wielu innych ustawach, a przykładowo:

1. ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (zwana dalej uznk)[22].
2. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[23],
3. ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[24].

### 3. Wpływ informacji na stan wiedzy

Rodzaj i zakres posiadanych informacji istotnie wpływa na stan naszej wiedzy. Wiadomo, że nie jest możliwe uzyskanie doskonałego stanu wiedzy, gdyż nie jest możliwe uzyskanie i poznanie wszystkich informacji. Istotny jest jednak przepływ informacji, które ułatwiają podejmowanie decyzji i czynią bardziej atrakcyjne rynkowo osoby, które posiadają szeroki zakres informacji w określonej dziedzinie. Ponadto, wiedza obejmuje duży zakres doświadczeń i umiejętności.

Warto zatem określić pojęcia dotyczące informacji i wiedzy. Według J. Oleńskiego specyficzne cechy informacji, która może stanowić produkt to przede wszystkim:

- uzależnienie jej trwałości od trwałości nośnika materialnego, na którym została odwzorowana;
- uzależnienie jej odbioru i identyfikacji od rodzaju nośnika. Inaczej traktuje się informację podaną w telewizyjnej migawce, inaczej w pracy naukowej;
- masowość produkcji informacji, czego następstwem jest konieczność jej standaryzacji, polegającej na porządkowaniu właściwych danych;
- łatwość powielenia i upowszechnienia informacji oraz istniejące możliwości jej ochrony;
- niejednokrotnie występujący brak właściwych kryteriów oceny jej jakości jako produktu dla użytkowników.

21 t.j. Dz. U. z 2014 r. poz. 782, 1662.
22 t.j. Dz. U. 2003, Nr 153, poz. 1503 ze zm.
23 t.j. Dz. U. z dnia 3 września 2014 r. poz. 1182.
24 Dz. U. Nr 182, poz. 1228.

- możliwość dokonania właściwego oszacowania użyteczności i weryfikowania jej roli i wagi dla określonego użytkownika,
- możliwy brak odwzorowania rzeczywistości, jako celu tworzenia produktu, który niejednokrotnie dominuje przy wykorzystywaniu w formie produktu przydatnego do sterowania ludźmi oraz organizacjami społecznymi i gospodarczymi[25].

Specjaliści z zakresu organizacji i zarządzania uważają, że wiedzą jest zespół potwierdzonych przekonań i na tym ile odróżniają ją od informacji, będących wiadomościami. Wiedza jest zatem wytworem strumienia informacji, wytworem związanym z oczekiwaniami i przekonaniami odbiorcy. Zatem informacja jest niezbędna dla odkrywania i budowania wiedzy[26].

Na tym tle niezwykle ważnym zagadnieniem jest ekonomika informacji, która w formie ekonomiki szczegółowej jako przedmiot badań wyróżnia metody identyfikacji i pomiaru kosztów informacji w odniesieniu do wyrobów i usług informacyjnych[27]. Zakres podmiotowy tego zagadnienia obejmuje wszelkie klasy podmiotów społecznych i gospodarczych, które uczestniczą w procesach i systemach informacyjnych. konkurencyjnej www.ur.edu.pl/file/16795/28.pdf(2.06.2014) oraz

**4. Informacja a zarządzanie wiedzą**

Powszechnym staje się pogląd, że informacja jest zasobem strategicznym przedsiębiorstwa. Utwierdza w tym „nowa ekonomia", która jest modnym określeniem gospodarki napędzanej informacją i kapitałem, a jednocześnie o słabnącej roli zasobów materialnych. W nowej rzeczywistości konkurencyjność określają nie tyle potencjał ekonomiczny przedsiębiorstwa co jego zdolność do szybkich zmian i skutecznej pogoni za uciekającą wartością dodaną. Szanse w tym wyścigu mają przedsiębiorstwa o następujących cechach:

- elastyczne i szczupłe — zdolne do szybkich inwestycji i dezinwestycji, mało zintegrowane, o małych kosztach stałych, zarządzane przez projekty i struktury macierzowe,
- kooperatywne — poszukujące współdziałania a nie konkurencji, zawiązujące liczne umowy z dostawcami i nabywcami oraz alianse z konkurentami w celu budowy pełnej oferty bez własnych zasobów,
- inteligentne — mające rozbudowane zasoby intelektualne a nie materialne, inwestujące w pracowników oraz badania i rozwój, dysponujące wywiadem ekonomicznym i sprawnie działającym kontrolingiem[28].

W rozważaniach nad zagadnieniem roli informacji w życiu społecznym, warto zwrócić uwagę przede wszystkim na termin, który może być efektem właściwego zarządzania informacją. Kapitał intelektualny – to ważny termin w zarządzaniu. Najczęściej definiowany jest jako różnica między wartością rynkową a wartością księgową przedsiębiorstwa. Kapitał intelektualny to inaczej wytworzone bogactwo, powstałe z wiedzy zatrudnionych pracowników przedsiębiorstwa, zaangażowanych w stały proces przyrostu jego wartości. W literaturze brak jest jednej, powszechnie akceptowa-

25 Szerzej: J. Oleński, *Ekonomika informacji,* Warszawa 2001, s. 284, 285.

26 I. Noaka, H. Takanachi, *Kreowanie wiedzy w organizacji*, Warszawa 2000, s. 80-81.

27 Szerzej: J. Oleński, *Ekonomika informacji* ,wyd. cyt., s. 209.

28 M. Romanowska, *Kształtowanie wartości firmy w oparciu o kapitał intelektualny,* w: R. Borowiecki, M. Romanowska (red.) *System informacji strategicznej,* Warszawa 2001, s. 27.

nej definicji kapitału intelektualnego. Można określić, że jest to kapitał intelektualny, a więc w postaci niematerialnej, który jest różnicą między wartością rynkową a wartością księgową przedsiębiorstwa [29].

Wyróżnia się trzy składniki kapitału intelektualnego w przedsiębiorstwie[30]:

1. Kapitał ludzki (ang. *human capital*) – ma on największy udział w kapitale intelektualnym. Są to m.in. wykształcenie, kompetencje, postawy, umiejętności i doświadczenie pracowników.
2. Kapitał strukturalny (ang. *structural capital*, *organisational capital*) – procesy, systemy informatyczne, marki, patenty, licencje, majątkowe prawa autorskie, znaki towarowe, infrastruktura, strategie oraz kultura organizacyjna.
3. Kapitał relacyjny (ang. *relational capital*, *customer capital*) – relacje z interesariuszami, w tym zwłaszcza z klientami i dostawcami.

Jako podstawowe składniki kapitału intelektualnego w przedsiębiorstwie określa się: dane, informacje, wiedzę i mądrość. Pod pojęciem dane należy rozumieć wszystko co może być przetwarzane z użyciem umysłu w celu uzyskania informacji[31]. Informacja to uporządkowane dane i wszelkie istotne czynniki wykorzystywane do podejmowania decyzji. Informacja powstaje z danych przetworzonych i zinterpretowanych tak, aby mogły być użyteczne dla jej odbiorcy. Istnieje zarówno nadawca jak i odbiorca informacji, który dzięki przekazowi może uzyskać odpowiedzi na pytania: kto?, co?, gdzie?, kiedy? Informacja jest pojmowana jako wszystkie zdarzenia, zarejestrowane, zestawione, pogrupowane, zinterpretowane i uogólnione z punktu widzenia przyjętego celu[32]. Natomiast wiedza jest pojęciem znacznie szerszym w stosunku do danych i informacji. Ma ona nadrzędną pozycję w stosunku do danych jak i informacji, choć na nich bazuje. Dane definiuje się jako niepołączone ze sobą fakty. Poprzez informacje rozumiemy te dane, które zostały poddane kategoryzacji i klasyfikacji lub w inny sposób zostały uporządkowane.

Natomiast wiedza oznacza uporządkowane i „oczyszczone" informacje. Powstaje ona dopiero po wyciągnięciu wniosków z dostępnych danych i informacji. Posiadanie bogatej wiedzy na dany temat prowadzi zaś do mądrości[33]. Mądrość natomiast oznacza użycie wiedzy w praktyce.

Zagadnienie zależności, przedstawione w formie trójkąta, pomiędzy danymi – najniżej, a informacjami, wiedzą i mądrością – wyżej, wykazują istotne zależności. Okazuje się, że wartość składników kapitału intelektualnego w przedsiębiorstwie rośnie, kiedy posuwamy się od podstawy trójkąta do wierzchołka. Dane to podstawa, czyli surowe fakty. Wyżej są informacje, czyli przeanalizowane dane. Można zakładać, że zarówno dane, jak i informacje znajdują się w bazach danych. Samo posiadanie dobrych danych, nawet opracowanych w skomputeryzowanych bazach nie czyni organizacji mądrzejszą, jest jedynie punktem wyjścia do tworzenia wiedzy i umiejętności[34]. Do-

29 http://pl.wikipedia.org/wiki/Kapita%C5%82_intelektualny_przedsi%C4%99biorstwa(28.10.2014)

30 Tamże.

31 A. Adamczyk, *Klasyfikacja informacji i danych prawnie chronionych*, Poznań 2005, s. 153.

32 S. Galata, *Strategiczne zarządzanie organizacjami. Wiedza, intuicja, strategie, etyka,* Warszawa 2004, s. 59.

33 Tamże, s. 154.

34 L. Heracleous, *Better than the Rest: making Europe the Leader in the Next Ware of Innovation and Performance,* Long Range Planning, February 1998. Cyt. za: M. Romanowska, *Kształtowanie wartości firmy w oparciu o kapitał intelektualny*, R. Borowiecki, M. Romanowska (red.), *System informacji strategicznej*, Warszawa 2001, s. 29.

piero człowiek wsparty dobrą informacją kreuje wiedzę i osiąga mądrość, co właśnie przyczynia się do wzrostu konkurencyjności.

Wyniki badań z lat 90. XX wieku przeprowadzonych w ponad 700 firmach amerykańskich wskazywały, że wiedza przydatna do zarządzania firmą znajduje się zarówno w formalnych dokumentach, jak w umysłach pracowników. Źródła wiedzy wykorzystywanej w zarządzaniu firmą to:

1. dokumenty papierowe 26%,
2. dokumenty elektroniczne 20%,
3. komputerowe bazy danych 12%,
4. umysł pracowników 42%.

Niezwykle istotna jest analizowana i badana teza, że wartość kapitału intelektualnego to wartość rynkowa firmy pomniejszona o jej wartość księgową. Natomiast sytuacje, w których firmy o bardzo niskiej wartości księgowej osiągają wielokrotnie wyższą wartość rynkową dowodzą istnienia firm, w których kapitał intelektualny jest głównym źródłem wzrostu ich wartości. Wyniki analiz 500 największych firm amerykańskich w maju 2000 roku wykazały, że wskaźnik ten wynosił średnio w tej grupie sześć, co oznacza, że w każdych sześciu dolarach wartości rynkowej przedsiębiorstwa, tylko jeden dolar reprezentuje wartość zasobów materialnych i finansowych, pozostałe pięć dolarów reprezentują zasoby niewidzialne, nie wycenione w majątku czyli wiedzę[35].

Zarząd przedsiębiorstwa dysponując kapitałem intelektualnym musi podjąć właściwy system zarządzania tymi dobrami. Waga tego problemu jest na tyle istotna, że powinna doprowadzić do zdobycia przewagi przede wszystkim w zakresie innowacji, ale także w dziedzinie reputacji, co w rezultacie doprowadzi do przewagi konkurencyjnej, do jej utrzymania przez długi okres. Niezbędna jest również szybka, nadążająca za zmianami otoczenia umiejętność wykorzystania posiadanych zasobów i umiejętności. Ze względu na strategiczne znaczenie i ulotny charakter kapitału intelektualnego zarządzanie nim jest niezwykle trudne. W związku z tym zasoby informacyjne podobnie jak inne zasoby:

- powinny mieć strategiczne znaczenie,
- muszą mieć charakter zasobów rzadkich,
- nie mogą być możliwe do zastąpienia przez inne zasoby[36].

Ponadto, należy szukać źródeł kapitału intelektualnego wewnątrz organizacji. Jest on bowiem ulotny i ukryty. Na uwagę zasługuje japońskie podejście do zarządzania wiedzą. Zdaniem japońskich menedżerów wiedza wyrażona w słowach i liczbach stanowi tylko wierzchołek góry lodowej, jaką jest istniejąca wiedza przydatna w przedsiębiorstwie. Wysoko ceniona jest wiedza „ukryta", indywidualna i trudna do sformalizowania, a także głęboko zakorzenioną w osobowości pracowników ich kulturze[37].

Odwołując się do polskiej literatury przedmiotu warto podkreślić, że najbardziej doskonałym i złożonym narzędziem zarządzania zasobami informacyjnymi w przedsiębiorstwie jest system wywiadu ekonomicznego. W związku z tym M. Kwieciński definiuje *wywiad gospodarczy jako zespół działań polegających na poszukiwaniu,*

35 Tamże, s. 30.
36 Tamże.
37 I. Nonaka, H. Takeuchi, *Kreowanie wiedzy w organizacji***,** Warszawa 2000, s. 24.

*przetwarzaniu i rozpowszechnianiu informacji przydatnej podmiotom gospodarczym oraz narzędzie permanentnego poznawania rynków, technik i sposobów myślenia konkurentów oraz ich partnerów, ich kultury, intencji i zdolności realizacji zamierzeń*[38]. Niezbędne jest również zwrócenie uwagi na zarządzanie procesami uczenia się w przedsiębiorstwie. Proces ten składa się z trzech faz: nabywania wiedzy, dzielenia się wiedzą i przekształcania wiedzy w decyzje.

Nabywanie wiedzy polega na powiększaniu kapitału intelektualnego bądź poprzez doskonalenie i rozwijanie posiadanych zasobów kadrowych bądź poprzez kupowanie wiedzy na zewnątrz.

Dzielenie się wiedzą polega na upowszechnianiu wiedzy w ramach organizacji lub poza nią, dzięki czemu proces uczenia się obejmuje szerokie kręgi ludzi i przyspiesza proces wdrożenia wiedzy do praktycznych zastosowań. W procesie dzielenia się wiedzą następuje synergia wynikająca z połączenia różnych zakresów wiedzy, doświadczeń zawodowych i sposobów myślenia, dzięki czemu ostateczny efekt procesu uczenia się nie jest prostą sumą wiedzy uczestników tego procesu. Dzielenie się wiedzą może przybierać takie formy, jak:

- praca w ramach projektu specjalistów z różnych podsystemów organizacji i o różnej wiedzy,
- dyskusje i grupowe rozwiązywanie problemów,
- codzienna współpraca zespołów z danej dziedziny np. w formie zespołów innowacyjnych czy laboratoriów,
- alianse z konkurentami i dostawcami, dzięki którym następuje transfer wiedzy z nieznanych nam sektorów, rynków i technologii.

Przekształcanie wiedzy w decyzję to najtrudniejszy i najważniejszy etap procesu uczenia się w organizacji. Wówczas ujawnia się prawdziwa wartość zasobów informacyjnych, rzeczywista wiedza i mądrość pracowników. Na tym etapie weryfikuje się wartość konkurencyjną wiedzy, czyli następuje jej zamiana na wartość. Do najważniejszych czynników decydujących o powodzeniu tych działań należą:

- zaangażowanie w proces decyzyjny najhardziej kompetentnych ludzi;
- wykorzystanie najlepszych kadr w procesie zbierania informacji, formułowania rozwiązań, doboru kryteriów, symulacji skutków każdego z wariantów;
- sprawnie działający i dostosowany do potrzeb określonych decydentów syslem wywiadu gospodarczego lub inny system wspomagający decyzje;
- systemy oceny i wynagradzania menedżerów promujące nowatorskie i śmiałe i rozwiązania, wydłużające okres oceny, w których należy unikać decyzji koniunkturalnych[39].

M. Romanowska zaznacza, że badania, na których się oparła nie dotyczyły jednak przeciętnych przedsiębiorstw, ale największych, najbogatszych, najlepiej zarządzanych przedsiębiorstw amerykańskich. Dla większości przedsiębiorstw na świecie myślenie w kategorii kapitału intelektualnego i permanentnego uczenia się to pieśń przyszłości. Na co dzień pracują w oparciu o szczątkowe informacje, z niedouczonymi ludźmi, koncentrują uwagę nie na wymyślaniu przyszłości czy przywództwa intelektualnego, ale na przeżyciu najbliższego roku i utrzymaniu się na rynku. Autorka zaznacza również, że badania prowadzone nad informacyjną podstawą decyzji

38 M. Kwieciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem,* Warszawa 1999, s. 30, 31.
39 M. Romanowska, *Kształtowanie wartości firmy w oparciu o kapitał intelektualny,* wyd. cyt. s. 33 - 36.

kierowniczych prowadzone w Polsce m.in. przez A. Sopińską[40] i M. Kwiecińskiego[41] potwierdzają niski stan wiedzy w polskich przedsiębiorstwach i nie docenianie wagi tego problemu dla konkurencyjności przedsiębiorstw.

Pomimo tego kontrowersyjne obecnie wydaje się stwierdzenie B. Wawrzyniaka, który kilkanaście lat temu określił stan wiedzy w odniesieniu do polskich przedsiębiorstw jako: „Zarządzanie wiedzą rozumiane zarówno jako sprawdzona strategia jak i codzienna praktyka nie wchodzi na razie w grę. Brak jest bowiem sprawdzonych modeli i procedur, które mogłyby służyć im jako rodzaj przewodnika ... Jest to faza, której określenie «okruchy wiedzy o zarządzaniu wiedzą» jest uzasadnione"[42]. Zatem przed środowiskiem naukowców i doradców z zakresu zarządzania stoi niezwykle ważne zadanie w postaci zaproponowania praktykom rozsądnego systemu tworzenia i wykorzystywania wiedzy w zarządzaniu.

## 5. Informacja jako narzędzie rywalizacji przedsiębiorstw

Rola i znaczenie informacji we współczesnej gospodarce stale wzrasta. Informacja staje się dla wielu przedsiębiorstw poważnym narzędziem rywalizacji. Funkcja, jaką pełni informacja we współczesnym społeczeństwie jest nie do przecenienia. Stała się podstawowym zasobem wiedzy. Ma wpływ na każdy proces i jest niezbędnym składnikiem w podejmowaniu każdej decyzji. Jest istotnym czynnikiem w osiąganiu przewagi konkurencyjnej i motorem wzrostu rozwoju. Powszechnie już uważa się, że nadeszła nowa era – era informacji i zarządzania wiedzą[43].

Podejście metodyczne, umożliwia wypracowanie miar informacji jako zasobu ekonomicznego. Zatem informacyjnym zasobem ekonomicznym są wszelkie użyteczne zbiory informacji, zgromadzone i przechowywane w czasie, w miejscach, w formach, przy wykorzystaniu technologii i organizacji, które umożliwiają dostęp do tych informacji oraz ich wykorzystanie przez finalnych użytkowników działających jako podmioty ekonomiczne, społeczne, a także administracja państwowa i samorządowa[44].

W literaturze przedmiotu spotyka się wiele definicji i klasyfikacji informacji. Warto podjąć próbę omówienia niektórych. Przykładowo, informacje dzieli się na proste i przetworzone. Jakościowo nowa informacja, czyli nieistniejąca dotychczas w przyjętej ostatecznie treści i postaci, jeżeli żądanie (zamówienie) udzielenia informacji dotyczy informacji prostych, lecz wiąże się z potrzebą przeprowadzenia analiz, wyciągów, usuwania danych chronionych prawem, to czyni je informacją przetworzoną[45].

Zwraca się słusznie uwagę na fakt, że szczególne znaczenie ma dostęp do informacji publicznej, której uzyskanie może wymagać szczególnego interesu publicznego. Dotyczy to przykładowo spraw związanych z funkcjonowaniem państwa oraz innych organów publicznych jako prawnej całości zwłaszcza, jeżeli związane jest z gospodarowaniem mieniem komunalnym lub majątkiem Skarbu Państwa. Należy wówczas wykazać, że taka informacja nie tylko jest ważna dla dużego kręgu potencjalnych odbiorców, ale również jej uzyskanie stwarza realną możliwość wykorzystania uzyska-

40 Szerzej: A. Sopińska, *Podstawa informacyjna zarządzania strategicznego przedsiębiorstwem*, Warszawa 2000.
41 Szerzej: M. Kwieciński, *Wywiad gospodarczy*, wyd. cyt.
42 B. Wawrzyniak, *Raport o Zarządzaniu nr 5,* „MBA", nr 1, 2001.
43 J. Oleński, *Ekonomika informacji. Metody,* Warszawa 2003, s. 19.
44 Tamże, s. 21.
45 Patrz wyrok NSA Nr I OSK 1870/10 z 27 stycznia 2011 r.

nych danych dla poprawy funkcjonowania organów administracji[46]czy określonego przedsiębiorstwa. Natomiast inne, nie zawsze zgodne z prawem możliwości wykorzystywania informacji, w zasadzie nie są ograniczone szczególnie wówczas, gdy mogą być w zainteresowaniu wywiadu gospodarczego czy konkurencyjnego, a także szpiegostwa gospodarczego.

W literaturze przedmiotu bardzo szeroko omawiana jest problematyka informacji, jej rola i znaczenie w funkcjonowaniu przedsiębiorstwa, a w szczególności:

- znaczenie informacji we wzbogacaniu wiedzy, prawdziwości i aktualności w podejmowaniu decyzji,[47]
- rodzaje informacji w ramach tajemnic zawodowych[48],
- rola informacji uzyskiwanych ze źródeł zagranicznych[49],
- wykorzystywanie informacji w pracy instytucji finansowych, policji, służb specjalnych i prokuratury[50],
- potrzeby selekcji, oceny, syntetyzowania i interpretowania informacji[51],
- system informacyjny jako element zarządzania strategicznego[52],
- rola informacji w biznesie i administracji[53],
- rola informacji w zarządzaniu przedsiębiorstwem[54]
- rola selekcji informacji w zarządzaniu przedsiębiorstwem[55],
- rola w entropii informacji[56],
- w technologii informacji i komunikacji w samorządach[57],
- rola informacji w controllingu strategicznym[58],

---

46 M. Jaśkowska*, Dostęp do informacji publicznej w świetle orzecznictwa Naczelnego Sądu Administracyjnego,* Toruń 2002, s. 58-62.

47 L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy...* wyd. cyt., s. 125-147.

48 R. i M. Taradejna, *Ochrona informacji w działalności gospodarczej, społecznej i zawodowej oraz życiu prywatnym,* Warszawa 2004, s. 24-234.

49 E. Cilecki, *Penetracja rynków zagranicznych. Wywiad gospodarczy*, Warszawa 1997, s. 41-68.

50 Szerzej: M. Wysocki, *Wykorzystanie otwartych źródeł informacji przez instytucje finansowe* w: W. Filipkowski, W. Mądrzejowski (red.) *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012, s. 72-84.

51 B. Martinet, Y.M. Marti, *Wywiad gospodarczy…* wyd. cyt*.,* 72-98.

52 A. Sopińska, *Rola systemu informacyjnego w procesie zarządzania strategicznego* w: R. Borowiecki, M. Romanowska (red.) *System informacji strategicznej*…, wyd. cyt., s. 86-103.

53 T. Aleksandrowicz*, Informacje w biznesie i administracji* w: R. Borowiecki, M. Romanowska (red.) *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001, s. 231-242.

54 M. Kwieciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa-Kraków 1999.

55 C. Żurak-Owczarek, *Business Intelligence – nowoczesna koncepcja zarządzania informacjami w przedsiębiorstwie* w: J. Kaczmarek, M. Kwieciński (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 233-254.

56 J. Duńczyk, Z. Klimkiewicz, *Cyberterroryzm w aspekcie entropii informacji* w: T. Jemioło, J. Kisielnicki, K. Rajchel, *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009 s. 261-269.

57 A. Masny A. Osika, *Wykorzystanie technologii informacji i komunikacji w samorządach* w: R. Borowiecki, M. Kwieciński (red*.) Informacja w zintegrowanej Europie. Koncepcje i narzędzia wobec wyzwań i zagrożeń*, Warszawa 2006, s.73-80.

58 M. Krwawicz, S. Marciniak, *Rola informacji w budowie bazy planistyczno- normatywnej controllingu strategicznego* w: R. Borowiecki, M. Kwieciński (red.) *Informacja w zintegrowanej Europie*..wyd. cyt., s. 271-292.

- rola informacji w zarządzaniu sytuacją kryzysową[59],
- w szerokiej problematyce bezpieczeństwa informacji[60],
- zarządzanie bezpieczeństwem informacji[61],
- w prawnych, kryminologicznych i kryminalistycznych aspektach wywiadu i kontrwywiadu gospodarczego[62],
- roli informacji w cyberprzestrzeni[63],
- w zagadnieniach prawnej ochrony informacji w cyberprzestrzeni[64],
- Ponadto, należy mieć na uwadze fakt, że informacja jest nie tylko produktem, lecz również atrakcyjnym i poszukiwanym towarem[65].

## 6. Wywiadowcze zapotrzebowanie na informacje

Powszechnie wiadomo, że podglądanie czy szpiegowanie, bez względu na jego rodzaj, jest zajęciem uniwersalnym, istnieje od wielu wieków, a zakres zainteresowania wszelkiego typu wywiadów, jest praktycznie nieograniczony. Zagrożenia są powszechne, lecz nie zawsze doceniane, gdyż stosowane metody wywiadowcze są niezwykle zróżnicowane: od podstępnego działania pracownika firmy aż po wywiad satelitarny, od kradzieży informacji z komputerowej bazy danych aż po podsłuch komputerowy i szpiegostwo komputerowe.

W każdym kraju działają jawne i tajne państwowe służby zajmujące się zbieraniem informacji. Tymczasem wywiadowca gospodarczy – analityk informacji gospodarczej pracuje oficjalnie i nie tylko w zaciszu swego gabinetu. Bywa na konferencjach naukowych, ma szerokie kontakty towarzyskie, aktywnie uczestniczy w pracach swojej firmy i branży. Zgromadzone informacje analizuje, opracowuje wnioski i przedstawia zarządowi. Nie ma natomiast zwyczaju, aby jakaś firma czy organizacja ujawniła, że w ramach jej struktur działa jednostka analityki gospodarczej.

Zapotrzebowanie na informacje narasta na całym świecie. Są poszukiwanym towarem, który niejednokrotnie umożliwia zdobycie fortuny. Brak informacji może doprowadzić do niepowodzeń nie tylko w biznesie. Specjaliści zajmujący się gromadzeniem i analizowaniem informacji tworzą niezwykle ważną dziedzinę rynkową, która w gospodarce wolnorynkowej polega na obrocie informacjami.

Informacje, a szczególnie informacje o charakterze gospodarczym, finansowym czy handlowym, są traktowane obecnie jako jeden z najbardziej atrakcyjnych towa-

59 Przykładowo: J.W. Wójcik, *Zarządzanie sytuacją kryzysową na przykładzie napadu rabunkowego na bank* w: R. Borowiecki, M. Kwieciński (red.) *Informacja w zintegrowanej Europie*..wyd. cyt., s. 158-178.

60 Przykładowo: K. Owczarek, C. Żurak-Owczarek, *Bezpieczeństwo informacji w handlu elektronicznym* w: R. Borowiecki, M. Kwieciński (red.) *Informacja w zintegrowanej Europie*, wyd. cyt. s. 116-133.

61 T. Wawak (red.) *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Bielsko Biała 2007.

62 J.W. Wójcik, *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego* w: R. Borowiecki, M. Romanowska (red.) *System informacji strategicznej*…, wyd. cyt., s. 326-355.

63 J.W. Wójcik, *Z problematyki ochrony informacji nie tylko w sytuacjach kryzysowych*, w: R. Częścik i inni (red.) *Zarządzanie kryzysowe w administracji*, Warszawa-Dęblin 2014, s. 400-434.

64 J.W. Wójcik, *Wywiad gospodarczy a prawna ochrona informacji*, Warszawa 2000, s. 43-84, tego autora *Cyberprzestępczość a prawo*, "Problemy Prawa i Administracji", Nr 1/2011.

65 J.W. Wójcik, *Ochrona informacji a wywiad gospodarczy. Zagadnienia kryminalistyczne, kryminologiczne i prawne*. Warszawa 2016.

rów, a stanowiące tajemnice przedsiębiorstwa, są produktem wymagającym szczególnej troski i profesjonalnej ochrony. Każda duża organizacja czy mała firma, która chce liczyć się na rynku i starannie zabiega o renomę, podejmuje wiele działań by pozyskiwać dobrych klientów. Klienci natomiast chcą mieć zaufanie do firmy i odczuwać, że jest ona nie tylko przyjazna i kompetentna, lecz przede wszystkim bezpieczna.

Wprowadzenie gospodarki rynkowej skutkuje różnorodnymi nowymi wartościami i jakością przede wszystkim w aspektach ekonomicznych, organizacyjnych, administracyjnych i prawnych, które stwarzają nie tylko konieczność nowych uregulowań prawnych, niekiedy tworzenia nowych lub zmiany zakresu dotychczasowych pojęć. Dotyczy to również nowego spojrzenia na zagadnienie tajemnicy handlowej, przemysłowej, zawodowej, bankowej, ubezpieczeniowej i innych – w świetle aktualnych zagrożeń.

Od dawna wiadomo, że sukcesy wywiadowców gospodarczych (analityków informacji) umożliwiają podejmowanie najbardziej trafnych decyzji dla przedsiębiorstwa. Prognostycznie rzecz biorąc, przewiduje się hasło: każdy pracownik jest wywiadowcą na rzecz swojej firmy i tego typu zadania będą zapisane w zakresie obowiązków, po odpowiednim przygotowaniu personelu[66].

Współczesnym motorem zachodzących zmian – cywilizacji przemysłowej i informacyjnej – jest fakt, że informacja zaczyna odgrywać rolę podstawowego zasobu produkcyjnego, a nawet decydującego czynnika produkcji - obok kapitału, pracy i surowców. Decydujący dla ekonomicznego sukcesu przedsiębiorstwa staje się więc dostęp do światowych zasobów informacji i umiejętność ich wykorzystania. Nie spotkamy natomiast wykazu organizacji czy instytucji zainteresowanych zbieraniem informacji. Pamiętać jednak należy o zasadzie wyznawanej przez wielu przedsiębiorców: *Podglądaj jak to robią inni*.

Z punktu widzenia organizacji i zarządzania jest to zresztą podstawowa zasada przetrwania. Zatem ochrona tajemnic każdej instytucji czy firmy nie powinna budzić najmniejszych wątpliwości. Kwestią są odpowiednie uregulowania prawne oraz przestrzeganie określonych zasad zachowania cennych informacji.

Współczesna sytuacja gospodarcza w wielu przedsiębiorstwach może być związana z zasadą przetrwania. Żaden prezes czy przedsiębiorca nie przyzna wprost, że w jego firmie działa komórka analizująca informacje gospodarcze, a jej konstruktywne wnioski niejednokrotnie są niezbędne.

Cywilizacja informacyjna związana jest również z cywilizacją przemysłową, która wymaga nowych jakości. Informacja zyskuje nowe atrybuty, do których można zaliczyć:

- przydatność informacji, czyli jej dostosowanie do potrzeb użytkownika;
- aktualność informacji, czyli jej dostosowanie do czasu użytkowania;
- odpowiedzialność informacji, czyli gwarancje jej poprawności;
- typ własności informacji, czyli określenie praw dostępu do niej:
- typ ochrony informacji, czyli sposoby utrudniające dostęp oraz modyfikację informacji przez osoby niepowołane[67].

66 B. Martinet, Y.M. Marti, *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji,* Warszawa 1999, s. 325. Francuskie wydanie tej pracy to: *L'intelligence economique – Les yeux et les oreilles de l'entreprise*, Paris 1995.

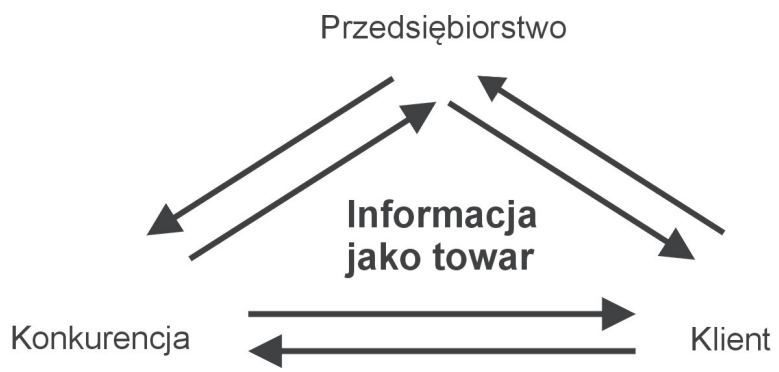
67 Por. A. Wierzbicki, *Informacje jako zasób: wpływ na stosunki społeczne i gospodarcze w krajach rozwiniętych*, "Gospodarka Narodowa' 1996, nr 12, s. 76.

W konkluzji stwierdzić należy, że **informacja jest niezbędnym instrumentem zarówno obywatelskiego i publicznego, a także politycznego, jak i społecznego oraz ekonomicznego i kulturowego działania. W aspektach gospodarczych jest również narzędziem pracy porównywalnym ze środkami produkcji, transportu czy konsumpcji.** Bez informacji wszelka działalność, np.: produkcyjna, usługowa, bankowa, ubezpieczeniowa, naukowo-badawcza - byłaby istotnie ograniczona. Zatem jednym z decydujących czynników o ekonomicznym sukcesie przedsiębiorstwa staje się dostęp do światowych zasobów informacji oraz możliwość i umiejętność ich wykorzystania Coraz powszechniej podstawowym narzędziem tego dostępu stają się sieci informatyczne. Nie jest to jednak cywilizacja informatyczna, (która tak powinna być określana zdaniem wielu informatyków), lecz jest to cywilizacja informacyjna[68].

## 7. Informacja jako produkt strategiczny

Mając na względzie sprawne funkcjonowanie każdego przedsiębiorstwa (również małej firmy), musimy mieć na uwadze specyficzną triadę strategiczną: przedsiębiorstwo – klient – konkurent. Wspomniana triada i zachodzące w niej interakcje pomiędzy poszczególnymi podmiotami nabierają coraz większego znaczenia, szczególnie zaś w okresie transformacji zmierzającej do usprawniania zasad ekonomicznych w ramach gospodarki rynkowej. Pamiętać należy, iż zasadniczym czynnikiem łączącym, a także nasycającym rywalizację pomiędzy tymi podmiotami jest informacja jako produkt będący poszukiwanym towarem.

**Wykres 1. Podmioty zainteresowane wymianą informacji w biznesie.**




Źródło: J.W. Wójcik, *Wywiad gospodarczy, a prawna ochrona informacji*, Warszawa 2000, s. 6.

Jeżeli informacja jest towarem, jest zatem zasobem przedsiębiorstwa. Zainteresowanie zasobami ma miejsce przynajmniej w kilku aspektach, a szczególnie: ekonomicznych, logistycznych, psychologicznych, konkurencyjnych, prawnych, kryminologicznych i kryminalistycznych. Dobrze zagospodarowane i chronione zasoby przydatne są do wymiany biznesowej, a przede wszystkim przynoszą istotne korzyści dla przedsiębiorstwa.

Wszystkie trzy podmioty, przedstawione w rys. 1, nawzajem na siebie oddziaływają. Jednakże podstawowym czynnikiem napędzającym jest konkurencja, czyli wyprze-

68 Tamże.

dzenie innych i osiągnięcie lepszych wyników. Natomiast istotnym celem działania tych podmiotów jest przede wszystkim:

1. wymiana, zdobywanie czy uzupełnianie informacji niezbędnej dla modernizowania dotychczasowej strategii funkcjonowania przedsiębiorstwa,
2. badania konkurencyjnego przedsiębiorstwa,
3. zakupu dobrego towaru, a także w konkurencyjnej cenie.

Przykładowo, pomiędzy firmą a konkurencją istnieje swoista rywalizacja o klienta, czyli działanie w ramach uczciwej konkurencji. Można zatem przyjąć, że wszystkie 3 podmioty realizują lub intensyfikują swoje działania zgodnie z zasadami dobrej konkurencji. Jednakże zdarzyć się może podstępna gra, w której daleko do zasad moralnych i uczciwej konkurencji. Prostym przykładem w tej mierze może być niska cena gry komputerowej, ale jej uzupełnienia kosztują setki złotych. Natomiast klienci oceniają firmę na podstawie informacji co do cen, na podstawie informacji o prestiżu przedsiębiorstwa. Dochodzi jednak do rozczarowania, gdyż niektóre działania nie zawsze są zgodne z etyką biznesu i obowiązującym stanem prawnym. Ponadto, efekty działania biznesowego pomiędzy przedsiębiorstwami określonej branży zależą od profesjonalnej konkurencji.

Mając świadomość, że podstawą wszelkiego rozpoznania jest informacja, należy uwzględniać zasadę, że podstawą funkcjonowania nowoczesnego przedsiębiorstwa jest posiadanie sprawnego systemu polegającego na pozyskiwaniu informacji, gromadzeniu ich oraz przetwarzaniu czyli analizowaniu skutkującym jednocześnie rozpoznaniem, a także na umiejętnym przetwarzaniu, tj. opracowywaniu komunikatywnych raportów. Taki właśnie system informacyjny powinien cechować się wysoką „inteligencją" w wykorzystaniu, czyli prezentacji zebranych i przetworzonych informacji, który skutkuje opracowywaniem właściwych komunikatów kierowanych do odpowiednich stanowisk zarządzania[69].

Informacja na całym świecie jest poszukiwanym towarem. Uzyskana w porę pozwala zbić fortunę. Jej brak, np. o nieuczciwości partnera gospodarczego, może spowodować stratę lub nawet bankructwo. W Polsce, od wprowadzenia wolnego rynku zaczęto informację należycie doceniać. Działają już firmy, które zajmują się zawodowo uzyskiwaniem, gromadzeniem i sprzedawaniem informacji. Są to m.in. wywiadownie gospodarcze, agencje detektywistyczne, firmy headhunterskie, czyli tzw. łowcy głów. Jednakże gromadzeniem i analizowaniem informacji zajmują się wszyscy, tj. zarówno instytucje państwowe, spółki, jak i osoby fizyczne. Zajmują się również przestępcy i terroryści. Przykładem może być Internet, który jest też wykorzystywany przez terrorystów do dezinformacji i celów propagandowych, w tym wzniecania niepokojów, szerzenia nienawiści, a ogólnie do prowadzenia wojny psychologicznej. Znane są powszechnie groźby, a nawet pokazywane akty egzekucji dziennikarzy i innych osób, w tym członków akcji humanitarnych.

Rangę informacji jako produktu podkreśla J. Konieczny i inni autorzy, którzy określają specyficzne cechy, a które warto przytoczyć. Są to mianowicie:

- uzależnienie jej trwałości od trwałości nośnika materialnego, na którym została odwzorowana. Jej trwałość może zależeć od trwałości nośnika;

69 J. Walkowiak, *Misja firmy a etyka biznesu*, Warszawa 1998, s. 31.

- uzależnienie jej odbioru i identyfikacji od rodzaju nośnika. Różnorodność odbioru zależy od rodzaju i nadawcy informacji;
- masowość produkcji informacji, czego następstwem jest jej standaryzacja, polegająca na typowości porządkowania danych i typowości ich treści;
- łatwość powielenia i upowszechnienia informacji, która zależy od formy jej reprodukcji mającej istotny wpływ na wysokość ceny jej ochrony;
- brak trafnych, ogólnych kryteriów oceny jakość i informacji jako produktu, co jest utrudnieniem dla jej użytkowników;
- możliwość dokonania oszacowania użyteczności informacji dopiero po jej otrzymaniu, czyli dopiero wówczas można dokonać oceny jej przydatności;
- zanik odwzorowania rzeczywistości, jako celu tworzenia informacji – produktu. Dominuje bowiem wykorzystanie informacji do sterowania ludźmi, organizacjami społecznymi i gospodarczymi[70].

## 8. Powszechność manipulowania i asymetrii informacją

Termin manipulacja pochodzi od łacińskiego *manus pellere* co oznacza trzymać dłoń w czyjejś dłoni, mieć kogoś w ręce. Manipulacja, jako termin psychologiczny i socjologiczny, polega na celowym i świadomym kształtowaniu poglądów, postaw, zachowań lub emocji bez wiedzy i woli człowieka. Natomiast w politologii to metoda zakamuflowanego oddziaływania na świadomość i zachowania zarówno jednostek, jak i grup społecznych dla realizacji określonych przez nadawcę celów politycznych. Manipulator umiejętnie posługuje się np. danymi statystycznymi, informacjami, faktami, aby ukryć przed odbiorcą rzeczywiste cele.

Niezbędne jest zwrócenie uwagi na specyficzną grę, w której dochodzi do powszechnie znanych technik manipulacji jak: moralizatorstwo, prowokacja, ośmieszanie rozmówców, przekazywanie fałszywych bądź zniekształconych informacji, fragmentaryzowanie (typowe jest tu punktowe ukazywanie jakiegoś problemu, zwiększając lub zmniejszając jego znaczenie), upowszechnianie stereotypów (narodowych, rasowych). W kategoriach etycznych manipulacja oceniana jest zdecydowanie negatywnie, wiąże się bowiem z nierespektowaniem norm moralnych, oszukiwaniem i kłamstwem.

Manipulacja, zapewne towarzyszyła człowiekowi od samego początku. Paradoksalnie, sam akt komunikacji czyli wymiany informacji, nosi znamiona przypominające manipulację. Podstawowym kryterium manipulacji jest celowość i skrytość działania. Jest to również zespół świadomych lub nieświadomych działań podejmowanych w celu wywarcia na określoną osobę (lub grupę) wpływu skłaniającego do zachowań odpowiadających planom sprawcy manipulacji. Natomiast istotą omawianego zjawiska jest ukrycie rzeczywistych zamierzeń, ich konsekwencji, a nade wszystko samego faktu wywierania wpływu[71]. Może zatem doprowadzić do negatywnych skutków prawnych.

Manipulowanie informacją może mieć miejsce w każdym środowisku, a przykładowo: w polityce, w reklamie, w miłości. Może być manipulowanie umysłem, pranie mózgu, wywieranie wpływu na drugą osobę za pomocą słów, mimiki, gestów, dzia-

70 Szerzej: J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, Warszawa 2004, s. 145, J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 284, 285.

71 http://library.republika.pl/manipulacja.html(28.01.2015)

łania na emocjach, uczuciach, instynktach, a także dezinformacja. Celem manipulacji jest uzyskanie określonego efektu, a także korzyści manipulatora.

Środowisko informacyjne, w którym istnieje i działa współczesny człowiek charakteryzuje się, m.in. takimi cechami jak wypaczanie wartości informacji, granie informacją na uczuciach, fałszowanie informacji, uzależnianie od informacji, wykorzystywanie czyjeś podatności na działanie informacji. Stanowi to obszar bardzo podatny na manipulowanie, a co za tym idzie przejrzystość informacji staje się coraz bardziej utopią. Manipulowanie informacją jest zjawiskiem powszechnym, jest to środek, za pomocą którego steruje się ludźmi, ich zachowaniami i upodobaniami a nawet podmiotami gospodarczymi i społecznymi[72].

Szczególnym typem manipulacji w biznesie jest *insider trading* (lub *insider dealing*). Ten rodzaj manipulacji informacją polega na wywieraniu wpływu na transakcje papierami wartościowymi notowanymi na rynku giełdowym określonej spółki. Manipulacji dokonują osoby mające dostęp do informacji niejawnych dotyczących tej spółki i wykorzystujących te informacje do osiągnięcia prywatnego zysku[73].

Takie działanie to tzw. przestępstwo wtajemniczenia czyli handel przez osoby wtajemniczone, inaczej „obrót poufny" (*insider trading*) - polega na podawaniu do publicznej wiadomości informacji fałszywych o danej spółce mającej notowania na giełdzie. Informacje te mogą być zarówno pozytywne, jak i negatywne. Wprawdzie współczesna technika pozwala na szybkie weryfikacje informacji o znaczeniu handlowym, to w tym przypadku chodzi o udostępnienie informacji wąskiej grupie osób, która potrafi wykorzystać je pomimo, że stanowią one tajemnicę zawodową. Karalne jest bowiem nie tylko ujawnienie wiadomości stanowiących tajemnicę prawnie chronioną, lecz także obrót akcjami przez osoby, które są uprzywilejowane do uzyskiwania informacji poufnych w sposób legalny. Niektórzy maklerzy w porozumieniu z inwestorem kupują duże pakiety akcji spółek, co do których posiadają informacje, że ich notowania wkrótce wzrosną. To najpopularniejsze, na wszystkich giełdach świata przestępstwo, sprawia duże trudności wykrywcze, gdyż metody działania są wyrafinowane[74], a sprawcy posiadają możliwości dysponowania wielkim kapitałem. Dla przeprowadzenia dużych operacji giełdowych, o charakterze przestępczym, tworzone są specjalne spółki i firmy fikcyjne, najczęściej rejestrowane w oazach podatkowych. Przepływ kapitałów przez wiele krajów i banków, ułatwia ściąganie kapitałów, a utrudnia badanie dokumentacji i ujawnienie przestępnych powiazań i udowodnienie winy[75].

W tej kwestii można podać wiele przykładów. Wiele z nich nie udaje się wyjaśnić. Upłynęło już ponad 10 lat od głośnego tzw. Polskiego akcentu – „100 sekund". Wciąż jeszcze służby dążą do wyjaśnienia zdarzenia, które miało miejsce w dniu 4 lutego 2004 roku. Tego dnia makler Bankowego Domu Maklerskiego PKO BP złożył dwa duże zlecenia na kontrakty terminowe. Spowodowało to niespodzianie gwałtowne zmiany notowań. Wszystko to przewidział tajemniczy inwestor z brytyjskich Wysp Dziewiczych. Wystarczyło mu bowiem tylko 100 sekund, by kosztem BDM PKO BP i kilkuset nieświadomych inwestorów warszawskiej giełdy, tajemniczy inwestor zarobił blisko 2,6 mln zł. Jakie miał informacje i jak je uzyskał pozostaje wciąż tajemnicą.

72 W. Babik**,** *O manipulowaniu informacją w prywatnej i publicznej przestrzeni informacyjnej* http://www.ktime.up.krakow.pl/symp2011/referaty2011/babik. pdf(28.01.2015)

73 http://pl.wikipedia.org/wiki/Insider_trading (28.01.2015)

74 Szerzej: J.W. Wójcik, *Oszustwa finansowe*, wyd. cyt., s. 78-96.

75 J.W. Wójcik, *Przestępstwa w biznesie*, Warszawa 1998, s.162

Według Komisji Papierów Wartościowych i Giełd w wyniku zamieszania na rynku kontraktów tego dnia stratę w wysokości 5,44 mln zł poniosło 307 inwestorów. Łączny zysk w identycznej wysokości zanotowało 777 inwestorów. Jednakże największy zysk, tj. 2,56 mln zł osiągnęła spółka z siedzibą na Brytyjskich Wyspach Dziewiczych. Tego dnia o godz. 15:16:38 gigantyczne zlecenie sprzedaży doprowadziło do nagłego spadku o 6,6 proc. ceny kontraktu terminowego FW20F4. Zaledwie 17 sekund później sytuacja odwróciła się o 180 stopni – kurs kontraktu wzrósł o 9,9 proc. Do załamania kursu kontraktu przyczyniło się zlecenie sprzedaży 4 tysięcy kontraktów terminowych złożone za pośrednictwem Bankowego Domu Maklerskiego PKO BP. O godz. 15.15 pracownik tego biura nie posiadający licencji maklerskiej otrzymał od jednej z klientek zlecenie zakupu 4 kontraktów terminowych po każdej cenie (PKC). Następnie pracownik ten, korzystając z kodu dostępu do systemu giełdowego Warset, należącego do zatrudnionego w tym samym biurze licencjonowanego maklera, wprowadził do systemu zlecenie kupna 4 tysięcy kontraktów FW20H4[76].

W klasycznych formach *modus operandi* sprawców oszustw giełdowych można wymienić różnorodne manipulacje informacjami, a także: przecieki poufnych informacji, rozpowszechnianie chronionych prawem informacji z zakresu tajemnic zawodowych, puszczanie w obieg mylących informacji lub zatajanie informacji o spółce i jej działalności, które mogą mieć dla inwestorów istotne znaczenie, np. uzyskanie specjalnej koncesji, zwolnienie z podatku dochodowego, straty, zawieszenie działalności itp.

Sprawa manipulowania informacjami poufnymi o spółkach giełdowych była przedmiotem badań socjologicznych. Okazuje się, że badani nie widzieli w tym większej szkodliwości społecznej. W sierpniu 1986 r. tygodnik Business Week przeprowadził badania anonimowe. Ponad połowa ankietowanych, tj. 53 proc. odpowiedziało, że skorzystaliby z poufnych informacji. Natomiast 82 proc. było zdania, że większość ludzi tak samo skorzystałoby z takiej informacji[77].

W literaturze przedmiotu słusznie zwraca się uwagę na asymetrię informacji. Oznacza to, że współczesne środowiska ekonomiczne to nieustanna walka o jakość, skuteczność czy nawet doskonałość w procesie podejmowania decyzji, na tle zasobów wartościowych informacji, które należy traktować w kategoriach zasobów strategicznych. Mają one istotny wpływ na poziom wiedzy w organizacji. Pozwala to nie tylko na przetrwanie i rozwój w stabilnym otoczeniu zewnętrznym, ale i przede wszystkim w stanie zagrożenia, do którego zalicza się również i kryzys. Jednakże powszechność asymetryzacji sprawia, że nie zawsze stan wiedzy zarządzających jest faktycznym odzwierciedleniem otaczającej nas rzeczywistości. Procesowi temu towarzyszy wręcz eksplozja informacyjna, która stanowi broń obosieczną, co oznacza, że może zaatakować zarówno konkurencję, jak i naszą organizację.

Szybkość przepływu informacji powoduje, że menedżerowie są zdolni do pozyskiwania informacji pochodzących z różnych źródeł. Występują tu jednak pewne ograniczenia spowodowane dostępem, który dzieli się na: ogólnie dostępne, częściowo dostępne i niedostępne. Wydaje się, że istotną wartość praktyczną dla każdego zainteresowanego pracownika organizacji posiadają jednak określone informacje niedostępne. Podkreśla to J. Oleński, a mianowicie: *Przyjmując, że informacją pragmatyczną jest tylko ta informacja, która jednocześnie odwzorowuje rzeczywistość (relacje: infor-*

76 *Zarobił inwestor z Wysp Dziewiczych*, „Rzeczpospolita" z 11 lutego 2004 r.

77 J.W. Wójcik, *Przestępstwa w biznesie* , wyd. cyt., s. 163.

*macja – obiekt rzeczywisty), zabezpiecza potrzeby użytkownika (relacje: informacja – wiedza) i umożliwia podejmowanie efektywnych działań*[78].

W literaturze światowej głośno o zalewie i szumie informacyjnym. Jednakże z informacji napływających codziennie do przedsiębiorstwa wyróżnić można trzy rodzaje:

- informacja „surowa" jako liczby lub fakty podawane bez kontekstu, istniejące w swoistej próżni; niepoddane analizie dane, z których można opracować informacje;
- informacja, jako liczby lub fakty podane w pewnym kontekście; przeanalizowane dane, zawierające pewne wiadomości;
- informacja wywiadowcza, jako przeanalizowana informacja sugerująca podjęcie działania, strategii, decyzji (wiedza)[79].

Napływające do odbiorcy wiadomości to informacje ogólnodostępne, dochodzą do przedsiębiorstwa lub są przez nie odbierane z najróżniejszych źródeł. Mają postać pewnych, kompletnych i jasnych faktów (np. statystyki rynkowe, sprawozdania finansowe, wycinki gazetowe). Dostarczycielem takich informacji może być praktycznie każdy, a w szczególności: media, biblioteki czy centra informacyjne. Wiadomości te przede wszystkim dostarczają informacji o aktualnym lub przeszłym stanie rzeczy.

Współczesne wyzwania to szanse i zagrożenia, które wymagają dostępu do szerokiego spektrum informacji, który pozwala aktywnie reagować na zachodzące zmiany, na które powinni być przygotowani przede wszystkim zarządzający organizacjami gospodarczymi. Zgromadzone wiadomości spełniają trzy podstawowe funkcje:

1. informacyjną, jako odwzorowanie rzeczywistości w formie informacji i tworzenie zasobów wiedzy;
2. decyzyjną, która zabezpiecza sytuację decyzyjną użytkownika informacji – decydenta;
3. sterowania, która po przekazana odbiorcy wywołuje określone skutki[80].

Przy kompleksowym podejściu do informacji, które jest istotne z punktu widzenia zarządzania informacjami, w organizacji gospodarczej wyróżnia się trzy podstawowe strumienie, i tak:

- pierwszy strumień, dotyczy informacji wytwarzanych przez organizacje gospodarcze dla własnych potrzeb,
- drugi strumień, obejmuje informacje wytwarzane przez otoczenie i wykorzystywane przez organizacje gospodarcze,
- trzeci strumień, to informacje wytwarzane przez organizacje gospodarcze z przeznaczeniem dla otoczenia zewnętrznego.

Prowadzona aktualnie walka informacyjna ma miejsce w każdej przestrzeni (w tym gospodarczej) ma ścisły związek ze współczesnymi przeobrażeniami cywilizacyjnymi. Zatem w procesie budowania systemu informacyjnego, należy mieć na uwadze to, że informacje te mogą być wiarygodne, prawdopodobne, wątpliwe i dezinformujące, i tak:

- wiarygodne – to informacje, które pochodzą z kilku źródeł (lub jednego, ale pewnego), stanowią odzwierciedlenie istniejącej sytuacji, jaka ma miejsce w otoczeniu zewnętrznym organizacji,

78 J. Oleński, *Standardy informacyjne w gospodarce*, Warszawa 1997, s. 132.
79 M. Ciecierski, *Wywiad gospodarczy w walce konkurencyjnej*. Warszawa 2007, s. 27-28.
80 J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 52.

- prawdopodobne – to informacje, które są zgodne z posiadanymi już informacjami, ale wymagają sprawdzenia i potwierdzenia,
- wątpliwe – to informacje, które są sprzeczne z posiadanymi informacjami i wymagają sprawdzenia i potwierdzenia,
- dezinformujące – to informacje, które nie odpowiadają aktualnej sytuacji organizacji gospodarczej konkurencji, co zostało stwierdzone na podstawie danych pochodzących z innego (innych) źródeł. Powinny być wykorzystywane w procesie poznawania metod dezinformacji stosowanych przez konkurencję.

W zarządzaniu „nie chodzi jednak o to, aby wiedzieć wszystko, lecz wiedzieć wystarczająco dużo, a przede wszystkim więcej niż przeciwnik”[81].

Niezwykle istotne jest zagadnienie zakłócania informacyjnego, które w działalności gospodarczej spełnia dwie ważne funkcje:

- pierwsza ma ścisły związek z tzw. pozorowaniem, mającym na celu wprowadzanie w błąd konkurenta,
- druga to dezorganizacja pracy systemu kierowania konkurencji.

W ramach prowadzonego zakłócania informacyjnego w sferze gospodarczej prowadzone są takie przedsięwzięcia, jak:

1. penetracja, która polega na niejawnym przeszukiwaniu realizowanym przez konkurencję w miejscu pracy lub innym, dla uzyskiwania dostępu do chronionych informacji (dokumentów) w ramach zaplanowanych przedsięwzięć w stosunku do konkretnego biznesmena lub przedsiębiorstwa;
2. dezinformacja, jako zaplanowane przedsięwzięcia wprowadzania w błąd, najczęściej poprzez przekazanie lub umożliwienie pozyskania fałszywych informacji;
3. inspiracja, jako zaplanowane przedsięwzięcia mające na celu osiągnięcie skutku zaplanowanego przez konkurencję.

Celem tych przedsięwzięć jest podjęcie przez organizację gospodarczą działań, które będą osłabiać jej pozycję na rynku lub eliminować ją z rynku.

Zarówno dezinformacja, jak i inspiracja należą do tych przedsięwzięć, których wdrożenie obok planowania wymaga posiadania właściwych informacji na temat strony dezinformowanej lub inspirowanej. Powyższe działania stosowane są w nieuczciwej walce konkurencyjnej firm wówczas, gdy istnieje konflikt interesów. W zależności od metod, sposobów, stosowanych środków i kanałów transmisji oraz ich treści, a także charakteru działań pozornych, można wyróżnić trzy formy dezinformacji: przekaz (ustny, pisemny), dokument, a także określone działania[82].

Na szczególną uwagę zasługuje wyróżniony przez A. Żebrowskiego system walki w sferze przetwarzania danych cyfrowych, która aktualnie stanowi największe zagrożenia, a są to w szczególności:

- międzynarodowa lub prywatna korporacja (atakujący) – baza danych i rozwoju konkurenta (obiekt ataku) – uzyskanie dostępu do informacji stanowiącej tajemnicę (aktualny cel działania) – uzyskanie korzyści w walce konkurencyjnej (cel strategiczny), – przerwanie działalności firmy, przepływu informacji czy prowadzonych transakcji finansowych (aktualny cel działania) – wydanie oświadczenia (cel strategiczny),

81 J. Janczak, *Zakłócanie informacyjne*, Warszawa 2001, s. 10, 11.

82 R. Szpyra, *Militarne operacje informacyjne*, Warszawa 2003, s.13.

- nieuczciwy lub rozczarowany pracownik (atakujący) system księgowości firmy (obiekt ataku) transfer pieniędzy na fałszywe konto, nawet po rozwiązaniu umowy o pracę (aktualny cel ataku) korzyści finansowe (cel strategiczny)[83].

Problematyka zakłócania informacyjnego w sferze gospodarczej zasługuje na szersze badania i analizy. Warto jednak przychylić się do poniższych wniosków:

- procesy informacyjne to podstawowy element funkcjonowania organizacji gospodarczych, a skuteczne ich zakłócanie prowadzi do pogorszenia sytuacji konkurencji;
- zakłócanie informacyjne jest prowadzone w dostępnych obszarach pozyskiwania informacji przez państwowe, międzynarodowe i prywatne korporacje gospodarcze;
- wspomniana działalność nie jest nowym zjawiskiem, była prowadzona zawsze, a postęp cywilizacyjny i towarzyszący jemu rozwój technologii teleinformatycznych sprawia, że zakłócanie jest coraz bardziej wyrafinowane i skuteczne[84].

## 9. Dokument jako podstawowy nośnik informacji

Z pojęciami dotyczącymi: danych, informacji, wiedzy i mądrości – istotnie związane jest pojęcie dokumentu jako nośnika informacji, jego znaczenie, określenie, a przede wszystkim jego autentyczności oraz możliwościami analizy zawartej w nim wiedzy.

W kwestii analizy informacji , jak trafnie stwierdza T. Nowak, *niezmiernie ważna jest analiza treści dokumentu, która możliwa jest tylko dzięki temu, że ujęta (wyrażona) została ona w odpowiedni sposób (graficznie) i na odpowiednim podłożu (papier, deska, płótno itp.). W odróżnieniu od innych przedmiotów, gdzie głównym punktem zainteresowania organu procesowego może być część graficzna (podrobienie lub przerobienie pisma) lub część materialna (podłoże) – dokument jako przedmiot stanowi wartość dowodową zawsze ze względu na zawartą w nim treść.*[85] W związku z tym na pojęcie dokumentu składają się łącznie cztery elementy:

1. treść dokumentu, czyli wypowiedź człowieka jako wyraz myśli ludzkiej,
2. strona graficzna dokumentu, czyli myśl wyrażona w odpowiednich znakach graficznych,
3. podłoże dokumentu, czyli odpowiedni materiał, na którym zawarta jest treść dokumentu,
4. autor dokumentu, czyli podmiot wyrażający swoją myśl.

Należy również pamiętać, iż niejednokrotnie w sprawach karnych wykorzystuje się również takie pisma, jak: listy prywatne, notatki, odręczne spisy, adnotacje, pozycje w księgach handlowych, w księgach podatkowych, umowy handlowe, umowy na otwarcie i prowadzenie rachunku bankowego, umowy kredytowe, a także takie dokumenty jak grypsy i inne zapiski, a w tym anonimy, w których wyrażona została myśl ludzka, a badana treść pozwala poznać ustalony w procesie fakt, pomimo że nie zawsze znany jest autor takiego pisma.

---

83 A. Żebrowski, *Zakłócanie informacyjne elementem rozwoju organizacji gospodarczej* w: J. Kaczmarek, M. Kwieciński, *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, 28.

84 Tamże, s. 29.

85 T. Nowak, *Dowód z dokumentu w polskim procesie karnym,* Poznań 1994, s. 23.

Gamę nośników informacji poszerzyła możliwość zapisywania ich na nośnikach elektronicznych. Badaniem tych dokumentów w różnorodnych aspektach, a także co do ich autentyczności zajmują się eksperci z zakresu informatyki śledczej.

W pojęciu dokumentu mieszczą się przede wszystkim pojęcia cywilnoprawne i karnoprawne. Przykładowo z analiz K. Knoppka na temat wymagań i formy sporządzania dokumentu wynika, że: *Dokument wyraża jakąś myśl ludzką, a zatem musi zawierać pewną treść. Pismo podpisane in blanco i jeszcze nie wypełnione treścią nie stanowi dokumentu. Nie jest bowiem dokumentem sam tylko podpis. Nie stanowi zarazem dokumentu zbiór bezsensownych zdań lub słów nie wyrażających niczego, np. pismo zawierające wyrazy pisane jako ćwiczenie językowe lub ortograficzne.*

Rola dokumentu jest wielostronna, a zatem nie musi być on sporządzony z zamiarem wywołania skutków prawnych lub w celu przygotowania ewentualnego dowodu dla sądu. Wydaje się, że najliczniejszą kategorią dokumentów są tzw. dokumenty przypadkowe, a wśród nich przede wszystkim listy, czyli dokumenty prywatne, a w ostatnich latach zapisy na płytach, pendrive'ach, elektronicznych bazach danych i innych nośnikach elektronicznych.

Definicja sprawozdawcza dokumentu w ujęciu prawa cywilnego procesowego brzmi: *Dokument to każda wyrażona na piśmie w jakimkolwiek języku stosowanym myśl ludzka opatrzona podpisem wystawcy, uzewnętrzniona w sposób trwały, nadający się do zwielokrotnienia oraz – przynajmniej formalnie – do zastosowania w postępowaniu cywilnym*[86].

Istotne znaczenie ma definicja zawarta w art. 6 ust. 2 uodip., która stanowi, że: *dokumentem urzędowym w rozumieniu ustawy jest treść oświadczenia woli lub wiedzy, utrwalona i podpisana w dowolnej formie przez funkcjonariusza publicznego w rozumieniu przepisów Kodeksu karnego, w ramach jego kompetencji, skierowana do innego podmiotu lub złożona do akt sprawy.*

Natomiast według art. 115 § 14 k.k. *dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.*

Definicja ta ujmuje pojęcie dokumentu szerzej od jego potocznego znaczenia. Forma dokumentu jest bowiem zróżnicowana. Może to być dokument papierowy albo treść o znaczeniu prawnym zapisana na innym materiale, czy nośniku elektronicznym.

Dokumentem jest zatem nie tylko zaświadczenie wystawione przez urząd, metryka, dyplom, umowa, kwit itp., lecz także bilet kolejowy, numerek z szatni i inne tego rodzaju przedmioty stanowiące dowód istnienia stosunku prawnego. Jak trafnie określa L. Gardocki przedmiot niebędący normalnie dokumentem może stać się dokumentem w rozumieniu prawa karnego w określonej sytuacji. Natomiast prywatny list nie jest dokumentem, ale może nabrać takiej cechy, jeżeli jego treść posiada znaczenie prawne np. w kontekście istnienia zobowiązania cywilnoprawnego, albo gdy może stanowić dowód faktu istotnego dla procesu[87].

Natomiast art. 393 § 1 k.p.k. wymienia następujące dokumenty mające znaczenie procesowe, a mianowicie: *protokoły oględzin, przeszukania i zatrzymania rzeczy, opinie biegłych, instytutów, zakładów lub instytucji, dane o karalności, wyniki wywiadu środowiskowego oraz wszelkie dokumenty urzędowe złożone w postępowaniu przygo-*

86 K. Knoppek, *Dokument w procesie cywilnym*, Poznań 1993, s. 35.

87 L. Gardocki, *Prawo karne*, Warszawa 2003, s. 302.

*towawczym lub sądowym albo w innym postępowaniu przewidzianym przez ustawę,* a ponadto: *zawiadomienie o przestępstwie*.

Kryterium karnoprocesowego podziału dokumentów na dokumenty urzędowe i prywatne zależy od roli i stanu prawnego wystawcy dokumentu. Zatem dokumenty urzędowe, czy publiczne pochodzą od:

1. organów i instytucji państwowych czy
2. organów samorządu terytorialnego, a także od
3. osób zaufania publicznego (np. notariuszy).

Warto przytoczyć wyniki rozważań G. Rejman, która niezwykle trafnie, a jednocześnie syntetycznie konkluduje, że problematyka prawna dotycząca dokumentów, (a także zawartych w nich informacji – dop. JWW) może być rozpatrywana z kilku punktów widzenia, a szczególnie:

1. z punktu widzenia określenia treści i istoty dokumentu,
2. funkcji spełnianych w życiu społecznym, a także
3. możliwości jego zniekształcenia i wprowadzenia do obrotu prawnego w sposób niedozwolony[88].

Z tego właśnie względu prawo karne zajmuje się przede wszystkim ochroną autentyczności dokumentu jako podstawą rzetelności obrotu prawnego, finansowego i gospodarczego. Nauki prawne związane z postępowaniem karnym i cywilnym poświęcają dokumentowi dużo więcej miejsca biorąc pod uwagę jego funkcję dowodową w ustaleniu istniejącego prawa, stosunku prawnego lub okoliczności mających znaczenie prawne. Wreszcie ustalenie prawdziwości lub nieprawdziwości dokumentu, jego zniszczenie, przekształcenie lub ustalenie zgodności z oryginałem jest domeną nauk kryminalistycznych, które prowadzą badania na ten temat.

Wszystkie te dziedziny wiedzy wiążą się ściśle ze sobą, a w niektórych wypadkach ustawa odsyła do biegłych z zakresu kryminalistyki celem ustalenia np. autorstwa czy autentyczności pisma albo zapisu na nośniku elektronicznym. W myśl art. 254 k.p.c. badania prawdziwości pisma dokonuje się z udziałem lub bez biegłych, zwłaszcza przez porównanie charakteru pisma na zakwestionowanym dokumencie z pismem tej samej osoby na innych dokumentach niewątpliwie prawdziwych[89].

Istotne jest zatem badanie autentyczności wszelkiego rodzaju dokumentów i nośników informacji, co do ich do wystawcy, producenta czy użytkownika, czyli znacznie szerzej niż tylko z punktu widzenia prawdziwości zapisanej informacji w określonym dokumencie, czy nośniku. Badanie autentyczności informacji zawartej w dokumencie może być prowadzone przykładowo przez właściwego eksperta na wariografie. Zatem problemem współczesnym jest nie tylko fałszerstwo dokumentu czy informacji, lecz również fałszerstwo nośników informacji, a także hakerstwo i piractwo internetowe poprzez nielegalny dostęp do cudzych dokumentów i informacji.

Współcześnie nośnikami informacji są dokumenty i właściwe urządzenia służące do przechowywania czy przekazywania danych, a także zbiorowego składowania oraz odczytu zebranych informacji. Są to: dokumenty, druki, nośniki elektroniczne, plany,

88 E. Bieńkowska, B. Kunicka-Michalska, G. Rejman, J. Wojciechowska, *Kodeks karny. Część ogólna.* Komentarz pod red. G. Rejman, Warszawa 1999, s. 1444.

89 Ustawa z dnia 17 listopada 1964 roku – Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296).

rysunki, opisy, pamięci taśmowe, dyski magnetyczne, dyski optyczne i pendrive'y[90]. Zapewne wkrótce powstaną nowe rodzaje nośników informacji służące przykładowo do utrwalania, przekazywania czy przechowywania informacji.

## 10. Informacja a zachowanie tajemnicy i oblicza prawdy

Niektóre informacje korzystają z ochrony prawnej. Zagadnienie ochrony informacji w różnych jej aspektach ma walor konstytucyjny zgodnie z art. 47, 49, 51 Konstytucji RP. Prawnokarna ochrona informacji ma także charakter wielopłaszczyznowy (chroni się bowiem integralność informacji, jej dostępność, a także poufność). Wspomniane przepisy można podzielić na trzy grupy:

1. przepisy chroniące informacje będące tajemnicą (zawodową lub prywatną oraz informacje niejawne),
2. przepisy chroniące informacje (ich nośniki) przed zniszczeniem lub naruszeniem,
3. przepisy chroniące urządzenia techniczne służące do utrwalenia i przekazywania informacji.

Z omawianym zagadnieniem wiąże się termin „tajemnica". Termin ten definiowany jest dość szeroko. Według *Słownika języka polskiego*, że jest to: „sekret czy nieujawnianie czegoś; wiadomość, której poznanie lub ujawnienie jest zakazane przez prawo; rzecz, której się nie rozumie lub nie umie wyjaśnić; najlepszy lub jedyny sposób na osiągnięcie czegoś"[91].

Istotą tajemnicy jest niejawność, czyli to, że informacje nią objęte nie są przeznaczone do udostępniania osobom postronnym, nieuprawnionym i z pewnych względów mogą czy też muszą pozostać znane tylko ściśle określonym jednostkom czy grupom osób.

Obowiązek zachowania tajemnicy to przede wszystkim zasada, by nie wchodzić w posiadanie informacji, do których nie ma się prawa dostępu. Ponadto, pracownicy powinni powstrzymać się od wykorzystywania i ujawniania informacji będącej tajemnicą osobom nieuprawnionym, bez względu na to czy zdobyli ją zgodnie z prawem. W przypadku ujawnienia zasady naruszenia tajemnic ustawowo chronionych pracownik lub inna osoba, która weszła w jej posiadanie, będzie podlegać odpowiedzialności karnej.

Ujawnianiem informacji jest każde zachowanie, w wyniku którego doszła ona do wiadomości osoby nieuprawnionej. Ujawnienia nie można utożsamiać z rozpowszechnianiem, które oznacza czynienie informacji powszechnie wiadomą, udostępnianie jej szerszemu, bliżej nieokreślonemu kręgowi osób. Sposób ujawnienia nie jest istotny – może to nastąpić w formie wypowiedzi ustnej, pisemnej, poprzez udostępnienie do odczytania dokumentów zawierających treści objęte tajemnicą, poprzez okazanie przedmiotów, przekazanie klucza umożliwiającego dostęp do miejsca przechowywania informacji, udostępnienie zapisu tekstowego czy elektronicznego, fotografii itp., a nawet przez gest lub mimikę92.

Ujawnić informację można zarówno przez działanie, jak i zaniechanie np. gdy sprawca pozostawi informacje objęte tajemnicą w miejscu do tego nieprzeznaczonym w taki sposób, że osoba nieuprawniona zapozna się z jej treścią.

90 http://mfiles.pl/pl/index.php/No%C5%9Bnik_informacji(21.04.2015).
91 http://sjp.pwn.pl/doroszewski/tajemnica;5506427.html(10.12.2014).
92 M. Mozgawa (red.), *Kodeks kamy. Komentarz*, Warszawa 2014, s. 663.

Ujawnienie to uczynienie jawnym tego, co dotychczas jawnym nie było. Forma czy sposób ujawnienia mogą być różne – może to być wypowiedź ustna, udostępnienie pisma zawierającego informacje niejawne, okazanie dokumentu lub przedmiotu, opublikowanie w masowych środkach przekazu, przesłanie informacji klasyfikowanej za pomocą technicznych środków przekazu, np. telefonu, e-maila.

Mając informację, a przynajmniej łatwy dostęp do niej, zespół wywiadu gospodarczego może prowadzić badania, opracowywać analizy oraz podejmować racjonalne decyzje. Otrzymuje bowiem materiał do przeanalizowania, wnioskowania i zarządzania. W dodatku może odpowiednio wcześnie podjąć działania zapobiegające powstaniu sytuacji kryzysowej.

W dobie informacji, wraz z upowszechnieniem się dostępu do informacji oraz zwiększeniem szybkości jej przepływu, informacja nabiera coraz większego znaczenia w codziennym życiu organizacji, firmy czy państwa. Subiektywność informacji niejednokrotnie powoduje, że jej wartość jest różna w zależności od jej odbiorcy i jego dotychczasowej wiedzy. Powoduje to problem w ocenie zarówno przydatności, jak i wartości, jaką reprezentuje analiza uzyskanych informacji.

Informacja, która stanowi etap pośredni w tworzeniu wiedzy, jest niezbędna przy podejmowaniu każdej decyzji. W aktualnym napływie informacji, a nawet w trakcie zalewu czy szumu często wyodrębnienie istotnych informacji stanowić może poważny problem. Zatem istotną umiejętnością jest właściwe zebranie i analizowanie informacji istotnych, możliwie jak najdokładniejszych, które będą decydujące w podejmowaniu decyzji dotyczących określonych przedsięwzięć.

Wiele różnorodnych zjawisk społecznych wymaga dociekań naukowych. Wieloma zebranymi w ten sposób informacjami można odpowiednio manipulować. Udaje się to nawet z pojęciem filozoficznym, jakim jest prawda. Arystoteles określił, że prawda „to zgodność, adekwatność treści sądu z rzeczywistym stanem rzeczy". Jednakże obecnie prawda jest pojęciem względnym. Wyniki analiz tego pojęcia uzależnione są od wielu czynników. Okazuje się, że mamy do czynienia z całym zestawem rodzajów i poziomów prawdy. Jako przykłady do dalszych analiz mogą być następujące oblicza prawdy:

- naukowa, odkrywana wraz z postępem nauki (np. do czasów M. Kopernika Słońce krążyło wokół Ziemi, od czasów odkrycia M. Kopernika Ziemia krąży wokół Słońca);
- statystyczna, która niejednokrotnie jest manipulowana i stosownie interpretowana według określonego zamówienia, zapotrzebowania czy potrzeb określonej grupy; zagadnienie to było już przedmiotem wielu uwag krytycznych; jeżeli nawet pominiemy te uwagi, warto podkreślić, że nie znamy rzeczywistych rozmiarów przestępczości, nie odzwierciedlają tego stosowane terminy: postępowania wszczęte czy przestępstwa stwierdzone; pomimo wielu osiągnięć naukowych to zagadnienie wciąż pozostaje wielką niewiadomą;
- procesowa, która mimo obowiązującej tajemnicy w trakcie prowadzonego postepowania jest wprawdzie zmienna wraz z rozwojem określonego etapu, lecz jest najlepiej rozpoznaną i wyznawaną przez strony procesowe, a jej wersje dotyczą przykładowo następujących etapów:

1. wszczęcia postępowania przygotowawczego,

2. wydania postanowienia o przedstawieniu zarzutów,
3. sporządzenia aktu oskarżenia,
4. wydania wyroków w pierwszej i drugiej instancji,
5. wydania aktu rehabilitacji,
6. wydania aktu łaski,
7. amnestii;

- sądowa, która ma również różne oblicza, a przykładowo, w powszechnie znanym procesie sądowym okazało się, że wyrok zasądzający przeprosiny w procesie o ochronę dóbr osobistych stanowi nie o tym, jaka jest prawda, ale o tym, że pozwany nie potrafił udowodnić swoich wypowiedzi93. W innej sprawie zapadł wyrok skazujący za zgwałcenie. Jednakże nikt już nie brał pod uwagę faktu, że sprawca i ofiara zostali małżeństwem, a ponadto zgodnie i szczęśliwie wychowują dwoje dzieci;
- medialna, która jest kształtowana przez media. Współczesny zalew informacji, a także szum informacyjny powoduje, że różnorodne, nie zawsze uczciwe tendencje doprowadzają do wielu trudności w rozpoznawaniu i ocenie rzeczywistego stanu rzeczy. Dotyczy to zarówno wielu zdarzeń i faktów, a także wypowiedzi i działań polityków oraz niektórych zachowań celebrytów94;
- emocjonalna, która wiąże się ze szczerością w ramach fikcji literackiej czy sytuacyjnej, a która nie jest moralnym przymiotem lecz tylko kwestią techniki wykorzystywanej w sztuce, a szczególnie w literaturze i filmie;
- obiektywna, czyli taka, która jest przedmiotem naszych dociekań i stałych dążeń do jej poznania.

Warto jeszcze zauważyć, że w niektórych przypadkach, w dążeniu do prawdy obiektywnej, dość często występuje jeszcze prawda polityczna, która wynika zarówno z poglądów określonej opcji politycznej, jak i z kierunków uprawiania polityki. Przykładem w tej mierze może być kontrowersyjne twierdzenie o wybuchu, który zniszczył polski samolot wraz z pasażerami w Smoleńsku. Różne opcje polityczne i ich eksperci mają na ten temat odrębne i podobno naukowo uzasadnione opinie[95].

93 M. Domagalski, *Prawda sądowa nie musi być całą prawdą,* „Rzeczpospolita" z 24 marca 2011 r.
94 Szerzej: P. Cyrek, *Rzeczywistość a przekaz medialny* w: A. Letkiewicz, A. Misiuk (red.) *Państwo, administracja, policja,* Szczytno 2012, s. 305 i n.
95 J.W. Wójcik, *Kryminologia. Współczesne aspekty*, Warszawa 2014, s. 60, 61.

# Rozdział 2

# Tajemnice zawodowe i szczególna rola tajemnicy przedsiębiorstwa

## 1. Obowiązek zachowania tajemnicy zawodowej

Termin tajemnica definiowany jest dość szeroko. Według *Słownika języka polskiego* jest to: „sekret czy nieujawnianie czegoś; wiadomość, której poznanie lub ujawnienie jest zakazane przez prawo; rzecz, której się nie rozumie lub nie umie wyjaśnić; najlepszy lub jedyny sposób na osiągnięcie czegoś"[96]. Według Wikipedii określany jest jako dane lub informacje, których ujawnienie osobom nieuprawnionym jest zakazane ze względu na normy prawne lub inne normy społeczne [97].

Dokonując podziału rodzaju informacji na jawne i poufne, a więc zawierające tajemnice zawodową lub inną prawnie chronioną, należy wspomnieć, że praktycznie w żadnym akcie prawnym nie jest zawarta pełna definicja tajemnicy zawodowej, pomimo że niektóre ustawy posługują się tą terminologią.

Warto zatem podkreślić, że termin tajemnica zawodowa istnieje wówczas, gdy wiadomość nią objęta została uzyskana przez osobę reprezentującą określony zawód, z tytułu wykonywania którego było możliwe wejście w posiadanie cudzej tajemnicy czy sekretu[98]. Ustalenie obowiązku zachowania tajemnicy zawodowej może wynikać wprost z przepisów regulujących tryb i zasady wykonywania określonych zawodów bądź z przyjęcia na siebie zobowiązania, co do nieujawniania faktów poznanych w związku z wykonywaną pracą zawodową[99]. Źródłem obowiązku zachowania dyskrecji w przypadku tajemnicy zawodowej nie muszą być wyraźne przepisy prawne, lecz także zasady etyki zawodowej.

Tajemnica zawodowa ma dwojaki charakter, tzn. może obejmować wiadomości, które dotyczą życia określonych osób, uzyskane w ramach dokonywania czynności zawodowych czy też pełnionych funkcji, oraz informacje dotyczące samego zawodu i sposobu jego wykonywania. Przykładem w tej mierze może być przepis art. 266 § 1 k.k., który nie dotyczy jednak tylko tajemnicy zawodowej, ma bowiem zakres o wiele szerszy – obejmuje także każdą tajemnicę, poznaną w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową.

96 http://sjp.pwn.pl/lista/T;6.html(22.9.2014)

97 http://pl.wikipedia.org/wiki/Tajemnica(12.12.2014)

98 W. Wróbel, *Niektóre problemy ochrony tajemnicy w projekcie kodeksu karnego,* "Przegląd Prawa Karnego" 1996, nr 14, 15.

99 Tamże.

Stąd też ten rodzaj tajemnicy określany jest także jako tajemnica funkcyjna[100]. Pojęcie tajemnicy prywatnej natomiast używane być może ze względu na rodzaj informacji stanowiących przedmiot tajemnicy, tj. dotyczących prywatnej sfery życia dysponenta informacji[101].

Źródłem obowiązku zachowania tajemnicy zawodowej jest art. 266 § 1 k.k. bądź inny konkretny przepis prawa (np. art. 40 ustawy o zawodach lekarza i lekarza dentysty), bądź też umowa pomiędzy dysponentem informacji i depozytariuszem, której treścią jest przyjęcie zobowiązania dyskrecji[102]. Oczywista staje się zatem uwaga, że tajemnicą nie może być informacja powszechnie znana.

Przepisy prawa regulują następujące rodzaje tajemnic, związanych najczęściej właśnie z pełnioną funkcją, wykonywanym zawodem, prowadzoną działalnością: sędziowską, prokuratorską, adwokacką, radcowską, notarialną i inne.

Kolejnym przykładem informacji, która jest chroniona przepisami kodeksu karnego jest tajemnica korespondencji. Pojęcie to oznacza, iż wszystko, co jest przedmiotem przekazu od nadawcy do adresata, należy wyłącznie do tych osób, z wyjątkiem sytuacji, gdy wyrażą one zgodę na udostępnienie również innym informacji, które między sobą przekazują.

Tajemnica korespondencji jest istotną częścią składową prawa do poszanowania życia prywatnego, w tym również do poszanowania jej tajemnicy. Naruszenie tajemnicy korespondencji podlega karze z mocy prawa (art. 267 § 1 kodeksu karnego). W sytuacjach szczególnych (np. związanych ze ściganiem poważnych przestępstw) przepisy zezwalają na naruszenie tajemnicy korespondencji[103]. Szeroki zakres tematyki skłania do konieczności omówienia jedynie wybranych zagadnień tego interesującego zagadnienia.

## 2. Wybrane rodzaje tajemnic zawodowych

Mówiąc o problemach ochrony informacji, najczęściej mamy na myśli tylko te elementy wiadomości, które są opatrzone klauzulą tajne specjalnego znaczenia czy tajne, Mamy jeszcze informacje poufne i zastrzeżone, które są również prawnie chronione.

Znanych jest przynajmniej 58 różnych aktów prawnych, regulujących te problemy; począwszy od Konstytucji RP aż po prawo kanoniczne i kodeks postępowania karnego oraz różne tajemnice zawodowe. Przepisy te regulują różnorodne rodzaje tajemnicy, nie tylko o charakterze strategicznym czy przemysłowym, ale przykładowo takie jak: tajemnica lekarska, spowiedzi, czy prawo geologiczne i górnicze. Wszystkie one podlegają ochronie prawnej zgodnie z przepisami szczegółowymi, a ich ujawnienie w niektórych przypadkach jest ścigane według regulacji karnoprawnych.

Zagadnienie ochrony informacji przejawia się w obowiązującym stanie prawnym. Można zatem wyróżnić szereg rodzajów tajemnic zawodowych prawnie chronionych[104], a przykładowo: tajemnica handlowa, ksiąg rachunkowych, bankowa, ubez-

100 Kunicka-Michalska *Przestępstwa przeciwko tajemnicy państwowej i służbowej*, w: *System Prawa Karnego* 1989, s. 445, 446. Cyt. za M. Mozgawa, *Kodeks karny. Komentarz*, Warszawa 2014, s. 666.

101 Tamże.

102 T. Bojarski (red.), *Kodeks karny. Komentarz,* Warszawa 2011, s. 638.

103 Tamże.

104 Szerzej R i M. Taradejna, *Ochrona informacji w działalności gospodarczej, społecznej i zawodowej oraz życiu prywatnym,* Warszawa 2004, s. 24-253.

pieczeniowa, publicznego obrotu papierami wartościowymi, doradcy podatkowego i biegłego rewidenta, tajemnice rzeczoznawców majątkowych, pośredników w obrocie nieruchomościami i zarządców nieruchomościami, adwokacka i radcowska, notarialna, komornika sądowego, funduszy inwestycyjnych, wynalazcza, skarbowa, statystyczna, dziennikarska, autorska, detektywistyczna, pomocy społecznej, spowiedzi[105], służby więziennej, wojskowa, geologiczna i geodezyjna, wolności sumienia i wyznania, akt stanu cywilnego, tajności głosowania w wyborach, ubezpieczeń społecznych, majątkowych i osobowych, postępowania administracyjnego, postępowania karnego, świadka koronnego, czynności operacyjno-rozpoznawczych gromadzenia, przetwarzania i przekazywania informacji kryminalnych i szereg innych.

W zasadzie tajemnice te chronione są właściwymi aktami prawnymi, a przykładowo:

- tajemnica lekarska – ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[106],
- prokuratorska – ustawa z dnia 20 czerwca 1985 r. o prokuraturze[107],
- radcowska – ustawa z dnia 6 lipca 1982 r. o radcach prawnych[108],
- notarialna – ustawa z dnia 14 lutego 1991 r. - Prawo o notariacie[109],
- komornicza – ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji[110],
- dziennikarska – ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe[111],
- pielęgniarska i położnicza – ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej[112],
- psychiatryczna – ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego[113],
- psychologa – ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów[114],
- przeszczepów – ustawa z dnia lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów[115].

Należy mieć na uwadze indywidualną czy specyficzną wiedzę pracownika, która nie stanowi tajemnicy przedsiębiorstwa. Dotyczy to osobistych umiejętności, specyficznego zakresu wiedzy i doświadczeń pracownika, o ile nabytych informacji nie można utrwalić lub przekazać innemu podmiotowi w postaci opisu, planu, rysunku

105 Z aktu oskarżenia przeciwko zakonnikowi z Zakroczymia wynika, że do uwodzenia chłopców poniżej lat 15 duchowny miał wykorzystywać informacje zdobyte w konfesjonale, a więc w ramach tajemnicy spowiedzi. Szerzej: J. Bilikowska, *Prokuratura: cztery ofiary zakonnika pedofila,* „Rzeczpospolita" z 11 sierpnia 2014 r.

106 t. j. Dz. U. z 2011 r. Nr 277, poz. 1634 ze zm.

107 t.j. Dz. U. z 2011 r. Nr 270, poz. 1599 ze zm.

108 t.j. Dz. U. z 2014 r. poz. 637 ze zm.

109 t.j. Dz. U. z 2014 r., poz. 164.

110 t.j. Dz. U. z 2011 r. Nr 231, poz. 1376 ze zm.

111 Dz. U. Nr 5, poz. 24 ze zm.

112 Dz. U. Nr 174, poz. 1039 z późn. zm.

113 t.j. Dz. U. z 2011 r. Nr 231, poz. 1375 ze zm.

114 Dz. U. Nr 73, poz. 763 ze zm.

115 Dz. U. Nr l69, poz. 1411 ze zm.

itp. W związku z tym zatrudnionemu wolno je swobodnie wykorzystywać w celach zawodowych. Przedsiębiorca może jednak ograniczyć posługiwanie się informacjami nabytymi mimo woli w związku z zajmowanym stanowiskiem poprzez wprowadzenie zakazu konkurencji. Stanowi to umowne ograniczenie pracownika w podejmowaniu działalności mogącej naruszyć interesy przedsiębiorcy. Zatem zakaz konkurencji stanowi dodatkowe narzędzie, które umożliwia pracodawcy zintensyfikowaną ochronę tajemnic firmy. Nie ulega wątpliwości, że jeśli pracownik podejmuje pracę u innego przedsiębiorcy, zwłaszcza na zbliżonym stanowisku, to z dużym prawdopodobieństwem będzie wykorzystywał informacje nabyte w pierwszej firmie. Jeżeli zatem szef wprowadzi pracownikowi zakaz konkurencji, to wyeliminuje lub ograniczy posługiwanie się przez niego informacjami poufnymi.

Zakres przedmiotowy tajemnicy przedsiębiorstwa ujęty został przez ustawodawcę bardzo szeroko. Opisany w ustawie katalog informacji mogących stanowić tajemnice przedsiębiorstwa w zasadzie wyczerpuje zakres informacji, które mogą zostać wykorzystane przez przedsiębiorcę w związku z prowadzoną działalnością gospodarczą. Na podstawie doświadczeń orzecznictwa sądowego oraz doktryny przedmiotu da się wskazać pewien zakres typowych informacji mogących stanowić tajemnicę przedsiębiorstwa. We współczesnej literaturze prawniczej przyjmuje się, iż tajemnicę przedsiębiorstwa stanowić mogą między innymi:

1. nieopatentowane wynalazki,
2. plany techniczne, listy klientów,
3. wiedzę i metody natury administracyjnej i organizacyjnej,
4. metody kontroli jakości, sposoby marketingu, organizacji pracy,
5. treść zawartych umów, porozumień, korespondencję handlową,
6. strategię funkcjonowania przedsiębiorstwa,
7. informacje dotyczące techniki czy sposobu produkcji,
8. informacje dotyczące struktury przedsiębiorstwa, przepływu dokumentów, sposobu kalkulacji cen, zabezpieczenia danych,
9. treść opinii prawnych udzielanych przedsiębiorcy,
10. treść negocjacji czy prace nad nowym rozwiązaniem[116].

Z kolei w praktyce sądowniczej jako tajemnice przedsiębiorstwa uznane zostały między innymi:

1. dane zawarte w sprawozdaniach podatkowych PIT-5 i F-01, gdyż obrazuję one pasywa jak i aktywa oferentów, dochód i zyski, koszty działalności, straty, zobowiązania finansowe[117],
2. dane obrazujące wielkość produkcji i sprzedaży, a także źródła zaopatrzenia i zbytu[118],
3. informacje o planach wydawniczych[119],
4. wyniki finansowe stowarzyszenia i regulamin repartycji wynagrodzeń autorskich[120].

116 R. Bieda, *Zakres pojęcia „tajemnica przedsiębiorstwa" na gruncie ustawy o zwalczaniu nieuczciwej konkurencji*, http://www.itlaw.pl, s. 4 (23.09.2014).

117 Orzeczenie Sądu Antymonopolowego z 10.07.2002 r. XVII Am 78/01, Dz. Urz. UOKiK z 2002, Nr 5, poz. 224.

118 Postanowienie Sądu Antymonopolowego z 15.10.1997 r. XVII Ama 1/96, "Wokanda" 1997, Nr 10, poz. 55.

119 Wyrok Sądu Apelacyjnego w Krakowie z 11.06.2003 r. I A Ca 469/03, TPP 2004, Nr 1-2, s. 157.

120 Wyrok SN z 05.09.2001 r. I CKN 1159/00, OSNC 2002, Nr 5, poz. 67.

Nie ulega wątpliwości, że przedsiębiorca może ustanowić tajemnicę przedsiębiorstwa dotyczącą również danych o: klientach, dostawcach, metodach i procedurach szkolenia pracowników, planach inwestycyjnych i produkcyjnych, założeniach cenowych produktów, wynikach przeprowadzonych testów i badań marketingowych, a także o wynagrodzeniach pracowników.

## 3. Czyny nieuczciwej konkurencji jako manipulowanie informacją

Jednym z kluczowych zagadnień w gospodarce narodowej jest działalność przedsiębiorców i tajemnica przedsiębiorstwa. Mają one oczywiste związki biznesowe z konkurencją, a niejednokrotnie z nieuczciwą konkurencją, a ponadto z manipulowaniem informacją czy z wywiadem gospodarczym lub szpiegostwem gospodarczym.

Konkurencja (z jęz. łacińskiego *concurrentia*) czyli współzawodnictwo towarzyszy zachowaniu przedsiębiorców uczestniczącym w rynku. Wynikają z tego przynajmniej dwa wnioski: konkurencja jest zjawiskiem zupełnie naturalnym oraz możliwe jest jej występowanie tylko w ramach gospodarki wolnorynkowej. Można się pokusić o stwierdzenie że w sensie ekonomicznym konkurencja jest jednym z podstawowych elementów napędzających rozwój gospodarczy. Konkurencja to *dążenie wielu niezależnych przedsiębiorców na wspólnym dla nich rynku do osiągnięcia takiego samego celu gospodarczego, w szczególności prowadzenia interesów z dostawcami, odbiorcami i pracownikami*[121].

Czyny nieuczciwej konkurencji zostały określone w art. 1-17d ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (uznk)[122]. Zgodnie z art. 3 tej ustawy czynem nieuczciwej konkurencji jest działanie sprzeczne z prawem lub obyczajami, zagrażające lub naruszające interesy innego przedsiębiorcy lub klienta. Oznacza to, że muszą być spełnione określone zachowania przedsiębiorcy, aby można było uznać, że są one czynem nieuczciwej konkurencji. Uzasadniony jest pogląd, że muszą wystąpić łącznie następujące przesłanki:

1. przedsiębiorca musi działać w obrocie gospodarczym, tj. w ramach działalności gospodarczej;
2. działanie przedsiębiorcy musi być niezgodne z prawem lub dobrymi obyczajami;
3. czyn ten musi zagrażać lub też naruszać interes innego przedsiębiorcy lub klienta – w ramach interesu o charakterze gospodarczym[123].

Zachowania, które zawarto w regulacji ustawowej jako czyny nieuczciwej konkurencji zostały ujęte w artykułach od 5 do 17d uznk. Jako główne znamiona tych czynów w szczególności są:

1. wprowadzające w błąd oznaczenie przedsiębiorstwa (art. 5, 6 i 7);
2. fałszywe lub oszukańcze oznaczenie pochodzenia geograficznego towarów albo usług (art. 8, 9 i 10);

121 J. Szwaja, *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, Warszawa, 2006, s.42

122 Dz.U. z 2010 r. nr 113, poz. 759.

123 M. Mrzygłód, *Jak bronić się przed nieuczciwą konkurencją,* http://msp.money.pl/wiadomosci/prawo/artykul/jak;bronic;sie;przed;nieuczciwa;konkurencja,51,0,707379.html(3.03.2012)

3. wprowadzające w błąd oznaczenie towarów lub usług, jeżeli może wprowadzić klientów w błąd co do tożsamości producenta lub produktu (art. 10 i 13);
4. naruszenie tajemnicy przedsiębiorstwa (art. 11) oraz szpiegostwo gospodarcze (art. 23 ust. 2 uznk);
5. nakłanianie do rozwiązania lub niewykonania umowy (art. 12);
6. naśladownictwo produktów (art. 13)
7. pomawianie lub nieuczciwe zachwalanie (art. 14);
8. utrudnianie dostępu do rynku, na przykład poprzez stosowanie cen dumpingowych (art. 15);
9. przekupstwo osoby pełniącej funkcję publiczną (art. 15a);
10. nieuczciwa lub zakazana reklama (art. 16);
11. organizowanie systemu sprzedaży lawinowej (art. 17a),
12. prowadzenie lub organizowanie działalności w systemie konsorcyjnym (17c i 17d).

Celem omawianej ustawy jest zabezpieczenie istnienia konkurencji. Dopiero działanie sprzeczne z prawem lub dobrymi obyczajami jest zabronione, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta. W różnych krajach występują formy obrony przed nieuczciwą konkurencją. Natomiast w naszym kraju występuje również pojęcie dobrych obyczajów.

Czyny nieuczciwej konkurencji powodują wiele różnorodnych skutków oraz konsekwencji społecznych, ekonomicznych i prawnych. Przykładowo, zgodnie z art. 89 ust. 1 pkt 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych[124], zamawiający odrzuca ofertę, gdy jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów tej ustawy.

## 4. Naruszenie tajemnicy przedsiębiorstwa – pojęcie i zakres

Mając na względzie analizę informacji dotyczących obrotu gospodarczego, warto preferować tezę, która brzmi: Przedsiębiorstwo, które nie stosuje profesjonalnych zasad bezpieczeństwa, wkrótce zanotuje poważne straty. Natomiast bezpieczeństwo informacji prawnie chronionych jest podstawowym obowiązkiem związanym z bezpieczeństwem firmy i tajemnicą przedsiębiorstwa.

Regulacja prawna dotycząca naruszenia tajemnicy przedsiębiorstwa została zawarta w art. 11 ust. 4 uznk. Wynika z niej, że przez tajemnicę przedsiębiorstwa należy rozumieć 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.

Zatem tajemnicę przedsiębiorcy należy traktować jako tajemnicę przedsiębiorstwa. Należy podkreślić, że o uznaniu konkretnej informacji za tajemnicę decyduje zawsze sam przedsiębiorca, podejmując działania w kierunku zachowania ich poufności. Zatem za czyn nieuczciwej konkurencji uznaje się: przekazanie, ujawnienie, wykorzystanie, nabycie od nieuprawnionego cudzych informacji, stanowiących tajemnicę przedsiębiorstwa.

124 Dz. U. z 2010 r. nr 113, poz. 759.

Definicje tego czynu stosuje się również do osoby, która świadczyła pracę na podstawie stosunku pracy lub innego stosunku prawnego – przez okres 3 lat od jego ustania, chyba, że umowa stanowi inaczej albo ustał stan tajemnicy[125].

Zdarza się, że skrzętnie ukrywane receptury, składniki czy technologie, nowatorskie przedsięwzięcia organizacyjne, a nawet dane obrazujące wielkość produkcji i sprzedaży, źródła zaopatrzenia i konkurencyjnego zbytu – stanowią informacje, które przedostając się do konkurencji, mogą doprowadzić do poważnych perturbacji ekonomicznych, a nawet do upadłości dobrze dotąd prosperującej firmy.

W zasadzie zarządy przedsiębiorstw zwracają istotną uwagę na ochronę zagadnień informacji i tajemnic, stanowiących niematerialne walory, a nawet majątek przedsiębiorstwa. Zazwyczaj są to zarówno techniczne, jak i organizacyjne *know-how*, wypracowane specjalistyczne systemy technologiczne oraz inne informacje poufne. Takie informacje najczęściej stanowią tajemnicę przedsiębiorstwa, która jest prawnie chroniona w myśl art. 11 uznk. Niejednokrotnie przedsiębiorcy wykonują wiele przedsięwzięć w celu ochrony tych danych, lecz nie zawsze skutecznie. Ujawnienie tego typu informacji nawet przez byłego pracownika stanowi czyn nieuczciwej konkurencji.

Zgodnie z art. 11 ust. 2 uznk były pracownik, który w ciągu trzech lat od ustania stosunku pracy dopuści się przekazania, ujawnienia lub wykorzystania informacji stanowiących tajemnicę byłej firmy, jeżeli zagraża to lub narusza jej interes – może być pociągnięty do odpowiedzialności.

Dokładne kwestie powinny być sprecyzowane w ramach umowy konkurencyjnej. Natomiast ujawnienie tajemnicy przedsiębiorstwa nie zostanie zakwalifikowane w ten sposób tylko wtedy, gdy zawarta między pracownikiem a ówczesnym pracodawcą umowa stanowi inaczej albo ustał stan tajemnicy, czyli upłynął czas ochrony lub tajemnice stały się jawne.

Pracodawca nie będzie jednak miał gwarancji, że były pracownik nie podejmie zatrudnienia w konkurencyjnym przedsiębiorstwie. Jednakże fakt taki nie upoważnia do wykorzystywania informacji, które stanowiły tajemnicę poprzedniego pracodawcy. Niezwykle ważne są walory praktyczne tego przepisu. Istotą jest bowiem, aby informacje podlegające ochronie nie mogły być ujawnione do wiadomości publicznej. Zatem przedsiębiorca powinien zadbać, jeszcze w trakcie zatrudnienia, aby podejmować właściwe działania, zmierzające do zachowania określonych informacji w należytej staranności co do ich poufności. Związane jest to przede wszystkim z poinformowaniem pracowników o poufnym charakterze określonych działań i wiadomości.

W praktyce pracodawca dla zastosowania skutecznych działań ochronnych powinien przedstawić każdemu z zatrudnionych na piśmie zakres danych objętych tajemnicą przedsiębiorstwa. Każdy z właściwych pracowników powinien potwierdzić ich otrzymanie. Taka procedura zapewnia dochodzenie roszczeń od byłego pracownika, gdyby takie wiadomości ujawnił. Zatem należy:

1. określić chronione dane jako poufne, tuż po ich powstaniu,
2. powiadomić personel, że dane te nie mogą być ujawnione osobom niepoważnionym,
3. zastosować ochronę fizyczną lub elektroniczną np.: monitoring, dozór fizyczny, kontrola dostępu do pomieszczeń,

125 R. Blichniarz, J. Grabowski, M. Pawełczyk., K. Pokryszka , E. Przeszło, *Publiczne prawo gospodarcze. Zarys wykładu* pod red. J. Grabowskiego, Bydgosz-Katowice 2008, s.143.

4. zastosować środki prawne takie jak: wprowadzenie dodatkowych klauzul do umów o pracę, oddzielnych umów o poufności czy zakazie konkurencji,
5. przedstawić każdemu z zatrudnionych na piśmie zakres danych objętych tajemnicą przedsiębiorstwa. Każdy z pracowników powinien potwierdzić ich otrzymanie. Taka procedura zapewnia dochodzenie ewentualnych roszczeń od byłego pracownika..

Interesujące jest w tej kwestii stanowisko Sądu Najwyższego, który orzekł, że jeżeli nawet szef nie zawrze z podwładnym na piśmie zakazu konkurencji po ustaniu stosunku pracy, nie zwalnia to byłego pracownika z obowiązku zachowania w tajemnicy informacji poufnych. Zatem zwolnienie byłych pracowników z zakazu konkurencji po ustaniu stosunku pracy nie jest równoznaczne z godzeniem się przez byłego pracodawcę na ujawnienie informacji stanowiących tajemnice przedsiębiorstwa przez pracowników lub na uczynienie z nich dowolnego użytku, zwłaszcza sprzecznego z interesem pracodawcy[126].

Na tle omawianego zagadnienia istotne jest określenie informacji nieujawnionej. Zatem informacja nieujawniona do wiadomości publicznej to dane nieznane ogółowi lub osobom, które ze względu na wykonywany zawód są zainteresowane jej posiadaniem. Taka informacja mieści się w pojęciu „tajemnicy przedsiębiorstwa", w przypadku gdy przedsiębiorca wyraża (łatwo dostrzegalną) wolę, aby pozostała ona tajemnicą, zwłaszcza dla konkurencji[127].

Tym niezwykle ważnym zagadnieniem również zajął się Sąd Najwyższy, który zgodnie z wyrokiem z 3 października 2000 r., sygn. akt I CKN 304/00 orzekł, że wykorzystanie przez pracownika we własnej działalności gospodarczej informacji, co do których przedsiębiorca (pracodawca) nie podjął niezbędnych działań w celu zachowania ich poufności, należy traktować jako wykorzystanie powszechnej wiedzy, do której przedsiębiorca nie ma żadnych ustawowych uprawnień. Nie każda bowiem informacja (wiadomość) technologiczna i handlowa mieści się w pojęciu „tajemnicy przedsiębiorstwa". Istnieje różnica między wiadomościami odpowiadającymi treści pojęcia „tajemnica przedsiębiorstwa" a informacjami wchodzącymi w skład powszechnej, aczkolwiek specjalistycznej wiedzy zdobytej przez pracownika w wyniku własnej działalności zawodowej podczas zatrudnienia. Tajemnica przedsiębiorstwa jest chroniona z mocy ustawy przez cały okres zatrudnienia oraz w ciągu 3 lat od jego ustania, chyba że umowa stanowi inaczej lub ustał stan tajemnicy. Natomiast wiedza, doświadczenia i umiejętności zdobyte przez pracownika podczas zatrudnienia nie korzystają z ustawowej ochrony na rzecz przedsiębiorstwa, choć – ze względu na zasadę swobody umów – dopuszcza się możliwość zawarcia przez strony (pracodawcę i pracownika) porozumienia zawierającego klauzulę ograniczającą posługiwanie się tą wiedzą w celach konkurencyjnych po ustaniu zatrudnienia.

W podsumowaniu warto sprecyzować, że określona informacja stanowi tajemnicę przedsiębiorstwa, jeżeli spełnia łącznie trzy podstawowe warunki:

1. ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą,
2. nie została ujawniona do wiadomości publicznej,
3. podjęto w stosunku do niej niezbędne działania w celu zachowania poufności.

126 Wyrok SN z 25 stycznia 2007 r. nr I PK 207/06.

127 http://mojafirma.infor.pl/dzialalnosc-gospodarcza/56129,Ochrona-tajemnicy-przedsiebiorstwa.html(2.07.2012)

Aktualna treść tej regulacji jest zgodna z przepisem art. 39 *Agreement on Trade – Related Aspects of Intellectual Property* – TRIPS, tj. Porozumieniem sporządzonym w Marakeszu w sprawie Handlowych Aspektów Własności Intelektualnej z dnia 15 kwietnia 1994 r. [128]. Oznacza to, że osoby fizyczne i prawne będą miały możliwość zapobiegania, aby informacje pozostające w sposób zgodny z prawem pod ich kontrolą nie zostały ujawnione, nabyte lub użyte bez ich zgody przez innych, w sposób sprzeczny z uczciwymi praktykami handlowymi, jak długo takie informacje:

1. są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zespole ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które normalnie zajmują się tym rodzajem informacji;
2. mają wartość handlową, dlatego, że są poufne;
3. poddane zostały przez osobę, pod której legalną kontrolą informacje te pozostają rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich poufności.

Zatem ochronie podlegają wyłącznie informacje pozyskane zgodnie z prawem (tzw. przesłanka legalności). Przesłanka ta nie została jednak wprowadzona do treści art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji. W konsekwencji uzasadniając odmowę ochrony w ramach ustawy o zwalczaniu nieuczciwej konkurencji informacji uzyskanych w sposób nielegalny.

Powszechnie przyjmuje się, że informacja ma charakter technologiczny wówczas, gdy dotyczy najogólniej rozumianych sposobów wytwarzania, formuł chemicznych, wzorów i metod działania.

Natomiast informacja handlowa obejmuje, całokształt doświadczeń i wiadomości przydatnych do prowadzenia przedsiębiorstwa, niezwiązanych bezpośrednio z cyklem produkcyjnym.

Informacja nieujawniona do wiadomości publicznej to informacja nieznana ogółowi lub osobom, które ze względu na prowadzoną działalność są zainteresowane jej posiadaniem. Taka informacja staje się tajemnicą przedsiębiorstwa, kiedy przedsiębiorca chce, by pozostała ona tajemnicą dla pewnych kół odbiorców, konkurentów i jego wola jest jasna dla innych osób. Bez takiej woli, choćby tylko domniemanej, informacja może być nieznana, ale nie będzie tajemnicą[129].

## 5. Dobro zakładu pracy a tajemnica przedsiębiorstwa

Każdy pracownik ma obowiązek potwierdzenia faktu, że znane są mu przepisy dotyczące obowiązku poufności, a w szczególności art. 100 § 2 ustawy z dnia z dnia 26 czerwca 1974 r. kodeks pracy[130], który stanowi, że pracownik jest obowiązany w szczególności: dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę; przestrzegać tajemnicy określonej w odrębnych przepisach, a także potwierdzić znajomość art. 11 uznk oraz sankcje związane z naruszeniem obowiązku zachowania tajemnicy. Ponieważ skutkiem ujawnienia informacji ma być szkoda, przyjąć należy, że

128 Dz. U. WE L 336 z 23.12.1994, s. 214.

129 http://msp.money.pl/wiadomosci/prawo/artykul/tajemnica;przedsiebiorstwa;przy;starcie;w;przetargu,131,0,555651.html(2.07.2012)

130 tj. Dz.U. 2014 poz. 1502.

obowiązek zachowania tajemnicy chronić ma informacje istotne z punktu widzenia interesów pracodawców.

Przestrzeganie tajemnicy przedsiębiorstwa ma istotne znaczenie strategiczne w związku z prowadzoną działalnością, a zatem ma charakter ekonomiczny. Podstawowym wskaźnikiem ekonomicznego znaczenia tajemnic handlowych jest częstotliwość naruszania chronionych informacji. Można nawet wnioskować, że liczba ataków na chronione dobro wyznacza w pewnym sensie jego gospodarcze znaczenie. W prowadzonych badaniach przez różne wyspecjalizowane firmy na temat przestępczości gospodarczej, wśród wielu przedsiębiorstw z różnych krajów świata, wykazano, że działania naruszające tajemnicę przedsiębiorstwa, stanowią poważne zagrożenia w stosunku do wszystkich przypadków przestępstw gospodarczych, z którymi stykali się przedsiębiorcy. Wprawdzie najwięcej zanotowano przypadków kradzieży mienia (60%), jednakże, jak podkreślają autorzy raportu, takie dane są z pewnością konsekwencją faktu, że kradzież mienia jest stosunkowo łatwa do wykrycia, czego nie można na przykład powiedzieć o bezprawnym przywłaszczeniu tajemnic przedsiębiorstwa. Jeżeli jednak przyjrzymy się wysokości szkody, której doznało przedsiębiorstwo w wyniku naruszenia tajemnic przedsiębiorstwa, pomimo że tylko 7% przedsiębiorców zetknęło się z tym rodzajem naruszenia, wysokość strat wyniosła ponad 4 mln dolarów i była wyższa niż w przypadku np. fałszerstw produktów, z którym zetknęło się aż 19% przedsiębiorców[131].

Powyższe dane potwierdzają przyjęte założenie o strategicznym znaczeniu pewnych informacji w działalności przedsiębiorstwa. Wyniki analiz naświetlają kilka interesujących faktów związanych z ochroną tajemnic przedsiębiorstwa, a mianowicie:

1. wskazują, że najczęściej przywłaszczane są tajemnice dotyczące procesu produkcyjnego i informacji o nowych rozwiązaniach technologicznych, co oznacza, że centralnym przedmiotem zamachu jest tradycyjnie rozumiane *know-how*, a dopiero w dalszej kolejności inne informacje, posiadające wartość gospodarczą;
2. ujawniają bardzo ciekawy aspekt źródeł zagrożenia dla tajemnic przedsiębiorstwa. W tym zakresie przedsiębiorcy za największe zagrożenie dla swoich tajemnic w relacjach wewnętrznych uznają partnerów handlowych w postaci dostawców lub partnerów strategicznych;
3. doprowadzają do uzasadnionej obawy, że do ujawnienia tajemnic przedsiębiorstwa następuje przez byłych i obecnych pracowników;
4. podmioty zewnętrzne, to duże zagrożenie powodowane przez konkurentów krajowych i zagranicznych[132];
5. hakerzy komputerowi, których działalność wskazuje na fakt, że rozwój informatyczny, który przyczynił się do zwiększenia roli informacji we współczesnym świecie, stał się jednocześnie zagrożeniem dla posiadanych przez przedsiębiorców tajemnic[133].

Co zatem jest istotne w ramach tajemnic, które może poznać konkurencja. Pracownik może wynieść m.in. bazy kontrahentów, informacje o cenach i upustach, którymi

131 A. Michalak, *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, Warszawa 2006, s. 22.

132 M. Duszczyk, *Polskie firmy na celowniku szpiegów*, „Rzeczpospolita" z 16 października 2014 r. oraz tegoż *Polski biznes rajem złodziei*, tamże.

133 J.W. Wójcik, *Z problematyki ochrony informacji nie tylko w sytuacjach kryzysowych*, w: R. Częścik i inni: *Zarządzanie kryzysowe w administracji*, Warszawa-Dęblin 2014, s. 400-434.

są przyciągani klienci, albo nowatorskie projekty czy receptury, nad którymi firma pracowała latami. Firma traci wówczas setki tysięcy, a czasami nawet miliony złotych. Takie straty spowodowane wyciekiem informacji wiążą się często z utratą kluczowych klientów, ponieważ konkurencja po prostu ich przejmuje, poprzez propozycje lepszych warunków.

W zapobieganiu działania nieuczciwych pracowników mogą pomagać właściwe procedury. Na każde kluczowe stanowiska, które się wyznacza – w zależności od branży – pisze się specjalne procedury zabezpieczeń, które udaremniają wyciek danych. Ścisła współpraca z firmą trwa do miesiąca i w znacznym stopniu eliminuje niebezpieczeństwo kradzieży tajemnic. Jeżeli wspomniana procedura jest weryfikowana (kontrolowana) co trzy miesiące, czyli jest robiony audyt, to można ujawnić nieprawidłowości[134].

## 6. *Know-how* a tajemnica przedsiębiorstwa

Z zagadnieniem tym związany jest *know-how,* termin pochodzący z jęz. angielskiego (*know* – „wiedzieć", *how* – „jak") określający konkretną wiedzę techniczną z danej dziedziny, umiejętność wykonania lub wyprodukowania czegoś, kompetencję, biegłość.

Definicja przyjęta przez Międzynarodową Izbę Handlową w Paryżu jako *know-how* określa całokształt wiadomości, czyli fachowej wiedzy oraz doświadczeń w zakresie technologii i procesu produkcyjnego dla określonego wyrobu.

W prawie europejskim definicja *know-how* zawarta jest w Rozporządzeniu nr 772/2004 z dnia 7 kwietnia 2004 r. w sprawie stosowania art. 81 ust. 3 Traktatu do kategorii porozumień o transferze technologii[135]. Stanowi ona, iż *know-how* to pakiet nieopatentowanych informacji praktycznych, wynikających z doświadczenia i badań, które są:

1. niejawne, czyli nie są powszechnie znane lub łatwo dostępne,
2. istotne, czyli ważne i użyteczne z punktu widzenia wytwarzania produktów objętych umową oraz
3. zidentyfikowane, czyli opisane w wystarczająco zrozumiały sposób, aby można było sprawdzić, czy spełniają kryteria niejawności i istotności.

Na gruncie polskiego prawa cywilnego umowa *know-how* upoważnia do korzystania z określonych praw podmiotowych. Jedna ze stron (przekazujący, dostawca, udzielający) zobowiązuje się do przekazania drugiej (zamawiającemu, odbiorcy) wiedzy technicznej lub organizacyjnej o charakterze poufnym lub tajnym, bezpośrednio użytecznej w działalności gospodarczej w zakresie określonym w umowie.

Jako cechy charakterystyczne tej umowy wymienia się, że:

1. przedmiotem umowy jest obrót wiedzą techniczną o poufnym charakterze,
2. dotyczy jedynie dóbr niematerialnych,
3. nie przenosi praw majątkowych,
4. w prawie polskim jest to umowa nienazwana – możliwość jej zawarcia wynika z zasady swobody umów według art. 353 k.c.,

134 G. Zawadka, Rozmowa z detektywem Alicją Słowińską, *Firmy oszczędzają na swoim bezpieczeństwie*, „Rzeczpospolita" z 16 października 2014 r.

135 Dz. U. UE L 123 z 27 kwietnia 2004, str. 11.

5. jest umową odpłatną, wzajemną, dwustronnie zobowiązującą.

Dobrami chronionymi umową *know-how* mogą być np.:

- nieopatentowane wynalazki,
- niezarejestrowane wzory użytkowe,
- informacje techniczne dotyczące stosowania patentów lub wzorów użytkowych,
- doświadczenie administracyjne i organizacyjne związane z własnością przemysłową.

W związku z tym umowa ta może stanowić uzupełnienie ochrony przewidzianej prawem na dobrach niematerialnych (własność przemysłowa: patenty, wzory użytkowe, także takie, które nie posiadają zdolności patentowej)[136].

Zatem nazwa *know-how* oznacza poufną, odpowiednio ustaloną wiedzę lub doświadczenie o charakterze technicznym, handlowym, administracyjnym, finansowym lub innego rodzaju, które nadają się do stosowania w działalności danego przedsiębiorstwa albo do wykonywania określonego zawodu.

Podstawową cechą chronionego prawnie *know-how* winna być poufność rozumiana przede wszystkim jako istniejąca u dysponenta informacji wola zachowania stanu tajemnicy wobec osób trzecich. Przesłanka ta nie musi oznaczać wymogu bezwzględnej tajemnicy – wystarczy, by informacja nie była dostępna osobom zainteresowanym w sposób zwykły i dozwolony. Dysponent informacji może zdecydować o jej ujawnieniu (np. wskutek zgłoszenia rozwiązania jako wynalazku). W zakresie, w jakim nastąpiło ujawnienie, dotychczasowy przedmiot know-how może ulec przekształceniu w inne dobro, zazwyczaj zmienia się wówczas podstawa jego ochrony.

Spod ochrony jako *know-how* wyłączone są informacje powszechnie znane oraz takie, których wykorzystywanie byłoby sprzeczne z prawem lub dobrymi obyczajami (np. sposoby oszukiwania klientów), nawet mimo przejawianej przez dysponenta woli zachowania ich poufności[137].

Mimo różnic terminologicznych przyjmuje się, że przepisy art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji, jak i art. 39 TRIPS15 w ten sam sposób definiują pojęcie „tajemnicy przedsiębiorstwa". Warto jednak dodać, że Sąd Najwyższy w wyroku z 28 lutego 2007 r. (sygn. akt V CSK 444/06)17 stwierdził, że: zarówno art. 39 ust. 2 TRIPS, jak i art. 11 ust. 4 z.n.k. nie precyzują dokładnie, jakim konkretnie działaniom ochronnym muszą być poddane tajemnice przedsiębiorstwa (informacje nieujawnione), aby można było traktować je jako poufne. W unormowaniach tych mówi się jedynie, że działania te muszą być „odpowiednie", „rozsądne w danych okolicznościach"[138].

Pomimo niejasności i wielości definicji *know-how* można przyjąć założenie, że know-how poufne, obejmujące informacje zarówno o charakterze technicznym, jak i nietechnicznym, jest tożsame z pojęciem tajemnicy przedsiębiorstwa. Zatem tylko w takim znaczeniu terminy *know-how* i „tajemnica przedsiębiorstwa" mogą być używane zamiennie.

---

136 http://pl.wikipedia.org/wiki/Know-how(22.06.2012)

137 Inne aspekty tego zagadnienia patrz: K. Czub, *Ochrona prawna know-how*, „Rzeczpospolita" z dnia 20 czerwca 2011 r.

138 1. Galińska-Ręczy, *Opinia prawna w sprawie interpretacji pojęcia „tajemnica handlowa"*, *„*Zeszyty Prawnicze*"* nr 4(40) 2013 s. 233.

## 7. Tajemnica kontraktu handlowego

Warto wspomnieć o tajemnicy kontraktu handlowego, gdyż niejednokrotnie w praktyce gospodarczej pojawiają się wątpliwości, które dane przekazywane podczas negocjacji firm objęte są klauzulą poufności. Negocjacje mają miejsce przed zawarciem umowy. Zazwyczaj ustalane są szczegółowe warunki pomiędzy przedsiębiorcami – przyszłymi kontrahentami. Zdarza się, że do umowy nie dochodzi. Wówczas otwarta pozostaje kwestia związana z poufnością udostępnionych w czasie negocjacji danych na temat różnych spraw kontrahentów. Przed podjęciem negocjacji przedsiębiorcy mogą ustalić trochę inne reguły ponoszenia odpowiedzialności za ujawnienie sekretnych informacji. Dobrze jest z góry określić zasady negocjacji. Aby lepiej zabezpieczyć interesy stron, można te zasady zawrzeć je piśmie w specjalnym krótkim porozumieniu. Określi ono zarówno informacje objęte klauzulą poufności, jak i ewentualnie sankcje za ich przekazanie osobom postronnym. Nie jest to prosta sprawa, gdyż w praktyce gospodarczej często pojawiają się wątpliwości, które konkretnie informacje objęte są klauzulą poufności. Odpowiedzialność za naruszenie tajemnicy istotnych i konkretnych informacji może zaistnieć bez względu na to, czy było w tej sprawie pisemne porozumienie. W przypadku naruszenia zakazu udostępniania informacji, strona udostępniająca lub wykorzystująca informacje obowiązana jest do naprawienia wyrządzonej szkody, a nawet do wydania uzyskanych w związku z tym korzyści. Warunkiem jest jednak aby strona, która doznała uszczerbku w wyniku naruszenia umowy, wykazała poniesioną szkodę, jej wysokość oraz udowodnienie związku pomiędzy zaistniałą szkodą a ujawnieniem konkretnej informacji poufnej, (co niejednokrotnie stwarza istotne trudności). Warto wcześniej ustalić przewidywane kary umowne za naruszenie poszczególnych postanowień mających wpływ na tajemnicę negocjacji[139].

Celem opracowania klauzuli o zachowaniu poufności jest zabezpieczenie firmy przed nieuprawnionym ujawnieniem przez drugą stronę umowy informacji dotyczących jej przedmiotu, warunków i wszelkich innych danych.

Warto pamiętać, że okres obowiązywania zastrzeżenia poufności może być dowolnie ustalany przez strony w umowie. Często brane są przy tym pod uwagę terminy przedawnienia roszczeń związanych z konkretną transakcją czy też termin przedawnienia roszczeń za zobowiązania podatkowe. W konsekwencji tego odpowiedzialność za naruszenie umowy o zachowaniu poufności może trwać w okresie jej obowiązywania, a także przez określony czas po jej wygaśnięciu[140].

Niekiedy strony jeszcze przed rozpoczęciem negocjacji bądź podpisaniem umów decydują się na zawarcie umowy o zachowaniu poufności. Zawierane są one w szczególności w sytuacji, gdy strony przekazują sobie informacje stanowiące tajemnicę przedsiębiorstwa, czyli np. określone informacje techniczne, technologiczne i inne dane stanowiące wartość gospodarczą. Bardzo ważne jest, żeby zwrócić uwagę na to, kogo obowiązuje zastrzeżenie poufności. Odnosi się ono nie tylko do stron umowy, ale również do ich pracowników, doradców i wszelkich innych osób, które uzyskają dostęp do zastrzeżonych informacji.

Przy opracowywaniu umowy należy wziąć pod uwagę, że zasadniczo zastrzeżenie takie nie może dotyczyć informacji, które:

139 M.J. Nowak, *Które informacje zachować w tajemnicy*, „Rzeczpospolita" z 4 września 2014 r.

140 M. Ciechomska, *Ile tajemnic w kontraktach*, „Rzeczpospolita" z 4 września 2014 r.

1. muszą być ujawnione zgodnie z obowiązującymi przepisami prawa lub na mocy postanowień sądów;
2. są powszechnie dostępne lub zostały podane do publicznej wiadomości;
3. strona znała je przed ich ujawnieniem w ramach prowadzonych rozmów i może to wykazać.

Przekazywanie drugiej stronie informacji poufnych zawsze dokonywane jest w określonym celu, w zależności od przedmiotu transakcji.

## 8. Tajemnica przedsiębiorstwa a jawność zamówień publicznych

Na uwagę zasługuje również zagadnienie tajemnicy przedsiębiorstwa w problematyce zamówień publicznych. Jawność postępowania jest fundamentalną zasadą zamówień publicznych zgodnie z art. 8 ust. ustawy z dnia 29 stycznia 2004 r. –Prawo zamówień publicznych[141] (dalej pzp). Zarówno jawność czynności zamawiającego związanych z postępowaniem o zamówienie publiczne, jak i wszelkich dokumentów składających się na oferty wykonawców jest istotnym elementem każdego postępowania. Gwarantuje bowiem jego przejrzystość oraz pozwala na urzeczywistnienie zasad uczciwej konkurencji i równości traktowania wykonawców.

Jeżeli zatem postępowanie o udzielenie zamówienia jest jawne, to jednak istnieje możliwość zastrzeżenia przez wykonawcę określonych informacji zawartych w jego ofercie jako tajemnicy przedsiębiorstwa. Składane dokumenty, jak np.: opinie biegłych, oświadczenia, zawiadomienia, wnioski i inne dokumenty i informacje składane przez zamawiającego i wykonawców oraz umowa w sprawie zamówienia publicznego stanowią załączniki do protokołu zgodnie z art. 96 par. 2 pzp, a wszystkie te dokumenty są jawne i udostępnia się je w postępowaniu od jego otwarcia[142].

Jawność i przejrzystość prowadzonego przez zamawiającego postępowania może zostać ograniczona poprzez zastrzeżenie informacji zawartych w ofercie jako tajemnicy przedsiębiorstwa. Jednakże zamawiający nie może bezkrytycznie akceptować zastrzeżenia tajemnicy przedsiębiorstwa, wobec czego zobowiązany jest do przeprowadzenia badania, podczas którego ustala, czy zastrzeżone przez wykonawcę informacje mają charakter tajemnicy przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Nieuprawnione zastrzeżenie informacji w formie tajemnicy przedsiębiorstwa lub zastrzeżenia informacji, które są jawne na podstawie przepisów ustawy (art. 86 ust. 4 pzp) oznacza dla zamawiającego konieczność odtajnienia tych informacji oraz udostępnienia ich innym wykonawcom. Potwierdza to Sąd Najwyższy w uchwale z 21 października 2005 r. (sygn. akt. III CZP 74/05). SN uznał, że następstwem stwierdzenia przez zamawiającego bezskuteczności zastrzeżenia jest wyłączenie zakazu ujawnienia informacji zastrzeżonych.

141 T. j. Dz. U. z 2013 r. poz. 907.

142 A. Gilowska, *Nie każda informacja może być utajniona*, „Rzeczpospolita" z 28 stycznia 2014 r.

## 9. Cyberszpiegostwo gospodarcze jako metoda naruszania tajemnicy przedsiębiorstwa

Dziś nie ma już wątpliwości, że szpiegostwo przemysłowe opanowało cyberprzestrzeń. Taka właśnie konkluzja wynika z raportu Biura Dyrektora Krajowego Kontrwywiadu (*Office of the National Counterintelligence Executive*) dla Kongresu z 2011 roku pt. „Zagraniczni szpiedzy wykradają gospodarcze tajemnice USA w cyberprzestrzeni", obejmującego analizę działań szpiegowskich skierowanych przeciwko amerykańskiej gospodarce w latach 2009-2011. We wspomnianym raporcie podkreśla się, że cyberprzestrzeń z racji swoich unikalnych właściwości jest szczególnie podatna na akty cyberszpiegostwa, na które – co warto podkreślić szczególnie mocno – straciły monopol państwowe służby specjalne. Dzisiaj liczącymi się aktorami w tym procederze są konkurencyjne przedsiębiorstwa, instytuty badawcze, uniwersytety, a także pojedynczy, wynajęci do konkretnego zlecenia, hakerzy[143].

W ramach nieuczciwej konkurencji w działalności gospodarczej rozpoznano kolejne nowe zagrożenie, które określono jako cyberszpiegostwo. W ostatnich latach przedsiębiorcy zastanawiają się, a niektórzy czynią starania jak ujawnić kreta w firmie. Jeżeli firma działająca w określonej branży nagle zaczyna przegrywać przetargi, choć były one organizowane w różnych częściach kraju, a zawsze wygrywa jeden konkurent, którego oferty tylko nieznacznie różniły się od propozycji firmy, można podejrzewać cyberszpiega. Uzasadnione staje się zatem wynajęcie informatyków śledczych. Ci przez kilka tygodni w ukryciu sprawdzą dane z firmowego sprzętu. Nie jest to nowość, a można o tych metodach prasy dowiedzieć się w mediach. Nie trudno bowiem ustalić, czy winę za wyciek dokumentacji ponosi technologia na usługach kogoś (konkurencja zdalnie włamała się do systemu), czy czynnik ludzki (w firmie jest kret, który donosi)[144].

Z raportu PwC pt. „Globalny stan bezpieczeństwa informacji 2014" wynika, że polskie firmy nie są przygotowane do przeciwdziałanie szpiegostwu gospodarczemu, czy nawet wywiadowi gospodarczemu[145]. Czy rzeczywiście nie dostrzegają one zagrożenia w zakresie kradzieży ich tajemnic?

Wśród ekspertów panuje przekonanie, że zazwyczaj niebezpieczeństwo widzą dopiero wtedy, kiedy kradzież już nastąpi, i to w takich rozmiarach, że przedsiębiorstwu zmniejsza się obrót, ponosi ono znaczące straty czy przegrywa masowo przetargi. Każda firma ma wyznaczony próg dopuszczalnych strat i dopóki on nie zostanie przekroczony, zwykle nie podejmuje działań. Kiedy staje się oczywiste, że tajemnice już wyciekły, bo ktoś je wyniósł, straty są kolosalne.

Niezwykle ważną sprawą jest rozpoznanie dotyczące branżeyszczególnie zagrożonych utratą ważnych informacji, a także jakimi metodami to się stało i jakie czynniki temu pomagały. Okazuje się jednak, że w okresie gospodarki konkurencyjnej, praktycznie zagrożona jest każda branża. Nawet jeśli liczących się firm w danym obszarze jest na rynku kilka. Do kradzieży danych dochodzi w tradycyjny sposób, kiedy są

143 http://biznes.interia.pl/wiadomosci/news/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen,1885978,4199?utm_source=paste&utm_medium=paste&utm_campaign=chrome(dostęp 8.11.2017).

144 S. Czubkowska, *Informatyka śledcza, czyli po e-mailu do kłębka*, „Dziennik" z 24-26 września 2010 r.

145 http://www.pwc.pl/pl/publikacje/giss-2014-bezpieczne-informacje-bezpieczna-przyszlosc.jhtml(7.04.2015)

wynoszone przez pracowników – oni są najsłabszym ogniwem. Najbardziej nowoczesnymi metodami są kradzieże w formie cyberprzestępczości.

Mając na względzie złożoną materię omawianego zagadnienia, warto wnieść uwagę ogólną, związaną z możliwościami skutecznego ścigania cyberprzestępczości przez organy ścigania. Zagadnienie realizacji przepisów prawa karnego, a szczególnie rozpoznawania, wykrywania i zapobiegania cyberprzestępczości, wciąż jeszcze stanowi swoiste *novum* w aspektach kryminologicznych i kryminalistycznych, a przede wszystkim w systemie prawa oraz wkracza bardzo głęboko w sferę techniczną działania systemów przetwarzających dane.

Niezbędne staje się wdrożenie kompleksowych zasad nauczania i edukacji w tym zakresie nie tylko studentów, lecz również funkcjonariuszy wszystkich służb policyjnych, prokuratorów i sędziów. Istotna rola przypada intensywnie rozwijającej się kryminalistyce informatycznej, określanej również jako informatyka śledcza.

## 10. Zasady odpowiedzialności z tytułu czynów nieuczciwej konkurencji i ujawnienia tajemnicy przedsiębiorstwa

W razie dokonania czynu nieuczciwej konkurencji, przedsiębiorca, którego interes został zagrożony lub naruszony, może pociągnąć do odpowiedzialności cywilnoprawnej, a także odpowiedzialności karnoprawnej przedsiębiorcę, który tego czynu dokonał.

W pierwszej kolejności należy niezwłocznie poinformować naruszającego własność intelektualną podmiotu, którego prawa zostały naruszone, o formie ich pogwałcenia, konieczności zaniechania naruszenia prawa, a także o prawach przysługujących poszkodowanemu.

Jednocześnie można przedstawić pozostałe roszczenia, których realizacji oczekuje poszkodowany w związku z dokonanym naruszeniem. Dalsze kroki uzależnione będą od reakcji naruszającego na takie wezwanie. Najczęściej dojdzie do próby wyjaśnienia spornej sytuacji, przy czym najlepszym rozwiązaniem jest zawsze ugodowe załatwienie sprawy. Na mocy ugody można ustalić zaprzestanie bezprawnego używania praw poszkodowanego i wysokość satysfakcjonującej gratyfikacji z tytułu uprzedniego ich naruszania. Może się również okazać, że dojdzie do ugody oraz za właściwym wynagrodzeniem udzielona zostanie dotychczasowemu naruszającemu licencja lub nawet przeniesienie prawa.

### 10.1. Odpowiedzialność cywilna za czyny nieuczciwej konkurencji z art. 18-22 uoznk

Zasady odpowiedzialności cywilnej za czyn nieuczciwej konkurencji, którego ofiarą może być nie tylko przedsiębiorca lecz również klient stosować można właściwe środki zaradcze. Przedsiębiorca, którego interes został naruszony, lub chociażby tylko zagrożony, w związku z dokonanym czynem nieuczciwej konkurencji, może żądać od przedsiębiorcy dokonującego czynu nieuczciwej konkurencji roszczeń o charakterze majątkowym, jak i niemajątkowym:

1. zaniechania niedozwolonych działań,
2. usunięcia skutków niedozwolonych działań,

3. złożenia określonego oświadczenia, tj. w odpowiedniej treści i formie,
4. naprawienia wyrządzonej szkody, na zasadach ogólnych,
5. wydania bezpośrednio uzyskanych korzyści, na zasadach ogólnych zawartych w kodeksie cywilnym,
6. zasądzenia odpowiedniej sumy pieniężnej na określony cel społeczny związany ze wspieraniem kultury polskiej lub ochroną dziedzictwa narodowego – jeżeli czyn nieuczciwej konkurencji był zawiniony.

## 10.2. Odpowiedzialność karna za czyny nieuczciwej konkurencji – art. 23-26 uoznk

Art. 23 ust. 1 – *Bezpodstawne ujawnienie tajemnicy przedsiębiorstwa*

*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.*

Tajemnica przedsiębiorstwa wynika z art. 11 ust. 1-4 uoznk. Jej zakres dotyczy: informacji o charakterze technicznym, technologicznym, organizacyjnym, lub innych posiadających wartość gospodarczą. Są to informacje poufne, co oznacza, że nie zostały ujawnione do wiadomości publicznej. Natomiast przedsiębiorca podjął niezbędne działania w celu zachowania poufności takich informacji.

Art. 23 ust. 2 – Szpiegostwo gospodarcze

*Tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej.*

Art. 24 – Bezprawne skopiowanie produktu i wprowadzenie do obrotu

*Kto, za pomocą technicznych środków reprodukcji, kopiuje zewnętrzną postać produktu lub tak skopiowany wprowadza do obrotu, stwarzając tym możliwość wprowadzenia klientów w błąd co do tożsamości producenta lub produktu, czym wyrządza poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Art. 24a – Organizowanie lub kierowanie sprzedażą lawinową

*Kto organizuje system sprzedaży lawinowej lub takim systemem kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.*

Art. 25 ust. 1 – Wprowadzenie klientów w błąd z powodu nieoznaczenia towarów lub usług

*Kto, oznaczając lub wbrew obowiązkowi nie oznaczając towarów albo usług, wprowadza klientów w błąd co do pochodzenia, ilości, jakości, składników, sposobu wykonania, przydatności, możliwości zastosowania, naprawy, konserwacji lub innych istotnych cech towarów lub usług albo nie informuje o ryzyku, jakie wiąże się z korzystaniem z nich, i naraża w ten sposób klientów na szkodę, podlega karze aresztu albo grzywny.*

Art. 25 ust. 2 – Nieuczciwa reklama lub sprzedaż lawinowa lub konsorcyjna

*Tej samej karze podlega, kto dopuszcza się czynu nieuczciwej konkurencji w zakresie reklamy lub sprzedaży, o której mowa w art. 17a.(reklamowanie sprzedaży lawinowej lub konsorcyjnej)*.

Art. 26 ust. 1 – Rozpowszechnianie fałszywych informacji o przedsiębiorstwie, towarach i usługach lub jego kierownictwie

*Kto rozpowszechnia nieprawdziwe lub wprowadzające w błąd wiadomości o przedsiębiorstwie, w szczególności o osobach kierujących przedsiębiorstwem, wytwarzanych towarach, świadczonych usługach lub stosowanych cenach albo o sytuacji gospodarczej lub prawnej przedsiębiorstwa, w celu szkodzenia przedsiębiorcy, podlega karze aresztu albo grzywny.*

Art. 26 ust. 2 – Rozpowszechnianie fałszywych informacji o przedsiębiorstwie towarach i usługach lub jego kierownictwie w celu przysporzenia korzyści majątkowej lub osobistej

*Tej samej karze podlega, kto, w celu przysporzenia korzyści majątkowej lub osobistej sobie, swojemu przedsiębiorstwu lub osobom trzecim, rozpowszechnia nieprawdziwe lub wprowadzające w błąd wiadomości o swoim przedsiębiorstwie lub przedsiębiorcy, w szczególności o osobach kierujących przedsiębiorstwem, wytwarzanych towarach, świadczonych usługach lub stosowanych cenach albo o sytuacji gospodarczej lub prawnej przedsiębiorcy lub przedsiębiorstwa.*

Z powyższych regulacji ustawowych wynika, że karą grzywny, ograniczenia, a nawet pozbawienia wolności do lat dwóch zagrożone jest ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa, jeżeli skutkiem tego ujawnienia jest poważna szkoda. Takiej samej karze podlega ten, kto uzyskawszy bezprawnie taką informację, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej. Takimi samymi karami zagrożone są czyny polegające na kopiowaniu zewnętrznej postaci produktu innego przedsiębiorcy albo wprowadzaniu do obrotu tak podrobionych wyrobów, jeżeli skutkiem tych działań możliwe jest wprowadzenie klientów w błąd co do tożsamości producenta lub produktu i ponownie wyrządza to poważną szkodę przedsiębiorcy, którego produkty są kopiowane.

Warto zwrócić uwagę na karalność pozostałych czynów nieuczciwej konkurencji. *Modus operandi* sprawcy polega na manipulowaniu informacją. Najsurowiej w omawianej ustawie karane jest organizowanie lub kierowanie systemem sprzedaży lawinowej, czyli systemu polegającego na proponowaniu nabywania towarów lub usług poprzez składanie nabywcom tych towarów lub usług obietnicy uzyskania korzyści materialnych w zamian za nakłonienie innych osób do dokonania takich samych transakcji, które to osoby uzyskałyby podobne korzyści materialne wskutek nakłonienia następnych osób do dokonania zakupu. Zgodnie z przepisami, kto organizuje taki system lub nim kieruje, podlega karze pozbawienia wolności od sześciu miesięcy do ośmiu lat.

Karą aresztu lub grzywny zagrożone są także nieuczciwe czyny, które skutkują wprowadzeniem w błąd klientów, narażając ich tym samym na szkodę. Przede wszystkim chodzi tu o nieprawidłowe znakowanie towarów, które może wprowadzać w błąd co do pochodzenia, ilości, jakości, składników, sposobu wykonania, przydatności, możliwości zastosowania, naprawy, konserwacji lub innych istotnych cech towarów lub usług albo nie informuje o ryzyku, jakie wiąże się z korzystaniem z nich.

Wreszcie takiej samej karze (aresztu lub grzywny) może podlegać ten, kto chce wyrządzić szkodę innemu przedsiębiorcy, ośmieszając go lub deprecjonując jakość jego wyrobów albo usług czy też rozpowszechniając o nim nieprawdziwe informacje. Przykładowo może tu chodzić o rozpowszechnianie informacji o rzekomo złej sytuacji finansowej danego przedsiębiorcy, co może narazić go na utratę dotychczasowych kontrahentów lub klientów, albo też rozpowiadanie o zawyżonych cenach oferowanych przez niego produktów, gdy nie jest to prawdą.

Zgodnie z art. 27 uoznk ściganie przestępstw i wykroczeń następuje na wniosek pokrzywdzonego. Z żądaniem ścigania wykroczeń w zakresie reklamy mogą wystąpić także organizacje konsumentów i organizacje przedsiębiorców.

Z danych zawartych w statystyce policyjnej wynika, że organy ścigania w ostatnich latach prowadzą tylko jednostkowe sprawy z art. 23 i 24 uoznk, t.j. o naruszenie tajemnicy przedsiębiorstwa i szpiegostwa gospodarczego, a ich wykrywalność jest bliska 100 procent. Może to zapewne oznaczać, że przedsiębiorcy zgłaszają organom ścigania jedynie te sprawy, w których znają sprawcę[146]. Mankamentem tych danych jest fakt, że zarówno poszczególne artykuły, jak i ich paragrafy dotyczące zupełnie innych czynów z uoink, nie zostały w statystyce policyjnej ujęte oddzielnie. Zatem nie można racjonalnie wnioskować co do zarejestrowanych czynów.

## 11. Inne przepisy prawne ograniczające jawność informacji ze względu na interes publiczny i społeczny

Zgodnie z art. 1 ust. 3 uoznk przepisy przedmiotowej ustawy nie naruszają przepisów innych ustaw takich jak: o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych. Oznacza to, że istnieją również inne możliwości wyłączenia jawności, znajdujące się w wielu przepisach innych ustaw regulujących szereg tajemnic zawodowych. W tym względzie można dokonać różnorodnych klasyfikacji według specyficznych klasyfikacji, a przykładowo:

- ze względu na interes publiczny jawność jest wyłączana w niektórych przepisach, a m.in. w:

1. ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa[147],
2. ustawie z dnia 25 czerwca 1997 r. o świadku koronnym[148],
3. ustawie z dnia 20 czerwca 1985 r. o prokuraturze[149],
4. ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej[150]

- ze względu na interes społeczny jawność jest wyłączana w przepisach:

1. *ustawy* z dnia 12 marca 2004 r. *o pomocy społecznej*[151],
2. ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych[152],
3. ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe[153],
4. ustawy z dnia 21 sierpnia 1997 r. – Prawo o publicznym obrocie papierami wartościowymi[154],
5. ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej[155],
6. ustawy z dnia 29 września 1986 r. – Prawo o aktach stanu cywilnego[156].

146 J.W. Wójcik, *Kryminologia. Współczesne aspekty*, Warszawa 2014, s. 275.
147 Dz. U. Nr 137, poz. 926 ze zm.
148 T. j. Dz. U. z 2007 r. Nr 36, poz. 232 ze zm.
149 T. j. Dz. U. z 2011 r. Nr 270, poz. 1599.
150 Dz. U. z 1995 r. Nr 88, poz. 439 ze zm.
151 Dz. U. 2004 Nr 64 poz. 593.
152 Dz. U. z 2009 Nr 205 poz. 1585
153 Dz. U. z 2002 r. Nr 72, poz. 665 ze zm.
154 Dz. U. z 2005 r. Nr 111, poz. 937 ze zm.
155 Dz. U. Nr 124, poz. 1154 ze zm.
156 Dz. U. z 2004 r. Nr 161, poz. 1688 ze zm.

# Rozdział 3

# Problematyka manipulowania informacją w realu i cyberprzestrzeni

## 1. Prawo i polityka prywatności

Niezwykle istotnym zagadnieniem są prawne, kryminologiczne i kryminalistyczne aspekty manipulowaniem informacjami, kradzieżą informacji i tożsamości oraz związane z tym fałszerstwa informacji i dokumentów. Znaczne możliwości w tym zakresie daje szerokie zastosowanie komputeryzacji. Istnieje nawet przekonanie, że jest to wyższy etap dla realizacji przestępczych planów, także w ramach różnego rodzaju wywiadów.

Dostęp do informacji bez wątpienia został ułatwiony w wyniku rewolucji informatycznej. Powszechna możliwość poszukiwania informacji, a także uzyskanie jej jest bez porównania łatwiejsze niż w XX wieku. Do niedawna jeszcze odbiorca informacji był skazany na pakiety informacyjne, które zostały dlań przygotowane. Aktualnie, w dobie interaktywności źródeł informacji, sami odbiorcy tworzą dla siebie takie pakiety, złożone z kategorii informacji, których uzyskaniem są zainteresowani.

Na tle pozytywnych zjawisk społecznych niejednokrotnie dochodzi do większych czy mniejszych ograniczeń. Niektóre z nich mogą być związane z zapewnieniem bezpieczeństwa państwa i ochroną prywatności jego obywateli. Zagadnienie to regulują właściwe przepisy prawa, ale z informacji z wielu regionów świata wynika, że nasza prywatność jest systematycznie ograniczana. Dotyczy to również dobrodziejstwa Internetu. Podłączenie komputera czy innych urządzeń mobilnych do sieci umożliwia hakerowi ingerowanie w nasze dane osobowe, otrzymanie naszego wizerunku, ustalenie miejsca pobytu, a nawet kontrolę naszego zachowania i działania[157], a zatem ingerencję w życie codzienne, a także kradzież tożsamości i nielegalne wykorzystanie jej w ramach cyberprzestępczości.

Praktyka śledcza wykazuje, że najpoważniejsze naruszenia prawa, w omawianej kwestii, mają miejsce w cyberprzestrzeni. Przestępczość, a szczególnie przestępstwa ekonomiczne istotnie związane są z cyberprzestrzenią, fałszerstwami dokumentów publicznych, poważnymi oszustwami finansowymi i podatkowymi, niejednokrotnie odbywa się to poprzez kradzież i fałszerstwa dokumentów osobistych i posługiwanie się nimi.

157 Przykładem może być również technika samochodowa, która nasycona jest elektroniką do tego stopnia, że najnowsze samochody mogą uczestniczyć w ruchu drogowym bez kierowcy. Natomiast podłączenie samochodu do Internetu, jak wykazały badania w USA, może mieć negatywne skutki dla bezpieczeństwa jazdy.

Szczegółowe regulacje prawa do prywatności zawarte są w przepisach prawa cywilnego. Prywatność nie jest dobrem samoistnym, gdyż nie przewiduje jej art. 23 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny[158], a wynika ona przede wszystkim z innego dobra osobistego jakim jest cześć, czyli np. godność i dobre imię. Przepis ten stanowi, że *dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.*

Jeżeli dobra osobiste zostały zagrożone lub naruszone, to na zasadzie art. 24 k.c. poszkodowany może żądać naprawienia stanu rzeczy, niezależnie od uprawnień wynikających z innych przepisów.

W informatyce, prywatność stanowi pokrewny do anonimowości problem z zakresu bezpieczeństwa teleinformatycznego. Zagadnienie to istotnie wiąże się z bezpieczeństwem narodowym, wewnętrznym i bezpieczeństwem każdego obywatela. Oprócz unormowań prawnych bezpieczeństwo teleinformatyczne, podlega także ochronie metodami technologicznymi, również tak specyficznymi jak np. kryptografia[159].

Istotnym zagadnieniem jest polityka prywatności, a zatem ujawnianie i przetwarzanie danych osobowych, które to zagadnienia są uregulowane ustawowo. W Polsce nadzór nad przetwarzaniem danych osobowych sprawuje Generalny Inspektor Ochrony Danych Osobowych w myśl ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[160].

Przetwarzanie wspomnianych danych, zgodnie z przepisami ustawy, jest dopuszczalne wówczas, gdy dana osoba wyrazi na to zgodę. Ponadto, zgodnie z art. 32 cytowanej ustawy, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, a są zawarte w zbiorach danych, zwłaszcza prawo do uzyskania wyczerpujących informacji w tej kwestii.

Z omawianymi zagadnieniami związana jest polityka prywatności w Internecie. Wikipedia podaje, że jest ona określana jest jako dokument umieszczany na witrynie internetowej w celu poinformowania użytkowników o tym, jakie dane osobowe są o nich zbierane i jak będą wykorzystywane. Tego typu polityka z reguły zawiera informacje na temat:

1. jakie dane są zbierane od użytkowników; mogą to być dane zbierane automatycznie przez serwer lub podawane przez użytkownika podczas np. rejestracji;
2. w jaki sposób są wykorzystywane, a w szczególności czy są przekazywane innym firmom;
3. w jaki sposób właściciel witryny internetowej będzie się kontaktował z użytkownikiem;
4. w jaki sposób można dokonać zmian w danych osobowych użytkownika;
5. w jaki sposób są zabezpieczane dane pobierane od użytkowników[161].

Warto również dodać, że polskie regulacje prawne zgodne są z przepisami UE, a w szczególności z dyrektywą Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.

158 Dz. U. Nr 16, poz. 93 ze zm.

159 http://pl.wikipedia.org/wiki/Prywatno%C5%9B%C4%87(14.05.2014)

160 tj. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.

161 http://pl.wikipedia.org/wiki/Polityka_prywatno%C5%9Bci(14.05.2014).

2002/58/WE w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej[162].

## 2. Rozpoznane formy kradzieży tożsamości

Systematycznie rozpoznawane są nowe metody i dziedziny oszustw, a szczególnie oszustw finansowych. Związane z tym wciąż rozpoznawane są kolejne formy kradzieży tożsamości. Przykładowo, z *raportu Identity Theft Resource Center – ITRC*[163] *opublikowanego 5 stycznia 2011 roku wynika, że* kradzież tożsamości w USA zanotowano w 662 przypadkach w 2010 roku. Autorzy mają świadomość, że jest to tylko fragment rzeczywiście zaistniałych naruszeń prawa w zakresie kradzieży tożsamości. Powszechnie wiadomo, że szereg informacji o naruszeniach prawa nie dociera do wiadomości organów ścigania z uwagi na kryminologiczny problem ciemnej liczby przestępstw[164]. Zatem wiele danych nie jest udokumentowanych, a wiele zaniżonych. Warto jednak posłużyć się kilkoma danymi z cytowanych wyników badań, a mianowicie:

- złośliwe ataki nadal stanowią więcej ujawnionych przypadków niż błąd pracownika. Przykładowo: włamania 17,1% i kradzieże poufnych informacji 15,4%;
- aż w 38,5% z wymienionych kradzieży poufnych informacji nie udało się ustalić *modus operandi* sprawców. Wskazuje to na wyraźny brak rozpoznania zagadnienia zagrożenia tymi problemami;
- kradzież numerów kart kredytowych lub debetowych to 26%, a 62% dotyczyło kradzieży numeru ubezpieczenia społecznego.

Kradzież tożsamości, a ściślej fałszerstwo tożsamości można zdefiniować jako celowe używanie używanie danych osobowych innej osoby, a także adresu zameldowania, numeru PESEL, najczęściej w celu dokonania oszustwa dla osiągnięcia korzyści majątkowej.

Kradzież tożsamości zwana jest także defraudacją tożsamości, gdyż chodzi o podszywanie się pod czyjeś dane, a nie „usunięcie" danych ofiary[165]. Zachodzi zatem zawładnięcie cudzymi danymi osobowymi i bezprawne posługiwanie się nimi. Takie czyny karalne są z właściwych przepisów kodeksu karnego[166], Przykładowo**:** z art. 190a k.k. za kradzież tożsamości. Sprawca może również odpowiadać za fałszerstwo dokumentów, które jest ścigane z art. 270 – 276 k.k., czy z art. 286 k.k. za oszustwo.

Nadal rozpoznawane są czyny polegające na kradzieży tożsamości, które związane są najczęściej z wyłudzeniem: cudzych danych osobowych, kserokopii cudzych dokumentów tożsamości przykładowo dla założenia internetowego rachunku bankowego, zaciągnięcia kredytu, dokonania zakupu na poważną kwotę – na uzyskane dokumenty.

162 Dz. Urz. UE L 201 z 31.7.2002.

163 *The Identity Theft Resource Center(r) (ITRC) is a nationally recognized non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft. Identity Theft Resource Center (r) (ITRC) jest organizacją non-profit ustanowioną w celu wspierania ofiar kradzieży tożsamości w rozwiązywaniu ich spraw i poszerzenie edukacji społeczeństwa i świadomości w rozumieniu kradzieży tożsamości. Visit* .Raporty i statystyki tej organizacji patrz*:* www.idtheftcenter.org. Pozostałe dane: http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2010.shtml (15.07.2012).

164 Szerzej: J.W. Wójcik, *Kryminologia. Współczesne aspekty*, Warszawa 2014, s. 102-132.

165 http://pl.wikipedia.org/wiki/Kradzie%C5%BC_to%C5%BCsamo%C5%9Bci(15.04.2014).

166 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. nr 88, poz. 553 ze zm.).

Cudzymi danymi operują również oszuści przy wyłudzaniu pieniędzy „na wnuczka" czy „na policjanta". Sprawca liczy na łatwowierność i życzliwość potencjalnej ofiary, a także na podawaniu obcemu naszych danych osobowych, a nawet na pozostawianiu obcego w mieszkaniu, informowaniu o dacie mającej nadejść emerytury czy innego przekazu pieniężnego, na zawieraniu „korzystnych" umów z obcymi osobami w mieszkaniu , a nawet na ulicy.

Latem 2013 r. podający się za Adama K. wynajął kawalerkę na warszawskim Mokotowie. Po kilku miesiącach postanowił ją sprzedać. W połowie lutego 2014 r. zamieścił ogłoszenie w popularnym serwisie internetowym. Za cudzą kawalerkę żądał 235 tys. zł. Kobiecie, która zainteresowała się ofertą, obiecał spory rabat. Na dowód, że jest właścicielem lokalu, pokazywał nawet akt notarialny. Klientkę zdziwił jednak fakt, że w portalu, gdzie wystawiono lokal, nie ma zdjęć mieszkania. Postanowiła poszukać ich w innych serwisach. Znalazła jednak przy starym ogłoszeniu anons o wynajmie ale rzeczywistym właścicielem mieszkania okazała się zupełnie inna osoba. Był tam też numer telefonu, pod który kobieta zadzwoniła. Zasadzka na oszusta doprowadziła do zatrzymania w kawalerce w dniu, w którym miał zawrzeć umowę przedwstępną na sprzedaż cudzego mieszkania. Okazało się, że posługiwał się trzema nazwiskami i okumentami tożsamości na różne nazwiska.

Czasami dopiero po śmierci przestępcy wychodzi na jaw, że dokonał kradzieży tożsamości i posługiwał się fałszywymi danymi. Policja olsztyńska ujawniła przypadek Piotra A., który zmarł w 2002 r., a od 1994 r. używał nazwiska Zbigniewa B., którego dowód znalazł na dyskotece. Okazało się, że pod adresem rzekomego zmarłego jest zdrowy właściciel tych danych osobowych. Dopiero po śmierci zaczęto badania kim rzeczywiście był zmarły. W trakcie ekshumacji pobrano DNA i przeprowadzono szereg czynności, które doprowadziły do ustalenia prawdziwych danych osobowych. Policjanci zadali sobie pytanie: dlaczego mężczyzna zmienił tożsamość? Okazało się, że nagrywał i nielegalnie rozprowadzał filmy oraz gry *science fiction*. Zarabiał na tym spore pieniądze, więc chciał ograniczyć ryzyko wpadki.

Policjanci tłumaczą, że im bardziej poszukiwany przestępca, tym lepsze ma dokumenty. Świadczy o tym chociażby sprawa Rafała S. ps. Szkatuła, który przez wiele lat był numerem jeden na policyjnej liście najbardziej poszukiwanych przestępców. Wielokrotnie udawało mu się uniknąć wpadki, bo korzystał z dokumentów wystawionych na inne nazwisko[167].

Charakterystyczna jest beztroska w traktowaniu własnych danych osobowych. Znajduje to powierdzenie w wynikach badań. Z raportu opracowanego przez firmę Fellowes przy współpracy z Biurem Informacji Kredyowej wynika, że aż 57 proc. ankietowanych zadeklarowało, iż nie niszczy wyciągów bankowych czy rachunków w taki sposób, aby odczytanie zawarych w nich danych było niemożliwe. Niemal co piąty jest gotów podać swój PESEL, adres zamieszkania czy nazwisko panieńskie matki tylko po to, by wziąć udział w konkursie internetowym. Ponadto, prawie co trzeci ankietowany nie wie, że w przypadku kradzieży dowodu osobistego należy o tym powiadomić policję[168].

W Polsce brak jest szczegółowych danych, jednakże zagrożenia są realne. Przykładowo, według TVN24 Bis, 5 milionów haseł i loginów do kont pocztowych Gmail

167 J. Bukowska, J. Ćwiek, *Człowiek z ukradzionym nazwiskiem*, „Rzeczpospolita" z 29-30 marca 2014 r.
168 Tamże.

wyciekło do sieci. Skradzione dane pojawiły się na rosyjskim forum Bitcoin Security, znaleziono tam również e-maile użytkowników z Polski[169].

W naszym kraju mamy do czynienia z kradzieżą tożsamości na mniejszą skalę. Ustaleni sprawcy to najczęściej cudzoziemcy z krajów bałkańskich, którzy w Polsce ustalają numery i PIN-y kart, a pieniądze wypłacają w swoich krajach (najczęściej w Rumunii). Przykładowo, w styczniu 2014 r. media polskie podały, że na Podkarpaciu dokonano kradzieży danych z kart płatniczych. Jeden z poszkodowanych stwierdził, że *w przedświątecznej gorączce nawet nie zauważyłem, że z mojego konta ubyło więcej pieniędzy niż powinno. Uświadomił mnie o tym dopiero pracownik mojego banku, który zatelefonował z pytaniem, czy 23 grudnia wypłacałem w Hong Kongu 4 tysiące tamtejszych dolarów, czyli prawie 1600 zł. Oczywiście nie, bo wtedy byłem w kraju. Ktoś mnie okradł.*

## 3. Lekkomyślne dysponowanie własnymi danymi osobowymi

Według danych policji stwierdza się systematyczny wzrost przypadków kradzieży tożsamości, szczególnie gdy chodzi o niespłacone *pożyczki, oszukańczo zaciągnięte w firmach internetowych.* W trakcie postępowania okazuje się, że sprawcy, którymi są najczęściej zorganizowane grupy przestępcze, posługują się cudzymi danymi osobowymi. Wystarczy im imię, nazwisko, numer PESEL *oraz* adres zamieszkania. Sprawcy nie kradną dowodu osobistego, lecz wykorzystują pozyskane dane personalne. Takie dane często sami lekkomyślnie udostępniamy. Zdarza się, że wysyłamy nawet kopie dokumentów, nabierając się np. na fikcyjne oferty pracy, w których rzekomy pracodawca domaga się wraz z CV, także skanu dowodu osobistego. Eksperci finansowi szacują, że takie oszustwa stanowią w granicach 1-3% udzielonych pożyczek przez firmy internetowe. O*znacza to,* że oszustom udało się wyłudzić nawet 60 mln zł.

Oczywiście nie wszyscy właściciele danych osobowych znają obowiązujące przepisy, chronią swoje dane i swoją prywatność. Należy zawsze mieć na uwadze fakt, że może istnieć pewien procent osób, które tych przepisów nie znają, znają ale nie respektują, czy również pewna grupa osób działa lekkomyślnie. Może zdarzyć się również sytuacja, w której tracimy kontrolę nad informacjami o nas i tym, kto je przetwarza. Niejednokrotnie dostajemy, jak by się wydawało, interesujące propozycje, które doprowadzają do tego, że bez zastanowienia dajemy swoje dane osobowe w zamian za rabaty handlowe czy darmowe wejściówki na imprezy. Za wstęp można wówczas zapłacić 50 proc. mniej, jeżeli wyrazimy zgodę przekazania organizatorom swoich danych osobowych.

Inne propozycje dotyczą przekazania danych różnym firmom, choćby w zamian za rabaty czy darmowe usługi. Także podczas niektórych wydarzeń kulturalnych uczestnicy w zamian za informacje o sobie dostają darmowe wejściówki. Analizując obowiązujące przepisy należy stwierdzić, że jest to działanie legalne. Strony, a więc dawca danych osobowych i biorca są stronami umowy, która może być swobodnie przez nie kształtowana. Nielegalne działanie jest wówczas, gdy zachodzi uzależnianie zawarcia takiej umowy od wyrażenia zgody na wykorzystywanie danych osobowych w celach markeingowych. Obserwacja życia społecznego wykazuje, że handel danymi osobo-

169 Szerzej http://www.bankier.pl/wiadomosc/Wyciek-danych-z-5-mln-kont-Gmail-Google-komentuje-7217944.html(12.09.2014)

wymi jest już codziennością. Dobrym przykładem może być żądanie danych w zamian za możliwość założenia darmowego profilu na portalu społecznościowym.

Zasada prawna w omawianej kwestii dotyczy tego, że osoba, która udostępnia swoje dane, musi mieć świadomość, że za informacje o sobie dostanie konkretną usługę. Musi być też poinformowana o tym, przez kogo i w jakim celu będą wykorzystywane jej dane oraz o odbiorcach tych danych.

Zdaniem Wojciecha Wiewiórowskiego, generalnego inspektora ochrony danych osobowych, niejednokrotnie możemy zdziwić się, że nasze dane osobowe są wykorzystywane przy ofertach nowych bądź dodatkowych usług, ubezpieczeń czy pożyczek. Często zastanawiamy się, skąd ktoś ma do nich dostęp. Bywa również tak, że na ich podstawie oraz informacji zebranych z portali społecznościowych, otrzymujemy reklamy produktów, które mogą nas zainteresować. Przekazując swoje dane osobowe w zamian za towary czy usługi, płacimy bardzo cenną walutą: informacjami o sobie, które mogą nam przysporzyć nieprzewidzianych problemów[170]. Powinniśmy bowiem spodziewać się utraty kontroli nad tym, kto przetwarza nasze dane. Wystarczy, że nieopatrznie zgodzimy się, by dane osobowe były przekazywane także innym firmom. Trudno będzie wtedy sprzeciwić się ich przetwarzaniu. Skąd mamy wiedzieć, do ilu firm i do jakich wysłać pismo z naszym protestem?

Dlatego im bardziej skonkretyzowana zgoda odnosząca się do stanu faktycznego, tym większe formalne bezpieczeństwo i nasza świadomość, kto konkretnie dysponuje naszymi danymi i czy komukolwiek będą przekazywane. Natomiast obowiązkiem firmy, która je otrzymała jest obowiązek poinformowania nas skąd są te dane. Trudno jednak ustalić czy ktoś w rzeczywistości takie informacje otrzymał.

Należy zatem mieć na uwadze, że przetwarzanie danych osobowych jest możliwe, a zgoda nie jest wymagana, gdy:

1. osoba, której dane dotyczą, wyrazi na to zgodę. Bywa jednak, że taka zgoda nie jest konieczna,
2. jest to niezbędne do wykorzystania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
3. jest to niezbędne do wykonania umowy, której dana osoba jest stroną. Zgoda na przetworzenie nie jest też wymagana, gdy
4. dane są niezbędne do określonych prawem zadań wykonywanych dla dobra publicznego lub dla wypełnienia prawnie usprawiedliwionych celów.

Administrator danych musi poinformować obywatela nie tylko o celu przetwarzania danych, ale i o swoim adresie oraz pełnej nazwie firmy, która dysponuje danymi. Ponadto konieczne jest poinformowanie o prawie dostępu do tych danych oraz możliwości ich poprawiania.

## 4. Manipulowanie informacjami w cyberprzestrzeni czyli socjotechnika hakera

Okazuje się, że hakerzy potrafią być dobrymi psychologami, a także umiejętnie stosują zasady socjotechniki. Niejednokrotnie przed dokonaniem ataku na wybrany

170 Ł. Kuligowski, *Zamiast pieniędzmi coraz częściej płacimy danymi*, „Rzeczpospolita" z 5 listopada 2014 r.

komputer przeprowadzają rozpoznanie również w formie wywiadu na temat wybranej firmy i jej pracowników. Chodzi przede wszystkim o zdobycie informacji na temat zasobów bazy danych, konfiguracji sieci, haseł użytkowników, innych interesujących zagadnień, a przede wszystkim na temat przydatności (do ich celów) pracowników.

Od początków swojej działalności hakerzy stosowali swego rodzaju chwyty psychologiczne i na przykład:

- wykonanie telefonu do administratora sieci podając się za pracownika firmy i prosząc o zmianę hasła swojego konta;
- podawanie się za pracownika serwisu i pod pretekstem konserwacji sprzętu poszukiwanie haseł (pod klawiaturą, na ekranie itp.);
- wykonanie telefonu do sekretarki firmy i podanie się za bogatego klienta, który chce skontaktować się z prezesem, a następnie zdenerwowanym głosem żądają zmiany hasła „swojego" konta, gdyż zostało zapomniane.

Socjotechniczne umiejętności hakera polegają na takim manipulowaniu pracownikami firmy, którą się interesują, aby skłonić ich do ujawnienia informacji lub przeprowadzenia takich działań (w penetrowanej firmie), by zdobyć informacje, szczególnie poufne, ułatwiające włamanie do systemu informatycznego.

Słynny haker M. Mitnick twierdzi, że: Jeżeli intruz nie ma możliwości uzyskania fizycznego dostępu do sysemu komputerowego lub sieci, będzie próbował manipulować ludźmi w taki sposób, aby coś za niego zrobili. W przypadkach, gdy bezpośredni dostęp do komputera jest konieczny, użycie ofiary jako pośrednika jest nawet lepsze, ponieważ napastnik nie naraża się na ryzyko złapania i aresztowania[171].

## 5. Podstępne wykorzystywanie portali społecznościowych

Analityk informacji, a szczególnie haker-socjotechnik, z zawartych w portalach społecznościowych informacji może uzyskać wiele danych bez posługiwania się podstępem, fałszerstwem czy kradzieżą dokumentów. Wiąże się to z kolejnym zagrożeniem, którym jest wykorzystywanie dość powszechnej mody na portale społecznościowe. Przykładowo miliony Polaków ma konta na Facebooku, który bije wszelkie rekordy, gdyż ma już ponad pół miliarda uczestników[172]. Natomiast dbający o karierę zawodową tworzą profile na: Profeto, GoldenLine czy Linkedln. Zainteresowania specjalistyczne obejmują np.: fotografowanie – Flickr i Plofo, muzykowanie – Last.fm. Blogerzy mają swój Blog.pl i Bloxie, a mikroblogerzy – Blipie i Twister. Nie wszyscy myślą o bezpieczeństwie informacji, gdyż w zasadzie wszyscy (z wyjątkiem 2 proc.) internauci podają dane o swoim życiu prywatnym i zawodowym. Okazuje się bowiem, że dane te nie zawsze są wykorzystywane zgodnie z wolą właściciela. Niejednokrotnie obserwujemy nie tylko naruszenie danych osobowych, lecz również publikację wizerunku i scen, które mogą sprawić ich legalnym posiadaczom wiele kłopotów. Przykładowo, Sebastian, lat 35, jest windykatorem. Przydatne mu są informacje z serwisów społecznościowych, które wykorzystuje w pracy zawodowej. Wyjaśnia, że: *Do windykacji najlepsza jest Nasza-klasa. Założyłem tam fikcyjne konto. Mam 700 ziomali. Ludzie sami mnie zapraszają. Dorzuciłem dla ściemy kilka zdjęć przyrody. Jak*

171 K. Mitnick, W. Simon, *Sztuka podstępu*, Gliwice 2003, s.224.

172 Facebook powstał 4 lutego 2004 r. założony przez Marka Elliota Zuckerberga i jego kolegów, studentów Uniwersytetu Harvarda. Jego twórca jest najmłodszym miliarderem świata.

*przychodzą akta od klientów, wstukuję w Naszą-klasę ich nazwiska*[173]. Te zwierzenia dotyczyły roku 2010, obecnie nasiliły się na Facebooku.

Aktualnie w życiu społecznym i politycznym pełno jest zainteresowanych, którzy potrafią (nie tylko służbowo) podglądać i podsłuchiwać. Jednakże wiele osób dąży do tego aby intensywnie nasilać zainteresowanie swoją osobą. Od dawna wiadomo, że na łamach Facebooka odbywają się swoiste polowania na tożsamość. Wynika z tego, że jeżeli ktoś chce, to dowie się: kim jesteś i gdzie pracujesz, jak mieszkasz i czego słuchasz, kim są twoi znajomi, co pijesz, a także z kim śpisz. Zdobycie tych informacji jest tak proste, że aż trudno uwierzyć[174].

Portale społecznościowe można wykorzystywać jeszcze na inne np. kryminalne sposoby, a przykładowo, wiosną 2010 roku media angielskie szeroko komentowały sprawę 42-letniego więźnia nazwiskiem Colin Gunn, uznawanego za jednego z najgroźniejszych przestępców w Nottingham. Został skazany za dokonywanie napadów rabunkowych, wymuszanie haraczy, handel narkotykami, a także był podejrzany o zabójstwa. Nawet w zakładzie karnym nie zaprzestał swej działalności, gdyż założył profil na Facebooku i zyskał ponad 500 korespondentów. Wkrótce zaczął grozić osobom, na których się zawiódł, żądał haraczu. Także poprzez Facebook wymieniał informacje z członkami swego gangu specjalizującego się w wymuszaniu haraczy i nadal nim kierował.

W literaturze można spotkać opisy zdarzeń, wydawałoby się wprost niewiarygodnych. Jednym z nich jest tzw. facebookowa kradzież. Jej bohaterami stali się rodzice, którzy wyjechali z nastoletnią córką na weekend w góry. Po powrocie z przerażeniem stwierdzili, że zostali okradzeni, a w ich mieszkaniu pozostały tylko gołe ściany. Sprawców nie zdołano wykryć, ale policjant poradził rodzicom, aby uważnie prześledzili konto córki na Facebooku. Okazało się, że córka, typowa zbuntowana nastolatka, miała szczegółowo opisane oraz sfotografowane całe mieszkanie. Ze swoimi znajomymi dzieliła się fotografiami i opisami wszystkich cenniejszych rzeczy w domu. Ponieważ rodzice byli dobrze sytuowani, więc lista dóbr była dość długa. Córka dostała dobrej jakości aparat cyfrowy, który – jak wykazało śledztwo – pozwolił wprawnemu złodziejowi ocenić nawet jakość oraz typ zamków zamontowanych w drzwiach wejściowych. Ponadto, nastolatka dokładnie informowała wszystkich znajomych o ważniejszych wydarzeniach z jej życia, również tych planowanych. Ostatni wpis donosił o wyjeździe w góry, do udziału w którym zmusili ją rodzice[175].

Wciąż jeszcze nie zdajemy sobie sprawy z tego sobie sprawę z faktu, że wiele informacji dostępnych na portalach społecznościowych może doprowadzić do różnego rodzaju kłopotów. Przykładowo, znając tylko imię i nazwisko potencjalnej ofiary oraz ewentualnie nazwę miasta, w którym ona mieszka, można:

- zobaczyć jej zdjęcie lub zdjęcia, a także zdjęcia jej rodziny i znajomych,
- poznać wiek, a na jego podstawie przybliżoną datę urodzenia (rok),
- poznać całe zastępy jej znajomych, przyjaciół i kolegów z pracy, członków rodziny itp.,
- jeśli wypełni swój profil szczegółowo – zyskać dodatkowe informacje o tej osobie i o tym, czym się aktualnie zajmuje, gdzie pracuje lub studiuje,

173 P. Miączyński, T. Grynkiewicz, *Kto nam skradł odciski palców*, "Gazeta Wyborcza – Gazeta na Święto" z dnia 2-3 czerwca 2010 r.

174 Tamże.

175 T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013, s.152, 153.

- poznać dokładny przebieg jej edukacji – szkoły, uczelnie, odbyte kursy,
- poznać numer Gadu-Gadu, Skype'a i telefonu, jeśli takie dane ujawni,
- poznać stan cywilny: po nazwisku, fotografiach lub porównując nazwiska znajomych,
- analizując fotografie i ewentualnie listę znajomych, dowiedzieć się, czy ma i ile dzieci oraz często poznać ich płeć i oszacować wiek,
- jeżeli ktoś publikuje zdjęcia ze ślubu i są to fotografie dobrej jakości (lub na przykład oznaczone geotagiem), to dobry socjotechnik odkryje, gdzie para brała ślub lub gdzie się bawiła,
- szczegółowo porównując nazwiska na liście znajomych, można odkryć powiązania rodzinne – rodzeństwo, kuzynostwo, bliżsi i dalsi krewni i powinowaci,
- porównując szkoły i uczelnie, w których się uczy z jej znajomymi, poznać znajomych z jej konkretnych szkół i uczelni,
- czytając podpisy pod fotografiami, komentarze do nich i do profilu, poznać wiele szczegółów z życia prywatnego ofiary – gdzie spędzała wakacje, w jakich klubach lubi się bawić, jakie preferuje formy spędzania wolnego czasu, jakie ma hobby itp., itd.,
- analizując daty i godziny dodawania kolejnych fotografii i lub udzielania odpowiedzi na komentarze, poznać w jakich porach korzysta z Internetu, czy ma dostęp do niego w pracy, czy może tylko wieczorem lub w nocy[176].

Również analiza danych z mechanizmu „Like" („Lubię to!") z Facebooka, w wyniku analizy przez hakera - socjotechnika, staje się kopalnią informacji, z których wiele powinno być chronionych. Skutki niefrasobliwej działalności, która była powodem wielkiej straty opisuje T. Tejderowski[177].

## 6. Konto i kredyt na „słupa"

*Modus operandi* sprawców oszustw bankowych działających techniką kredytu „na słupa", czyli najczęściej stosowaną typowo polską metodę kradzieży tożsamości, rozpoznano w pierwszej połowie lat 90. ubiegłego wieku. Wówczas popularną metodą działania oszustów stało się zakładanie firm i pobieranie kredytu „na słupa". Świadczą o tym rozpoznane zagrożenia, a także liczne sprawy z praktyki bankowej, śledczej i sądowej[178]. Niektóre banki, mając świadomość zagrożeń niezwłocznie podjęły działania wspólnie z policją w celu wypracowania metod przeciwdziałania[179].

176 Tamże, s. 148-150.

177 Tamże, s. 150.

178 J.W. Wójcik, *Kryminologiczna ocena transakcji w procesie prania pieniędzy*, Warszawa 2001, s. 519 – 572 oraz tego autora: *Pranie pieniędzy.* wyd. cyt., s. 308-336; *Fałszerstwa dokumentów publicznych. Rozpoznawanie i zapobieganie,* Warszawa 2005, s. 203-216.

179 W ramach „grubej kreski" nie dopuszczano myśli o zagrożeniu przestępczością zorganizowaną. Wówczas to nawet zlikwidowano pion do walki z przestępczością gospodarczą w KGP. Racjonalnie w tej mierze wiele inicjatyw przejawiało Biuro Zabezpieczeń Bankowych Centrali Banku Handlowego w Warszawie S.A., w którym już w styczniu 1992 roku powołano Zespół ds. Zapobiegania Przestępstwom na Szkodę Banku. Zespołem tym kierował autor tej książki. Jednym z pierwszych osiągnięć zespołu było opracowanie Programu Identyfikacja, tj. procedury dotyczącej weryfikacji dokumentów tożsamości i identyfikacji klientów posługujących się fałszywymi dokumentami tożsamości. Ponadto, opracowano bankowy program „Poznaj swojego klienta" na przykładzie programu angielskiego. Procedura

Jedna z pierwszych publikacji medialnych na ten temat dotyczyła zatrzymania przez stołeczną policję 28 letniego Marka Ł., który usiłował wyłudzić pieniądze z banku PEKAO S.A. Jego wspólnik zbiegł, ale pozostawił w okienku kasowym dowód osobisty z fikcyjnymi danymi. Okazało się, że czysty blankiet tego dowodu osobistego skradziono w 1994 r. w Bielsku Podlaskim[180].

W 1996 r. wrocławska policja zatrzymała 5 osobową grupę oszustów, którzy wyłudzili z banków 2 mln st. złotych. Sprawcy wykorzystywali bezdomnych, którym wyrabiano fałszywe dokumenty na podstawie których kupowali oni na raty luksusowy sprzęt elektroniczny, drogie meble itp. Dziennikarskie śledztwo przeprowadzone w sklepach wykazało, że sprzedawców nie dziwił ubogi wygląd czy ubiór klienta, który nie wyglądał na osobę, mogącą sobie pozwolić na nabycie drogiego sprzętu[181].

W międzyczasie zmieniono formę dowodu osobistego, który otrzymał dość dobre zabezpieczenia. Jednakże opisany *modus operandi* sprawców jest wciąż aktualny. Świadczy o tym fakt, że wrocławska policja w lutym 2005 r. zatrzymała 6-osobową grupę przestępczą organizatorów przysposabiających bezrobotnych do wyłudzania kredytów bankowych. Role były podzielone: jedni, wyszukiwali właściwych bezrobotnych czy bezdomnych, którym płacono po kilkaset złotych, inni załatwiali fałszywe zaświadczenia o zatrudnieniu i zarobkach, a kolejni specjalnie przygotowani, pilnowali aby wszystko przebiegało właściwie w czasie zawierania umów kredytowych. Oszuści wyłudzali kredyty na zakup sprzętu RTV, AGD i telefonów komórkowych. Uzyskane w ten sposób przedmioty szybko sprzedawali paserom.

Popularności tej metody i braku skutecznych metod zapobiegania dowodzi fakt, że podobne sprawy ujawniono również w Toruniu i innych miastach. W kilku rozpoznanych przypadkach na dokumenty „słupa" otwierano firmę. Po odpowiednim przygotowaniu bezrobotnego czy bezdomnego to właśnie jego „doradcy" wozili firmantów po odpowiednich urzędach, w których załatwiano nieomal od ręki zezwolenia na działalność gospodarczą, zakładano spółki, wyrabiano koncesje itp. [182]

Współdziałanie ze „słupem" jest dość proste szczególnie wówczas, gdy ma on dowód osobisty i meldunek. Jego wynajęcie kosztuje wówczas najczęściej 200-300 zł. Zadaniem słupa było udanie się z organizatorem do sklepu i tam nabycie na raty właściwego sprzętu. Jednakże najpierw organizator dba o proste czynności przygotowawcze, mycie i golenie oraz czyste ubranie, a następnie podrobione zaświadczenie o zarobkach i dokładne instrukcje w sprawie sprzętu, który ma zakupić. Jeśli jednak „słup" nie ma dowodu osobistego, otrzymuje dowód z fikcyjnymi danymi, które musi zapamiętać. Zdarza się, że niezbędna jest wizyta u fotografa, aby dowód osobisty z fikcyjnymi danymi personalnymi, zaopatrzyć jego zdjęciem.

Najrudniejszym i najbardziej ryzykownym momentem w sprzedaży ratalnej jest weryfikacja danych klienta. Zatem dobry organizator prowadzi „szkolenie" wynajętego „słupa" aby nie doszło do wezwania policji. Po załatwieniu formalności „słup" przekazuje zakupiony sprzęt organizatorowi. Jest to moment, w którym następuje za-

ta służyła nie tylko w zakresie przeciwdziałania praniu pieniędzy, lecz również była przydatna w weryfikacji klientów starających się o kredyt. Szerzej: R.A. Small, *„Know Your Customer" Policy* (w) Financial Action Task Force, Money Laundering Symposium, March 2-5, 1993, Warsaw. Aktualnie wspomniana problematyka realizowana jest w bankach przez zespoły *compliance*.

180 A. M., *Nowa metoda oszukiwania banków*, „Rzeczpospolita" z 4 września 1995 r.

181 B. Balicka, *Kloszard kupuje za miliardy*, "Super Express" z dnia 26 listopada 1996 r.

182 I. T. Miecik, *Ośmiornica czy krewetka*, "Polityka" nr 26 z 24 czerwca 2000 r.

płata i rozstanie. Natomiast organizator, zazwyczaj za pół ceny sprzedaje sprzęt paserowi czyli zamawiającemu.

Procedura, znana jako „stadium starania się o kredyt", zawiodła zarówno w bankach, jak i w firmach sprzedających towar, gdyż kredytu udzielano oszustom. Warto przy tym pamiętać, że bank jest instytucją zaufania społecznego posiadającą specjalne procedury, które – jak się okazało – w stosunkowo prosty sposób udaje się pominąć.

W stadium spłaty kredytu nic się nie dzieje oprócz tego, że do banku nie wpływają raty. Zatem bank rozpoczyna działanie windykacyjne: wysyła pierwszy monit, potem kolejny. Gdy monity okazują się nieskuteczne do klienta udaje się windykator. Dowiaduje się on, że kupujący na raty, a więc kredytobiorca od dawna tam nie mieszka lub nigdy tam nie mieszkał. Jest to dla banku wystarczający powód do wysłania do jednostki policji zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa polegającego na wyłudzeniu kredytu, czyli oszustwie kredytowym ściganym z art. 297 k.k.

Podstawową sprawą w tego typu postępowaniu przygotowawczym jest odnalezienie „słupa". Udaje się to jedynie przypadkowo, a i tak nie wróży sukcesu, gdyż organizator nie jest znany „słupowi". Ponadto, „słup" nie ma zakupionego na raty sprzętu. Dochodzenia w tego typu sprawach najczęściej są umarzane z powodu niewykrycia sprawcy, a skutki współdziałania zorganizowanych grup przestępczych ze „słupami" niejednokrotnie okazują się drastyczne[183]. Metoda „na słupa" jest nadal systematycznie stosowana. Według danych KGP świadczą o tym kolejne zatrzymania zorganizowanych grup oszustów, a przykładowo:

W Katowicach zatrzymano dwie kobiety i dwóch mężczyzn, którzy przywieźli „kredytobiorcę" do banku i zlecili mu zawarcie umowy pożyczki. Ustalono, że zorganizowana grupa oszustów wykorzystywała głównie osoby bezdomne lub bezrobotne, na które rejestrowano fikcyjną działalność gospodarczą. W dalszej kolejności oszuści wyrabiali pieczątki oraz zaświadczenia o zatrudnieniu, które miały zapewnić wiarygodność kredytobiorcy.

W Szczecinie zatrzymano 22-letniego mężczyznę, który na podstawie fałszywego zaświadczenia o zatrudnieniu wyłudził z banków ponad 16 tys. zł. Zatrzymania dokonano na gorącym uczynku wypłaty kredytu bankowego uzyskanego na podstawie wniosku kredytowego, do którego załączył on fałszywe zaświadczenie o zatrudnieniu.

Niezwykle interesującym przykładem jest informacja, że poznańska policja poszukuje konwojenta firmy ochroniarskiej, który w lipcu 2015 roku ukradł 8 mln złotych z banku w Swarzędzu pod Poznaniem. Publikowano wizerunek mężczyzny i proszono o pomoc w jego poszukiwaniach. Nie wiadomo nawet kim jest, gdyż zatrudniając się przed rokiem w firmie ochroniarskiej podał fikcyjne dane personalne. Dopiero w 2017 roku zorganizowana grupa została pociągnięta do odpowiedzialności karnej.

183 Nie każdy zdaje sobie sprawę z tego, że być :słupem" oznaczać może nie tylko korzyści, lecz również wielkie niebezpieczeństwo. Okazało się, że na zlecenie łódzkiej „ośmiornicy" zamordowano przynajmniej siedmiu bezdomnych „słupów". Tyle znaleziono ciał. Jeden został śmiertelnie upity, drugiego upojono alkoholem metylowym, kolejnego powieszono, innemu poderżnięto gardło, a inny jeszcze strzelił sobie w prawą skroń, choć był leworęczny.

## 7. *Modus operandi* zorganizowanej grupy „słupów”

W 2010 roku Prokuraura Apelacyjna w Warszawie wszczęła śledztwo w sprawie zorganizowanej grupy przestępczej dokonującej na wielką skalę oszustw finansowych m.in. poprzez kradzież tożsamości, kradzież dokumentów osobistych i fałszowanie dokumentów publicznych. Główna sprawczyni to dotychczas nienotowana przez policję Agnieszka B., lat 36, wykształcenie podstawowe, blondyna, dwucentymetrowe tipsy, w ubiorze błyszczącym od cekinów. To kobieta elokwentna, arogancka, a nawet bezczelna, jak twierdzą jej podwładni tj. kilkunastu werbowników. W grupie działało również ponad 100 słupów, jednakże nigdy nie mieli oni kontaktów z szefową. W kryminalnym dorobku grupa ma pół miliona PLN wyłudzonych kredytów bankowych, za co Agnieszce B. przedstawiono 400 zarzutów prokuratorskich. Natomiast jej najbliższemu współpracownikowi – 150.

Agnieszce B. zarzuty postawiono za wyłudzenia gotówki z banków, kredyty na zakup samochodów, sprzętu AGD i komputerów. W mieszkaniu zatrzymanej odkryto prawdziwe przestępcze archiwum: mnóstwo najróżniejszych dokumentów, a w tym NIP-y firm, bankowe wezwania do zapłaty, druki ZUS. Widniały na nich nazwiska różnych osób. Sprawdzenia i analizy zakwestionowanych dokumentów przy udziale banków potwierdziły, że wskazane osoby dostały kredyty na podstawie zaświadczeń o zarobkach z fikcyjnych firm figurujących na znalezionych u podejrzanej dokumentach. Po sprawdzeniu okazało się, że rzekomi biznesmeni to „słupy”, a ich firmy to wydmuszki powstałe tylko po to aby oszukiwać banki[184].

Podejrzana była profesjonalistką w fałszerstwach i oszustwach. To ona opracowywała *modus operandi* sprawców, osobiście fałszowała dokumenty, podszywała się pod pracodawców i odbierała telefony z banków, które chciały zweryfikować wiarygodność przyszłych kredytobiorców.

Głównym pomocnikiem podejrzanej, który zajmował się poszukiwaniem i angażowaniem zaufanych werbowników, był znany wielokrotny recydywista Roman M. Natomiast werbownicy wyszukiwali osoby, czyli słupy, na które brano kredyty. Kandydatów na słupy wyszukiwano w całym kraju, w noclegowniach czy hotelach pracowniczych. Przechodzili właściwe przygotowanie: golenie, strzyżenie, dostawali ubranie, po czym szli z werbownikiem do banku. Po otrzymaniu pieniędzy dostawali bilety powrotne do rodzinnego miasta i ślad po nich ginął. Nigdy nie poznali organizatorów grupy przestępczej.

Zakładane przez podejrzaną fikcyjne firmy wystawiały „słupom” zaświadczenia o zarobkach, konieczne dla otrzymania kredytu. Wspomniane firmy miały zatem zarówno prawnie nadany NIP, jak i REGON, ale żadnej działalności nie prowadziły. Rozpoznano przynajmniej kilka metod działania tej grupy. Najbardziej brutalne było podszywanie się pod prawdziwe spółki. W praktyce oszuści w Internecie szukali firm działających od lat, z ugruntowaną pozycją. Następnie wynajmowali mieszkanie na siedzibę rzekomej filii takiej firmy, zakładali telefon stacjonarny, gdyż wzbudzał większe zaufanie niż komórkowy. Jednakże jednocześnie wprowadzali kod przekierowujący rozmowy na telefon komórkowy Agnieszki B. Wszystko po to aby pracownicy banku, sprawdzający przyszłego kredyobiorcę, telefonując do firmy z pytaniem, czy osoba ubiegająca się o kredyt jest przez nią zatrudniona, otrzymywali potwierdzenie

184 G. Zawadka, *Mistrzyni wyłudzeń i kamuflażu*, „Rzeczpospolita” z 24-25 maja 2014 r.

o treści: „Oczywiście, pracuje i świetnie zarabia" – jak twierdziła Agnieszka B., podająca się np. za główną księgową firmy. Pieniądze z wyłudzonych kredytów bankowych trafiały zawsze do Agnieszki B., która dzieliła się nimi z werbownikami. Najniżej w tej hierarchii przestępczej byli ci, których określa się mianem słupy. Oni otrzymywali najmniejszą „dolę". Do wyłudzeń wykorzystywano również cudze, najczęściej skradzione dowody osobiste. Skruszeni werbownicy zeznawali, jak jednemu ze „słupów" Agnieszka B. przyklejała wąsy, by wyglądał jak mężczyzna na zdjęciu ze skradzionego dowodu osobistego.

Asortyment wyłudzeń gangu był szeroki – od kredytów bankowych w gotówce, przez kredyty na samochody, sprzęt AGD czy komputerowy. Wyłudzano więc np. laptopy za 5 tys. zł, telewizory, ekspresy do kawy i samochody średniej klasy. Ich łupem padł nawet wart 220 tys. Tir. Wszystko trafiało od razu do pasera. Na jednym „przekręcie" udawało się zyskać 20-30 tys. zł.

Do pierwszych wyłudzeń kredytów pod wodzą Agnieszki B. doszło w 2005 r., ale prawdziwy najlepszy okres działalności to lata 2008-2010. Sprawcy działali sprawnie i umiejętnie zacierali ślady. Jednakże zdaniem prokuratury, ok. 85% wyłudzeń było nieudanych, ale reszta była jednak wysoce opłacalna. Powstaje zatem uzasadnione pytanie: Jak to możliwe, że obowiązuje tyle procedur, a sprawcy długo działali bezkarnie?

Jak twierdzą prowadzący postępowanie, Agnieszka B. była tak sprytna, że z pieniędzy, jakie wyłudził słup, spłacała trzy raty kredytu. Kiedy kolejne już nie wpływały, bank kierował sprawę do windykacji, nie podejrzewając oszustwa. Wówczas komornik, szukając słupa, mógł wysyłać pisma jedynie na fikcyjne adresy. Jeśli bank nawet podejrzewał nadużycie, to sprawa trafiała do prokuratury rejonowej, która mając do wiadomości jednostkowy przypadek, nie była w stanie znaleźć dowodów, że jest to właśnie przestępstwo zorganizowane, czyli jedno z wielu oszustw. Jeśli nawet zatrzymano słupa, nie znał on organizatorów i zazwyczaj tłumaczył się: „Straciłem pracę, dalej spłacać nie mogę".

W ostatnich latach inwestowanie w zakup ziemi jest niezwykle opłacalne. Jednakże nie wszyscy inwestorzy dążą do ujawnienia swoich majątków. W związku z tym niektórzy z nich dokonują transakcji na słupa. Są na ten temat różne dociekania. Przykładowo, media wyrażają przekonanie, że na ziemi szczecińskiej, zakupiona w ten sposób ziemia staje się własnością cudzoziemców.

Interesująca jest skala i różnorodność omawianego zjawiska kradzieży tożsamości, które wykazuje tendencję wzrastającą przy braku radykalnych działań prewencyjnych w ramach procedur bankowych, handlowych, ubezpieczeniowych czy inwestycyjnych. Same banki i liczne inne firmy nie chcą ujawniać, ile razy zostały oszukane. Najczęściej zasłaniają się bezpodstawnie tajemnicą handlową i bankową. Z danych policji i prokuratury wynika, że rośnie w Polsce liczba zarówno różnych form kradzieży tożsamości, jak i wyłudzonych kredytów. Potwierdza się teza, że dochodzenia, w których podejrzanymi są „słupy" są umarzane ze względu na niewykrycie sprawcy. Natomiast według Komisji Nadzoru Finansowego nawet połowy wierzytelności, w tego typu sprawach, nigdy nie udaje się odzyskać[185].

185 J.W. Wójcik, *Oszustwa finansowe, Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008, s. 190-194.

## 8. „Słupy" w SKOK-ach

Przejęcie SKOK-ów pod rygory Komisji Nadzoru Finansowego wkrótce doprowadziło do ujawnienia szeregu nieprawidłowości. Jeżeli afera Amber Gold przyniosła straty 851 mln PLN, to afera SKOK-ów wyliczana jest na 3,2 mld PLN. W kwietniu 2015 roku aresztowano kolejnych czterech, a łącznie 17 współdziałających przestępców m.in. pracowników i członków zarządu SKOK Wołomin, którzy masowo przy udziale „słupów" wyłudzali wysokie kredyty bez właściwych zabezpieczeń.

Z początkiem 2015 roku zarówno Komisja Nadzoru Finansowego, organy ścigania, jak i niektórzy posłowie rozpoczęli wyjaśnianie afery w Spółdzielczych Kasach Oszczędnościowo – Kredytowych, o której wspominano w mediach od kilku lat. Wysoce niepokojące były domniemane kwoty oszustw i strat. Po ujawnieniu faktu bezpodstawnego wyprowadzenia z kraju kilkudziesięciu milionów złotych, które podobno przekazano do rajów podatkowych, nakłanianiu osób bezdomnych i bez pracy do zawierania umów kredytowych na wydawane im fałszywe dokumenty tożsamości, a także przyznaniu przez jednego ze słupów, że był prywatnie przyjmowany w SKOK-u, gdzie jego zdaniem zlecano mu pranie pieniędzy, sprawa stała się niezwykle podejrzana. Trudno bowiem wytłumaczyć procedurę zawierania kredytu przez bezdomnego i terminową spłatę tego kredytu tym bardziej, że „kredytobiorcy" byli werbowani pod budką z piwem. Z tego względu sprawą zainteresowała się Agencja Bezpieczeństwa Wewnętrznego. Natomiast oceniając ujawnione dane prof. Leszek Balcerowicz ocenił, że sprawa SKOK-ów to największa afera w sektorze finansowym[186].

Czterech członków gangu wyłudzającego pożyczki w wołomińskim SKOK-u zatrzymali na terenie Warszawy funkcjonariusze CBŚP. Wśród nich jest jeden z liderów grupy, biznesmen**.** Zatrzymani usłyszeli zarzuty udziału w zorganizowanej grupie przestępczej i dokonywania oszustw. Jan L., posiadający status rezydenta Szwajcarii, miał pośredniczyć w kontaktach przestępczych pomiędzy zarządem SKOK-u a liderami średniego szczebla grupy. Śledztwo w tej sprawie prowadzą policjanci rzeszowskiego Zarządu Centralnego Biura Śledczego Policji oraz Prokuratura Okręgowa w Gorzowie Wlkp. Z dotychczasowych ustaleń wynika, że od 2009 do 2014 r. ze SKOK Wołomin przelano na konta kilkudziesięciu „słupów" nie mniej niż 102 mln zł. gdy skala wyłudzeń w tym SKOK-u wynosi 800 mln zł. Wobec wielu podejrzanych zastosowano środek zapobiegawczy w postaci tymczasowego aresztowania. Szacowane kwoty są jednak znacznie większe, na co wskazują wnioski z analizy dokumentów kolejnych ustalonych pożyczek. Ujawniane są nowe wątki sprawy i powiązania personalne, a sprawa ma nadal charakter rozwojowy.

*Modus operandi* sprawców tej afery jest wyjątkowo prosty, a nawet prymitywny. Trudno zatem uwierzyć, że sprawcy mają powiazania nie tylko biznesowe, lecz również polityczne.

## 9. Rola dokumentu w ochronie tożsamości

W wielu przypadkach różnorodne informacje zostają sformalizowane, a wówczas zawarte są również w dokumentach. Termin „dokument" jest często stosowany w życiu codziennym. Niejednokrotnie nie zwracamy uwagi na jego szeroki zakres zna-

186 http://natemat.pl/64877,w-skok-ach-pierze-sie-brudne-pieniadze-bezdomni-zaciagali-w-nich-kredyty-i-je-splacali(11.07.2015)

czeniowy. *Document* (w jęz. łac.) oznacza wyrażenie i przekaz woli przez konkretną osobę, co wywołuje określone sytuacje faktyczne, będące skutkiem specyficznej czynności, natomiast w uogólnionej definicji to rzeczowe świadectwo jakiegoś zjawiska sporządzone w formie właściwej dla danego czasu i miejsca187.

Do podstawowych dokumentów należą: dokumenty tożsamości jak: dowód osobisty, paszport, książeczka wojskowa, prawo jazdy, legitymacja szkolna, studencka, emeryta / rencisty. Wyróżnia się również dokumenty elektroniczne i dokumenty urzędowe.

Terminologia stosowana w życiu codziennym, a także przez ustawodawcę może budzić poważne wątpliwości. W wielu aktach prawnych brak jest jednolitego nazewnictwa. Mamy zatem do czynienia nie tylko z dokumentami, lecz również z: pismami, pisemną formą czynności prawnych, pismem z datą pewną, papierem wartościowym, pokwitowaniem, oświadczeniem, zaświadczeniem, aktem notarialnym, testamentem i wieloma innymi[188], a także z informacjami zawartymi w dokumentach elektronicznych oraz kartami płatniczymi i bankowymi[189].

Znaczenie terminu dokument, szczególnie w obrocie prawnym i obrocie gospodarczym najczęściej jest doceniane wówczas, gdy ujawniona zostanie jego niewłaściwa forma, treść czy wręcz fałszerstwo dokumentu będącego przedmiotem sporu czy przestępstwa. Niezwykle ważna jest zatem definicja dokumentu zawarta w kodeksie karnym. Art. 115 § 14 k.k. stanowi, że *dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.* Wynika z tego, że kodeks karny nie wprowadza jakiegokolwiek podziału dokumentów, a przykładowo na dokumeny urzędowe i prywatne. Prawidłowość takiego stanu prawnego potwierdza również Uchwała SN z 12 marca 1996 r.[190] Natomiast obowiązujący kodeks postępowania karnego[191] w ogóle nie podaje definicji dokumentu. Jednakże w są wyliczone rodzaje dokumentów, które wolno lub które mogą być odczytywane na rozprawie, posługuje się pojęciem „dokumentu urzędowego" i „dokumentu prywatnego". Zatem art. 393. § 1 k.p.k. wymienia następujące dokumenty urzędowe i prywatne: *protokoły oględzin, przeszukania i zatrzymania rzeczy, opinie biegłych, instytutów, zakładów lub instytucji, dane o karalności, wyniki wywiadu środowiskowego oraz wszelkie dokumenty urzędowe złożone w postępowaniu przygotowawczym lub sądowym albo w innym postępowaniu przewidzianym przez ustawę,* a ponadto: *zawiadomienie o przestępstwie*. Następne to: *wszelkie dokumenty prywatne, powstałe poza postępowaniem karnym i nie dla jego celów, w szczególności oświadczenia, publikacje, listy oraz notatki.*

Aby dany zapis (na papierze) mógł być uznany za dokument, musi zawierać koniecznie 4 elementy:

187 http://pl.wikipedia.org/wiki/Dokument(22.06.2014)

188 Por.: K. Knoppek, *Dokument w procesie cywilnym*, Poznań 1993, s. 13.

189 Karta bankowa to elektroniczny instrument płatniczy wydawany przez bank lub instytucję finansową, stanowiący jedno z narzędzi zdalnego dostępu do pieniędzy zgromadzonych na rachunku bankowym. Natomiast karta płatnicza pozwala na podejmowanie gotówki z bankomatu lub dokonywanie bezgotówkowych płatności za towary i usługi. Jak potwierdzają badania, użytkownicy kart płatniczych są bardziej skorzy do wydawania pieniędzy http://pl.wikipedia.org/wiki/Karta_p%C5%82atnicza(22.06.2014)

190 Prawidłowość takiego stanu prawnego potwierdza również Uchwała SN z 12 marca 1996 r., OSP 1996, s. 7, 8, poz. 144.

191 Ustawa z dnia 6 czerwca 1997 roku (Dz. U. Nr 89, poz. 555 ze zm.)

1. oznaczenie wystawcy,
2. wskazanie miejsca i daty wystawienia dokumentu,
3. oświadczenie woli wystawcy dokumentu oraz
4. podpis wystawcy dokumentu.

Dokumenty urzędowe, zwane również „publicznymi", to dokumenty pochodzące zarówno od:

1. organów i instytucji państwowych czy
2. organów samorządu terytorialnego, a także od
3. osób zaufania publicznego (np. notariuszy).

Niewątpliwie dokumenty są istotną częścią dowodów z dokumentów. Pamiętać również należy, iż kryminalistyczna definicja dokumentu jest znacznie szersza od definicji kodeksowej, czyli karnoprawnej. Jak trafnie stwierdza T. Nowak, niezmiernie ważna jest możliwość analizowania treści dokumentu, która ma szanse wówczas, gdy została ujęta (wyrażona) w odpowiedni sposób (graficznie) i na odpowiednim podłożu (papier, deska, płótno itp.). W odróżnieniu od innych przedmiotów, gdzie głównym punktem zainteresowania organu procesowego może być część graficzna (podrobienie lub przerobienie pisma) lub część materialna (podłoże) – dokument jako przedmiot stanowi wartość dowodową zawsze ze względu na zawartą w nim treść.[192] W związku z tym na pojęcie dokumentu składają się łącznie cztery elementy:

1. treść dokumentu, czyli wypowiedź człowieka jako wyraz myśli ludzkiej,
2. strona graficzna dokumentu, czyli myśl wyrażona w odpowiednich znakach graficznych,
3. podłoże dokumentu, czyli odpowiedni materiał, na którym zawarta jest treść dokumentu,
4. autor dokumentu, czyli podmiot wyrażający swoją myśl[193].

Trudno jest stwierdzić, że nie będzie kolejnych definicji dokumentu albowiem takie przykłady są już z przełomu XX i XXI wieku[194].

Obowiązująca aktualna ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[195]w art. 2 pkt 3 stanowi, że *dokumentem jest każda utrwalona informacja niejawna*. Kolejne definicje dokumentu w tej ustawie zależą od niezbędnych procedur bezpiecznej eksploatacji systemu teleinformatycznego w ramach informacji niejawnych będących przedmiotem regulacji prawnych.

Już w orzecznictwie przedwojennym przyjęto pogląd, że dokumentami, których podrobienie podlega karze, są następujące dowody pisemne:[196]

192 T. Nowak, *Dowód z dokumentu w polskim procesie karnym*, Poznań 1994, s. 23.

193 Tamże.

194 Odmienna była definicja dokumentu według uchylonej ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Art. 2 ust. 5 określał, że*: dokumentem - jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych.*

195 Dz. U. Nr 182, poz. 1228 ze zm.

196 J. Bafia, K. Mioduski, M. Siewierski, *Kodeks karny. Komentarz,* Warszawa 1987, s. 446, 447.

1. pozew albo koperta stwierdzająca datę złożenia na poczcie środka odwoławczego,
2. kwit na otrzymany datek dobroczynny,
3. karta rowerowa na równi z dowodami wszelkiego rodzaju praw, np. polowania, rybołówstwa itp.,
4. bilet kolejowy,
5. książeczka członkowska spółdzielni, zawierająca wpisy dotyczące rozrachunku między członkiem a spółdzielnią,
6. paszport zagraniczny,
7. weksel oraz czek.

Natomiast w orzecznictwie powojennym dość liczne orzeczenia SN rozszerzyły ten zakres przedmiotów na szereg innych dowodów pisemnych. Warto przy tym dodać, że nie jest możliwe określenie indeksu fałszerstw dokumentów. Można jednak sprecyzować pogląd, że wykaz tego typu dokumentów stale się rozszerza.

Zgodnie z art. 3 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych[197] dowód osobisty jest dokumentem stwierdzającym tożsamość osoby oraz poświadczającym obywatelstwo polskie.

Specjalna rola przypada dokumentom elektronicznym (inaczej dokumentom cyfrowym, czy binarnym) w postaci pliku tekstowego, graficznego, muzycznego, filmowego lub mieszanego będącego wynikiem pracy z danym programem komputerowym, dającym się zapisać, a następnie odczytać. Cechy dokumentu umożliwiają potwierdzenie prawdziwości zaistnienia danego wydarzenia, okoliczności, zjawiska oraz cechy pliku. Mogą być więc dowodem w procedurach prawnych.

W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[198]. zawarte są następujące definicje: *dokument elektroniczny - stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych*, oraz: *informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej*. Natomiast w obrocie prawnym, jako dokument elektroniczny traktuje się każdy dokument, który daje się przedstawić w postaci cyfrowej. Dokumenty takie mogą być dowolnie konwertowane i zapisywane na wszelkich nośnikach, pod warunkiem, że można je później odczytać i przywrócić im pierwotną postać. Ten sam dokument elektroniczny może być zapisany w wielu różnych miejscach i na różnych nośnikach jednocześnie[199].

Postępująca powszechna informatyzacja życia publicznego i prywatnego doprowadziła w wielu przypadkach do rezygnacji z dokumentów papierowych na rzecz dokumentów elektronicznych. Mają one pełną wartość prawną gdy zawierają, podane wcześniej, wszystkie 4 elementy dokumentu papierowego. Cechy te zależne są jednak od wyrażenia ich w specyficznej formie od woli wystawcy czy nadawcy.

Samo opracowywanie i wysyłanie dokumentu elektronicznego nie stwarza już większych problemów i nie wymaga specjalizacji, gdyż z tą kwestią zapoznani już są uczniowie szkół podstawowych. Postępuje jednak specjalizacja związana z nieuprawnionym dostępem do informacji zawartych w tego rodzaju dokumentach, ich fałszowaniem i bezprawnym wykorzystywaniem.

197 Dz. U. z 2001 roku, Nr 87, poz. 960 - tekst jednolity).
198 Dz. U. nr 64. poz. 565
199 http://pl.wikipedia.org/wiki/Dokument_elektroniczny(22.06.2014).

## 10. Rodzaje fałszerstw dokumentów ujawnione w praktyce śledczej

Współczesny rozwój stosunków społeczno- gospodarczych oraz prawnych powoduje konieczność posługiwania się wyjątkowo dużą liczbą różnorodnych informacji zawartych zarówno w dokumentach papierowych, jak i elektronicznych, niezbędnych do normalnego funkcjonowania osoby fizycznej, firmy, instytucji, czy przedsiębiorstwa. Dokumenty regulują również stosunki publiczne pomiędzy obywatelem a państwem i stosunki prywatne pomiędzy poszczególnymi ludźmi. W związku z tym wiele rodzajów przestępstw, a szczególnie różnego rodzaju oszustw, łączy się w sposób bezpośredni lub pośredni z fałszerstwem dokumentów. Inaczej można określić, że fałszerstwo dokumentów, bez względu na metodę działania sprawcy, od historycznego już fałszerstwa stempla na dokumencie „na jajko" czy fałszerstwo komputerowe, po działanie w cyberprzestrzeni – zawsze stanowi narzędzie do przygotowania poważnego oszustwa finansowego.

W wielu ujawnianych aferach o charakterze oszustw gospodarczych charakterystyczne jest posługiwanie się cudzymi lub sfałszowanymi dokumentami tożsamości, obrotu finansowego i towarowego. Stanowi to niezbędny element metodyki przestępczego działania. Przedmiotem fałszerstwa najczęściej są: kwity magazynowe, rachunki, pokwitowania, upoważnienia do odbioru towaru, listy dostawców na punktach skupu, metki towarowe, listy płac (z tzw. martwymi duszami), dokumenty finansowe i bankowe, jak: polecenia przelewu i wypłaty, czeki, weksle, znaki pieniężne, stemple bankowe czy pocztowe, datowniki, karty kredytowe, znaczki pocztowe i inne. Specjalną uwagę należy poświęcić fałszerstwom dokumentów tożsamości, a także dokumentów potwierdzających wykształcenie, czy kwalifikacje, tj. świadectw i dyplomów, a także znaków towarowych, leków, kosmetyków i innych[200].

Kryminalistyczne badania wyróżniły cztery podstawowe rodzaje działań fałszerzy dokumentów, a mianowicie:

1. fałszerstwa całościowe, obejmujące wszystkie dokumenty od formularza do danych, jakimi zostaje wypełniony;
2. manipulacje fałszerskie, polegające najczęściej na zmianie fotografii i danych osobowych, głównie w dokumentach tożsamości skradzionych ich właścicielom;
3. fałszerstwa przy wykorzystaniu blankietów i istniejących dokumentów, (np.: wpisywanie fikcyjnych danych do skradzionych blankietów dokumentów tożsamości, a także produkowanie nowych lub kradzież istniejących pieczęci i wykorzystywanie ich do bezprawnego wystawiania dokumentów;
4. fałszerstwa intelektualne, czyli wykorzystanie treści dokumentu autentycznego wystawionego przez uprawniony organ do zawarcia w nim fikcyjnych danych, a więc nazwiska okaziciela dokumentu.

Niezmiernie ważne jest podkreślenie rozpoznanej w kryminalistyce zasady, że kradzież dokumentów osobistych, fałszowanie dokumentów publicznych (tożsamości czy finansowych) lub posługiwanie się cudzymi dokumentami to czynności przygotowawcze przestępców do poważnego oszustwa. Szczególnie niebezpieczne są fałszerstwa intelektualne[201]**.** W ramach czynności przygotowawczych do planowanego

200 Szerzej: J.W. Wójcik, *Fałszerstwa dokumentów publicznych. Rozpoznawanie i zapobieganie*, Warszawa 2005, s. 206-215.

201 Szerzej: Tamże.

oszustwa, przestępcy zaopatrują się w fikcyjne dokumenty tożsamości, niezbędne do planowanego przestępstwa. Odpowiednie zapisy mogą być natomiast poświadczone autentycznymi lub podrobionymi podpisami i stemplami urzędowymi. Uzyskany w ten sposób dowód osobisty, na nazwisko osoby fikcyjnej, ma wszelkie cechy dokumentu autentycznego i może być podstawą do wydania legalnych dokumentów przez instytucje, władze samorządowe czy administracyjne oraz służyć do zawierania umów o charakterze cywilnoprawnym, transakcji handlowych i usługowych. Na podstawie podrobionego dowodu tożsamości lub skradzionego autentycznemu właścicielowi, jak wykazuje praktyka śledcza, uzyskiwane są różnorodne dobra, z których największe szkody może przynieść otwarcie rachunku bankowego.

Przestępcze metody otwierania rachunku bankowego przy pomocy fałszywych dokumentów lub skradzionych autentycznych dokumentów tożsamości i wyrabianie na ich podstawie zezwoleń na prowadzenie działalności gospodarczej, zostały rozpoznane jako stosowane na dużą skalę od przełomu lat 80. i 90. XX wieku. Były to początki gospodarki rynkowej i konkurencyjnej. Szereg osób postanowiło wykorzystać ten okres do wzbogacenia się, a klimat towarzyszący ustawie z dnia 23 grudnia 1988 r. o działalności gospodarczej[202], sprzyjał pewnemu rozluźnieniu. Masowo rejestrowano działalność gospodarczą i nikt jeszcze tak naprawdę nie zdawał sobie sprawy ze skali rodzących się zagrożeń. Natomiast stosowanie metody na „słupa", czyli pozyskanie do współpracy, za drobnym wynagrodzeniem, osoby bezdomnej lub bezrobotnej rozpoznano na większą skalę w pierwszej połowie lat 90., lecz jeszcze przed tzw. aferą określaną jako „łódzka ośmiornica". W tym okresie tylko niektóre banki stosowały wówczas odpowiednie procedury bezpieczeństwa w zakresie identyfikacji tożsamości klienta. Najbardziej szkodliwy był brak procedury kredytowej. Ku przestrodze warto przypomnieć sposób działania zorganizowanych oszustów, którzy systematycznie wykorzystują opisany *modus operandi* sprawcy również współcześnie. Okazuje się, że w dość prosty sposób, w ramach obowiązujących procedur bankowych potrafią otworzyć konto, a następnie oszukać bank[203]. Pierwszym i podstawowym krokiem jest pozyskanie dokumentu tożsamości, a zatem oszust:

1. kradnie dowód osobisty, pozyskuje „słupa", który posługuje się tym dowodem,
2. ewentualnie zleca wyrobienie dowodu osobistego na fikcyjne nazwisko – co stanowi już istotną trudność, lecz wciąż jest możliwe. Posługuje się tym dowodem lub wręcza go „słupowi",
3. korzystając z dowodu osobistego jak wyżej wyrabia zezwolenie na działalność gospodarczą i jej faktycznie nie prowadzi,
4. uzyskuje REGON, tj. statystyczny numer identyfikacyjny pozwalający na prowadzenie handlu zagranicznego,
5. otrzymuje numer identyfikacji podatkowej – NIP,[204]
6. otwiera rachunek w banku i uzyskuje kartę płatniczą,
7. dokonuje wpłat na rachunek, by pozyskać zaufanie banku. Może także powodować

202 Dz. U. 1988 nr 41 poz. 324.

203 Szerzej: J.W. Wójcik, *Fałszerstwa dokumentów publicznych. Rozpoznawanie i zapobieganie*, Warszawa 2005.

204 Punkty 2, 3 i 4 mogą zatem stanowić fałszerstwo intelektualne, gdyż urzędy wydające te dokumenty nie posiadają innej procedury identyfikacyjnej klienta, niż okazanie dowodu osobistego i osobiste stawiennictwo oraz wniesienie odpowiedniej opłaty.

sztuczny ruch pieniądza, czyli operując najczęściej tą samą kwotą wpłaca i wypłaca, przelewając ją kilkakrotnie na inne swoje, niejednokrotnie fikcyjne firmy lub rachunki bankowe;

8. uzyskuje kredyt, gwarancję bankową lub inną formę płatności odroczonych, sprzedaż ratalną, leasing czy akredytywę.
9. w przypadku wydania karty płatniczej przestępca otrzymuje zarówno autentyczną kartę, jak i numer PIN. Zatem tylko od jego przedsiębiorczości zależą kwoty, które udało mu się wypłacić.

Dostrzec należy czynniki, które umożliwiały opisany stan rzeczy. Wszystkie nieprawidłowości miały bowiem związek z brakiem właściwych procedur sprawdzających we właściwych urzędach. Wystarczy bowiem osobiste stawiennictwo, przedstawienie dokumentów, które nie podlegają identyfikacji i wniesienie właściwej opłaty – oto zasady tej „procedury". W efekcie następowało wyłudzenie poważnych kwot przez osoby fikcyjne lub towarów na duże sumy z przedsiębiorstw, które nie zdołały zidentyfikować tożsamości lub bezpośrednio zaufały swoim partnerom transakcyjnym. Gdy mijał termin spłaty długu bank, firma leasingowa czy przedsiębiorstwo, poszukiwało właściciela skradzionego dowodu osobistego, a czasami tylko osoby autentycznej, przykładowo słupa, który nie posiada możliwości spłaty długu, albo osoby fikcyjnej. Poszukiwanie osoby fikcyjnej, jak powszechnie wiadomo, skazane jest na niepowodzenie. Tylko przypadek może spowodować, że nastąpi ustalenie osoby, która posługiwała się dokumentami wystawionymi na fikcyjne dane personalne

Łamiąc obowiązujące przepisy o tajemnicy bankowej i ochronie danych osobowych sprawcy potrafią w wyjątkowo sprawnej i profesjonalnej formie dojść do perfekcji w zakresie obserwacji lub dostępu do rachunków klientów i dokumentów bankowych, a także fizycznego czy elektronicznego podglądu wykazów i zestawień bankowych. Jeżeli ktoś ma możliwość takich działań, to nie sprawi mu jakichkolwiek trudności wprowadzenie do banku brudnych pieniędzy, wyprowadzenie nienależnego kredytu, czy posłużenia się danymi z cudzej karty płatniczej. Uzasadniona jest zatem teza, że fałszerstwa dokumentów są pospolitymi przestępstwami „satelitarnymi", nieodłącznie towarzyszącymi współczesnej zorganizowanej przestępczości ekonomiczno-finansowej, a przede wszystkim oszustwom i praniu pieniędzy, które jest najbardziej wyrafinowanym oszustwem finansowym.

Teza ta zasługuje nie tylko na uwagę, lecz także na propagowanie w ramach działalności profilaktycznej. W tego typu przestępstwach finansowych dokument jest najważniejszym narzędziem (środkiem popełnienia) przestępstwa. Jak się wydaje nieograniczony jest indeks obszarów, celów i przestępczego wykorzystywania dokumentów, a przykładem mogą być: przestępstwa przeciwko środowisku naturalnemu, przestępstwa związane z narkotykami, terroryzm, wszelkiego rodzaju oszustwa finansowe, a szczególnie kredytowe, przestępczość przeciwko kartom płatniczym, kredytowym oraz przestępczość z użyciem broni palnej. Ponadto, podrobione dokumenty tożsamości mogą być wykorzystane do: przemytu i handlu żywym towarem; nielegalnej imigracji; prania pieniędzy i finansowania terroryzmu; pracy na czarno; wielu innych przestępstw związanych z identyfikacją tożsamości klienta.

Zastanawiająca jest obszerność tego indeksu i formy zjawiskowe działania fałszerzy. Oczywiste staje się twierdzenie, że przestępcy zorganizowani wytworzyli spe-

cyficzny rynek dokumentów służących do ułatwienia inicjacji wszelkiej działalności przestępczej, bądź jej kontynuowania. Warto zastanowić się nad spektrum możliwości przestępnych, jakie daje posługiwanie się fałszywymi dokumentami, chociaż powszechnie wiadomo, że dokumenty identyfikacyjne spełniają ważną rolę społeczno-prawną, np. przy otwieraniu rachunków bankowych, zawieraniu umowy ubezpieczenia, transakcjach kupna i sprzedaży, kontroli policyjnej itp.

Profesjonaliści z organów ścigania słusznie uważają, że właściwe zabezpieczenie dokumentów tożsamości jest ważnym elementem prewencji w zakresie bezpieczeństwa wewnętrznego tym bardziej, że zakres działania zorganizowanych przestępców gospodarczych jest nieograniczony.

Od dawna wiadomo również, że przestępcy wykorzystują do swoich celów profesjonalistów z zakresu: księgowości, radców prawnych i innych prawników, pracowników biur rachunkowych, analityków i ekspertów z zakresu różnych dziedzin.

Nasilające się w ostatnich latach oszustwa tzw. vatowskie (od handlu pustymi fakturami sztucznie podwyższającymi koszty po skomplikowane międzynarodowe struktury fikcyjne rzekomo handlujące różnymi drogimi towarami), handel złomem, prętami stalowymi, oszustwa celne i akcyzowe (papierosy, alkohole, benzyna i ropa), oszustwo polegające na zakładaniu firm, w których z dużych zysków, a także przy udziale firm „słupów", nie odprowadza się podatków[205]. Niejednokrotnie następuje to również po zasięgnięciu opinii u doradcy podatkowego, który nie zawsze ma jasność, że ma do czynienia z brudnymi interesami[206].

Wagę problemu manipulacji fałszerzy i oszustów wszelkiego typu dokumentami oraz związanymi z tym zagrożeniami dostrzec można dopiero po głębszej i kompleksowej analizie, a szczególnie gdy występują poważne straty przedsiębiorstwa czy instytucji finansowej. Wiadomo, że dobrze w tym względzie służą osiągnięcia nauki, to jednak środki na badania w tym zakresie są ograniczone. Istotne są również osiągnięcia w tym względzie europejskiej praktyki śledczej. Warto również zauważyć, co charakterystyczne jest na podstawie badań ekspertów z zakresu kryminalistyki, a także praktyków z organów ścigania, że powszechne jest obecnie takie działanie przestępców, które polega na angażowaniu profesjonalistów i wykorzystywanie dostępu do najnowszych technologii, które umożliwiają podrabianie wszelkich dokumentów i znaków pieniężnych.

Nasilające się rozmiary kradzieży tożsamości i fałszerstw dokumentów publicznych stanowią poważne zagrożenia. Dotyczy to w szczególności dokumentów tożsamości i dokumentów bankowych czy transakcyjnych, które mogą służyć dokonaniu

205 Rozpoznane w ostatnich latach społeczno-prawne aspekty oszustw podatkowych polegają najczęściej na takim działaniu, które przewiduje budowę łańcucha sprzedaży. W pewnym momencie jedno z ogniw znika bez rozliczenia się z urzędem skarbowym. Natomiast skutki ekonomiczne zdaniem ekspertów związane są ze znacznym spadkiem dochodów z podatku VAT, który wynosi ok. 38-58 mld. PLN rocznie mniej niż powinno wpłynąć do Skarbu Państwa. Przykładem takich ustaleń mogą być przeprowadzone w I kwartale 2014 r. kontrole skarbowe w 1400 przedsiębiorstwach, a w ich wyniku wykryto wyłudzenia podatku VAT na 2 mld PLN. Stanowi to wzrost o 400 mln PLN do analogicznego okresu w 2013 r. co świadczy o istotnym wzroście tego rodzaju oszustw. Eksperci twierdzą, że rozpoznawaniu tej przestępczości nie zawsze sprzyjają przepisy prawa. Wiadomo także, iż jeśli są one bardziej skomplikowane tym lepiej orientują się w nich oszuści i uzyskują z tego przestępcze profity. Praktyka śledcza wykazuje, że współczesne przestępstwa ekonomiczne istotnie są związane z cyberprzestrzenią, kradzieżą tożsamości, fałszerstwami dokumentów publicznych i posługiwania się cudzymi dokumentami.

206 P. Rochwicz, *Przestępcy coraz częściej pukają do drzwi doradców*, „Rzeczpospolita" z 10-11.05.2014 r.

oszustwa finansowego. Ta prawidłowość w metodyce działania sprawców jest już powszechnie znana, a jej celem są przede wszystkim: oszustwa kapitałowe, np.: kredytowe, giełdowe, ubezpieczeniowe, skarbowe, a także pranie pieniędzy. Powodują one największe straty[207].

Wnikliwe badanie naruszeń prawa związanego z czynnościami bankowymi czy transakcyjnymi wskazuje na bardzo szeroki ich zakres. Obok prawa bankowego naruszane jest przede wszystkim: prawo cywilne, czekowe, wekslowe, dewizowe, ubezpieczeniowe, upadłościowe, ustawa o księgach wieczystych i hipotece oraz prawo karne.

Zorganizowane grupy przestępcze najczęściej wykorzystują następujące fałszywe, cudze i podrabiane dokumenty takie jak:

1. dokumenty tożsamości (dowody osobiste, karty pobytu, paszporty, prawa jazdy),
2. dyplomy ukończenia szkól i uczelni różnych typów oraz świadectwa uzyskania kwalifikacji zawodowych,
3. dokumenty związane z posiadaniem lub obrotem pojazdami (dowody rejestracyjne, dowody odpraw celnych, dowody ubezpieczenia),
4. dokumenty zakupu i obrotu towarami (faktury zakupu, świadectwa pochodzenia towaru, listy przewozowe, dokumenty transportu międzynarodowego, mienia przesiedleńczego),
5. różnorodne karty bankowe,
6. inne, w zależności od potrzeb rynku, kategorii przestępstwa, a przykładowo bilety komunikacji miejskiej, czy urządzenia do ich doładowywania.

Zagubienie lub nieostrożne użytkowanie aktualnych dokumentów tożsamości może spowodować nielegalne ich wykorzystanie przez osoby nieuprawnione. Wśród takich działań w ostatnich latach zarówno w polskiej, jak i w międzynarodowej praktyce śledczej rozpoznano szereg przypadków przestępczego wykorzystania cudzych lub fałszywych dowodów tożsamości, a przykładowo:

1. zarejestrowanie i prowadzenie działalności gospodarczej, czyli założenie fikcyjnej firmy (na tej podstawie uzyskiwano wpis do ewidencji działalności gospodarczej, który jest wówczas autentyczny) i umożliwienie dokonywania transakcji finansowych;
2. założenie osobistego konta bankowego i podpisanie umowy na zaciągnięcie pożyczki czy kredytu bankowego;
3. wyrobienie innych dokumentów, np. paszportu, prawa jazdy, karty płatniczej;
4. wyłudzenia towarów na podstawie reklamy w mediach a szczególnie w Internecie;
5. wykonywanie usług bez wymaganego zezwolenia lub z zezwoleniem, ale wystawionym na cudze lub fikcyjne nazwisko;
6. wyłudzanie różnorodnych poświadczeń;
7. uzyskanie pożyczki od łatwowiernych ludzi;
8. popełnienie bigamii;
9. wyłudzanie przy ratalnym systemie sprzedaży jak np.: wyłudzenie towarów, usług, maszyn i urządzeń na szkodę producentów i hurtowników oraz obciążanie kosztami;

207 Szerzej: J.W. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008.

10. tworzenie wysokiego debetu na koncie;
11. legitymowanie się cudzym lub fałszywym dowodem w przypadkach kontroli (np. sprawdzanie tożsamości przez policję, czy przy braku biletu w środkach komunikacji);
12. korzystanie z usług hotelowych i innych płatnych usług bez uregulowania rachunku;
13. korzystanie z usług biur podróży;
14. rejestrowanie się jako bezrobotny;
15. zatrudnianie się u pracodawcy, a następnie okradanie pracodawcy;
16. wypożyczenie i kradzież samochodu;
17. wypożyczenie różnorodnego sprzętu;
18. podpisanie umowy na usługi telefoniczne;
19. wypożyczenie i kradzież cennych książek z bibliotek;
20. zameldowanie w danej miejscowości (np. jako obcokrajowca do pracy);
21. wynajem lokalu i nieuregulowanie należności (czynszu, opłat za telefon itp.);
22. podjęcie cudzego depozytu ze skrytki depozytowej w banku.

Opisany proceder dotyka coraz częściej zarówno osoby prywatne, jak różnego rodzaju przedsiębiorców a w tym banki, a także wypożyczalnie sprzętu, biura obrotu nieruchomościami, firmy leasingowe, pośredników kredytowych itd.[208]

Obszerna w tej mierze praktyka śledcza wykazuje, że skradzione czy sfałszowane dokumenty tożsamości służyły najczęściej do:

1. wyłudzenia pieniędzy na szkodę instytucji obrotu gotówkowego (kredyty, oszczędności, karty kredytowe),
2. wyłudzenia towarów w systemach sprzedaży ratalnej, a także od producentów i hurtowników, przy wykorzystaniu sfałszowanych upoważnień do odbioru,
3. czerpania korzyści majątkowych z nielegalnego przerzutu osób przez granicę państwa,
4. egalizowania obrotu skradzionymi pojazdami, poprzez ich fikcyjną rejestrację i sprzedaż przez „słupy" oraz do rejestracji skradzionych samochodów (w powiązaniu z innymi dokumentami) przed ich sprzedażą,
5. założenia firmy, która prowadzić mogła:
   a. działalność w sferze wyłudzeń towarów i kredytów,
   b. zajmować się przemytem,
   c. legalizować wprowadzone na rynek wyłudzone lub przemycone towary,
   d. dokonywać tzw. pustych obrotów związanych z wyłudzeniem zwrotu podatku VAT,
   e. przeprowadzać fikcyjne operacje związane z praniem pieniędzy,
6. ukrywania się krajowych lub obcych przestępców,

208 Omawiany problem jest na tyle ważny, że przykładowo codziennie notuje się w kraju kilkadziesiąt przypadków różnych prób podobnego działania, które są skutecznie blokowane. Natomiast dzięki Systemowi Dokumenty Zastrzeżone w samym sektorze bankowym, w 2009 roku, udało się powstrzymać blisko 10.000 prób wyłudzeń kredytów na łączną kwotę 311 milionów złotych. Natomiast średnio tygodniowy przyrost zastrzeżonych dokumentów wynosi prawie 4.000 sztuk.

7. stworzenia pozorów legalności przy zatrudnianiu cudzoziemca,
8. legalizowania pobytu nielegalnych emigrantów.
9. uszczuplanie należności celnych i podatkowych Skarbu Państwa, poprzez fałszowanie faktur zakupu towarów i zaniżanie rzeczywistej ich wartości,
10. ukrywanie rozmiarów finansowych prowadzonej działalności gospodarczej w handlu międzynarodowym,
11. różnorodne oszustwa bankowe, ubezpieczeniowe, podatkowe i celne.

W praktyce śledczej znany jest przypadek ujawniony przez jeden z urzędów skarbowych w Białymstoku. Prowadzący działalność gospodarczą obywatel został wezwany do wyjaśnienia pewnych nieścisłości. Okazało się, że nie prowadzi on działalności gospodarczej, a dowód osobisty został mu skradziony półtora roku wcześniej. Nie zdołano ustalić, kto dokładnie prowadził działalność gospodarczą na cudze dokumenty, a także jak zdołał skutecznie wyczerpać procedurę związaną z jej rejestracją i jakie profity czerpał z tego procederu.

Rozpoznane społeczne i ekonomiczne skutki posługiwania się cudzymi i fałszywymi dokumentami wykazują, że w zdobyciu cudzych danych czy kradzieży tożsamości wykorzystywanych jest wiele środków, a dominującym staje się cyberprzestrzeń. Wspomniane czynniki ułatwiają przede wszystkim:

1. rozwój zorganizowanej przestępczości ekonomicznej i wzrost powodowanych przez nią strat;
2. wzrost kosztów przeciwdziałania tego rodzaju przestępczości, w której cudze lub sfałszowane dokumenty są środkiem do popełnienia lub ukrycia innego przestępstwa;
3. poszukiwanie nowych technik zabezpieczeń dokumentów i wzrost kosztów produkcji w celu zabezpieczeń przed fałszerstwami i oszustwami[209].

209 Szerzej na temat konsekwencji i skutków przestępczości patrz: J.W. Wójcik, *Kryminologia. Współczesne aspekty*, Warszawa 2014, s. 322-359.

# Rozdział 4

# Rozpoznawcze znaczenie wywiadu gospodarczego

*Podglądaj jak to robią inni – to nie tylko hasło konkurencji, to również podstawowa zasada przetrwania z punktu widzenia nauki organizacji i zarządzania, często stosowana nie tylko przez wywiad gospodarczy.*

## 1. Geneza i rozwój wywiadu gospodarczego

W aktualnej sytuacji społecznej i ekonomicznej a także prawnej, nie ma żadnych przesłanek, aby sądzić, że eksplozja informacji, jakiej jesteśmy świadkami, ulegnie zahamowaniu. Nie oznacza to jednak, że będziemy coraz lepiej poinformowani. W rzeczywistości bowiem możemy obserwować zwiększającą się liczbę kanałów informacyjnych i nasilenie szumu informacyjnego.

Warto mieć świadomość, że wzrastająca przestępczość gospodarcza, a szczególnie zorganizowane oszustwa finansowe wymagają zastosowania nowych i bardziej skutecznych instrumentów przeciwdziałania. Nowym narzędziem w tej kwestii może być właśnie wywiad i kontrwywiad gospodarczy.

Zastanawiając się zarówno nad rodowodem, jak i skutkami funkcjonowania wywiadu gospodarczego widzimy, że może on być postrzegany zarówno jako ciemna siła naszej cywilizacji, jak i siła napędowa konkurencji w wielu dziedzinach gospodarki. Dotykamy bowiem niezwykle ważnego zagadnienia, któremu zbyt mało miejsca poświęca się w literaturze przedmiotu. Aktualne analizy nie dają wyraźnej wskazówki: czy należy z nim walczyć, czy może stosować skutecznie dla realizacji własnego rozwoju i rozpoznanych potrzeb?

Zwięzła odpowiedź może brzmieć następująco: z prawnego punktu widzenia walczyć należy ze szpiegostwem gospodarczym, natomiast z ekonomicznego i etycznego punktu widzenia podchodzić racjonalnie do zagadnień wywiadu gospodarczego.

Jeżeli już zdecydujemy się na zainteresowanie wywiadem gospodarczym, a walkę ze szpiegostwem gospodarczym, należy je rozpoznać, to znaczy uważnie spojrzeć na te dziedziny, które obejmują wszystko to, co przejawia się jako ułomne, niesprawiedliwe, a nawet karalne, ponieważ ich istnienie w pewnych okolicznościach jest nie tylko niezbędne, ale i usprawiedliwione; szczególnie w przypadkach związanych z wywiadem wojskowym i politycznym, gdy celem jest bezpieczeństwo państwa i jego obywateli. Działalność polegająca na uzyskiwaniu informacji naukowych, technicznych i ekonomicznych, może przynieść korzyści polityczne bądź ekonomiczne. Może także prowadzić do:

- osiągnięcia różnorodnych korzyści przez osoby fizyczne, bądź podmioty gospodarcze;

- wzmocnienia polityki zagranicznej kraju;
- zwiększenia potencjału ekonomicznego, militarnego i obronnego kraju.

Problemem, który nurtuje specjalistów, czyli analityków i ekspertów jest wykrywalność przestępstw z zakresu szpiegostwa gospodarczego. Ich upublicznienie zwykle ma charakter statystyczny, podanie szczegółów jest często sprzeczne z interesami firmy, bowiem rozgłos o zaistniałych szkodach może dodatkowo nadwyrężyć opinię firmy. Nikt nie ma orientacji, jak wielka jest ciemna liczba przestępstw dotyczących ujawnienia tajemnicy przedsiębiorstwa i szpiegostwa gospodarczego, m.in. dlatego, że wciąż jeszcze nie uważa się tego za istotny problem kryminologiczny czy kryminalistyczny, a także ekonomiczny. Traktuje się to zagadnienie przede wszystkim jako problem polityczny.

Szpiegostwo gospodarcze różni się od kradzieży wartości materialnych czy oszustwa. Zazwyczaj straty są często przez dłuższy okres niedostrzegane, gdyż kradzież informacji nie powoduje przemieszczenia dokumentu, czy innego przedmiotu, który np. może być sfotografowany czy skopiowany. Trudno zatem rozpoznać ślady pozostawione przez intruza i zwykle upływa długi okres czasu, nim poszkodowana instytucja dowie się o szkodzie. Natomiast firma, która nielegalnie pozyskała korzyść, zazwyczaj sprawnie przystosowuje ją do własnego użytku. Stąd poszkodowana firma, często poprzestaje na domniemaniu, że konkurent prowadząc podobne badania samodzielnie doszedł do identycznych wyników.

Często uważa się, że zarówno wywiad gospodarczy, jak i szpiegostwo gospodarcze uprawiane dla zysku przez konkurujące ze sobą firmy, są logiczną konsekwencją zapotrzebowania na informacje, które w dzisiejszym skomplikowanym świecie gospodarczym stały się decydującym czynnikiem wpływającym na rentowność przedsiębiorstwa. Z drugiej strony nadmiar nieuporządkowanych informacji może stanowić problem dla gospodarki kraju.

Istotne są zatem, jak w każdej dziedzinie, specjalizacja i profesjonalizm. Przykładem może być wywiad wojskowy czy polityczny, którym zależy na zdobyciu zwięzłych i ściśle chronionych informacji. Świat biznesu potrzebuje rzeczowego przeglądu całokształtu sytuacji. W wielu dziedzinach wyspecjalizowane służby dyplomatyczne przygotowane są do zbierania, selekcjonowania, interpretowania informacji a nawet wnioskowania − tradycyjnymi metodami penetracji rynków w zakresie problemów, będących przedmiotem zamówień i zainteresowania specjalistów z określonych gałęzi gospodarki. Służby te w dużej mierze są w stanie dostarczyć odpowiedzi na większość zgłoszonych problemów badawczych w analizowanych środowiskach.

Można czasem, gdyby inne działania zawiodły, pożądaną informację lub produkt nabyć od właściciela, w formie zwykłej transakcji handlowej. Często legalne metody w rezultacie będą o wiele tańsze niż działania o charakterze szpiegostwa gospodarczego, którego destrukcyjny i kryminalny skutek jest bezsporny.

Wiadomo, że wywiad gospodarczy jest istotnym instrumentem walki konkurencyjnej pomiędzy rywalizującymi ze sobą firmami. Natomiast główną myślą przewodnią niniejszej książki jest teza, iż: Przedsiębiorstwo, które nie stosuje profesjonalnych zasad bezpieczeństwa, wkrótce zanotuje poważne straty. Bezpieczeństwo informacji prawnie chronionych jest podstawowym obowiązkiem związanym z bezpieczeństwem firmy.

Problem ten jest niezwykle ważny i niepokojący, gdyż wielokrotnie okazuje się, że w Polsce ochrona informacji jest daleka od pożądanej. W przekonaniu tym utwierdzają

nas nie tylko sporadyczne informacje medialne. Okazuje się bowiem, że różnorodne dokumenty zawierające chronione informacje czy tajemnice zawodowe, będące własnością niektórych organów państwowych, można znaleźć na wysypiskach śmieci. Podobnie jest z danymi dotyczącymi tajemnicy bankowej, ubezpieczeniowej, handlowej, a także chronionych danych osobowych i tajemnic przedsiębiorstwa.

Warto zadać proste pytanie: komu potrzebny jest wywiad gospodarczy?

Wywiad gospodarczy, czy jak wolą niektórzy autorzy – wywiad ekonomiczny, a raczej biznesowy, umożliwia podejmowanie bardziej trafnych decyzji o istotnym znaczeniu dla przedsiębiorstwa. Do tego typu decyzji należą duże przedsięwzięcia inwestycyjne, zmiana strategii służącej intelektualnym i ekonomicznym zaatakowaniem konkurenta. Kiedy decyzja już zapada, zdobyte informacje umożliwiają minimalizowanie związanego z nią ryzyka[210].

Tylko z pozoru odpowiedź nie sprawi trudności, gdyż jej uzasadnienie może okazać się kontrowersyjne, szczególnie dla tych, którzy poczują się poszkodowani efektami działań wywiadowczych. Zatem przed udzieleniem zdecydowanej odpowiedzi warto zapoznać się chociażby z najbardziej dostępnymi wydarzeniami zarówno z historii wywiadu gospodarczego, które przeplatają się ze szpiegostwem gospodarczym i wywiadem wojskowym czy państwowym.

Wywiad ekonomiczny i konkurencyjny jest praktyką starą jak świat, a niektóre metody działania – kontrowersyjne. Historia i literatura dostarczają na ten temat wielu dowodów. Przykładowo Republika Wenecka utrzymała swoją potęgę przez ponad 200 lat dzięki znakomitemu systemowi wywiadowczemu. Dobrze zorganizowana sieć własnych ambasadorów we wszystkich krajach europejskich służyła zbieraniu informacji zewnętrznych, a dziesięć tysięcy prostytutek, uzyskiwało informacje od osób bawiących w Wenecji. Ówcześni politycy i przedsiębiorcy działali zapewne w myśl słusznego powiedzenia Leonarda da Vinci, że: Brak przewidywania oznacza cierpienie już teraz.

Najnowsza historia wywiadu i szpiegostwa gospodarczego wyraźnie zwraca uwagę na wydarzenia w skali międzynarodowej. Przykładowo w połowie XIX wieku, rozpoczęła się istna inwazja Wschodu na rozwinięte kraje Zachodu. Japończycy, a następnie Chińczycy uświadomili sobie ogromne możliwości, jakie stwarza rozwijający się przemysł. W pełni wykorzystali zachodnie doświadczenia, wysyłając swoją najbardziej uzdolnioną młodzież nie tylko na studia, lecz przede wszystkim do pracy w przemyśle, głównie amerykańskim i brytyjskim. Wysyłano tysiące ludzi, którzy podejmowali pracę w przemyśle kluczowym, po to, by opanować tajemnice technologiczne. W Japonii w stosunkowo krótkim czasie, dzięki zdolnościom naśladownictwa i taniej sile roboczej, Japończycy byli w stanie konkurować z zachodnimi producentami. Wkrótce także młodzi chińscy businessmani penetrowali wszystkie dziedziny gospodarki i mimo rosnącej cenie siły roboczej i coraz wyższej stopy życiowej, ich zaawansowanie, technika i pozycja w przemyśle, a także ich zdolności umożliwiały utrzymanie wysokiego poziomu konkurencyjności.

W połowie XX wieku ujawniono, że w Japonii i Szwajcarii utworzono szkoły wywiadu gospodarczego. Istotnie wpłynęło to na działania przemysłowców brytyjskich, gdyż naczelny dyrektor *Steel Company of Wales*, we wrześniu 1966 r. w Nottingham poradził przemysłowcom angielskim naśladować Japończyków. W przemówieniu

210 B. Martinet, Y.M. Marti, *Wywiad gospodarczy…*, s. 16.

wygłoszonym na forum sekcji ekonomicznej Brytyjskiego Towarzystwa Krzewienia Wiedzy przyznał, iż jego koncern utrzymuje stale swych ludzi w Japonii; usiłują oni podpatrzeć, w jaki sposób Japończycy doszli do tych „nadzwyczajnych wyników", jakie uzyskają w swych zakładach przemysłowych. Mówca podkreślił, że zapewne jest to rezultatem silnego wpływu ich filozofii, która sprowadza się do formuły: Znajdź najlepszą na świecie technologię i jeszcze ją udoskonalaj.

Wydaje się, że formuła ta pomogła w realizacji wielu europejskich przedsięwzięć w tym okresie, a przykładowo:

- w Wielkiej Brytanii szpiegostwo gospodarcze zastąpiło bardziej tradycyjne **i** jawne metody zdobywania informacji, na co zebrano wiele przekonywających dowodów;
- wywiad francuski w tym okresie ogłosił, że posiada niezbite dowody na istnienie i szkodliwe skutki szeroko rozpowszechnionego szpiegostwa gospodarczego we Francji. W związku z tym wydano broszurę pt. *L'Espionage – une Realite*, którą otrzymało dziewięć tysięcy przemysłowców;
- w Belgii wzrosło zaniepokojenie szpiegostwem gospodarczym, zwłaszcza w powiązaniu z jego aspektami wojskowymi i politycznymi. Jeden z belgijskich ekspertów ds. bezpieczeństwa miał opracować rozprawę doktorska na ten temat. Z udziałem członków rządu odbyła się też konferencja poświęcona problemom bezpieczeństwa oraz szpiegostwu gospodarczemu. Powodem był fakt, że zamieszkały w Belgii cudzoziemiec został zidentyfikowany jako profesjonalny szpieg gospodarczy;
- w Niemczech ujawniono kilka przypadków szpiegostwa, z których najpoważniejszy dotyczył próby przekupienia naukowca, zatrudnionego w ważnym laboratorium przemysłowym;
- w USA zanotowano przypadek Włocha, który przeniknął do firmy medycznej, aby podpatrzyć u amerykańskiego producenta farmaceutycznego tajemnicę produkcji leków. Był to ważny sygnał, że wkrótce w wielu krajach, wywiady gospodarcze zaczną aktywnie interesować się biotechnologią.

Z wielu różnorodnych informacji wynika, że wywiady polityczne krajów socjalistycznych osiągnęły liczne sukcesy w zakresie zdobywania nowości technicznych w rozwiniętych krajach Zachodu.

Najnowsze doniesienia wykazują, że w wielu zaprzyjaźnionych krajach Wschodu i Zachodu prowadzone są nie tylko działania w zakresie wywiadu gospodarczego, lecz również szpiegostwa gospodarczego i szpiegostwa politycznego. Ujawnione afery podsłuchowe wyraźnie wskazują, że mimo wspólnych działań politycznych i ekonomicznych prowadzone są działania sprawdzające i weryfikujące oficjalne informacje.

Na skutek wielu różnorodnych czynników prawnych i społeczno-ekonomicznych, na przełomie XX i XXI wieku wywiad gospodarczy wszedł w fazę intensywnego rozwoju. Sprawdzanie wiarygodności klientów i partnerów transakcyjnych stało się obowiązkiem wynikającym z procedur dotyczących bezpiecznego funkcjonowania przedsiębiorstwa.

Mało ryzykowna jest teza, że współczesne realia stwarzają sytuacje, w których prowadzenie wywiadu gospodarczego i biznesowego (konkurencyjnego) dla wielu przedsiębiorstw stało się koniecznością ze względów ekonomicznych. Głównym powodem jest konieczność dostosowania się do nowych warunków prowadzenia polityki handlowej, cenowej i marketingowej. Aby je szybko poznać i sprawnie na nie reago-

wać z powodzeniem prowadzi się działania rozpoznawcze, analityczno-prognostyczne i wywiadowcze w formie wywiadu gospodarczego.

Zdobyta wiedza o konkurencji umożliwia podejmowanie trafnych decyzji w ramach działania przedsiębiorstwa, które mogą mieć znaczenie o charakterze inwestycyjnym, handlowym czy o zmianie ceny, nowej produkcji, sprzedaży i na tym tle wyprzedzeniu konkurencji, a przede wszystkim pozwalają uniknąć zagrożeń oraz obniżyć poziom biznesowego ryzyka. Może również służyć do ustalenia głównych decydentów konkurencji i określenie ich profili psychologicznych.

Podstawą wywiadu gospodarczego jest prowadzenie wszelkich działań w granicach prawa i etyki zawodowej, które ściśle wiążą się z etyką bezpieczeństwa biznesu[211]. Eksperci w tej branży skupieni są także w krajowych i międzynarodowych stowarzyszeniach w celu: wymiany doświadczeń i promowania tej profesji w społeczeństwie[212].

W połowie XX wieku eksperci angielscy, specjaliści z zakresu wywiadu gospodarczego zauważyli, że niezmiernie ważne jest prowadzenie w badanym kraju czy konkurencyjnej korporacji działań, obejmujących zarówno cele wywiadu gospodarczego, jak i szpiegostwa gospodarczego. Zmierzają one zazwyczaj do:

- poznania planowanych w przyszłości przedsięwzięć ekonomicznych rządu czy korporacji, które są zazwyczaj informacjami chronionymi;
- uzyskania danych dotyczących planowanych przedsięwzięć marketingu innych państw czy firm;
- ustalenia kierowniczego personelu korporacji w celu wykorzystania jej członków w planowanych przedsięwzięciach oraz rozpoznanie ich zainteresowań i słabości;
- określenia zalet ekonomicznych i organizacyjnych badanego konkurenta, bądź firm, które zamierza on przejąć;
- utrwalenia i utrzymania własnego stanowiska kierowniczego.

Możliwe jest również rozpoznanie różnorodnych działań wywiadowczych mających na celu:

- przywłaszczenia, oszustwa finansowego czy innego tego typu przestępstwa;
- zdobycie poufnych informacji ekonomicznych, będących wyłącznie w gestii zarządu, w celu ich przedwczesnego opublikowania, co miałoby wpływ na cenę giełdową akcji;
- pozyskania poufnych informacji dotyczących planowanych cen, które wkrótce znajdą się w ofercie konkurencyjnej firmy[213].

211 J. Konieczny, *Wstęp do etyki biznesu*, Warszawa 1998, s. 5–14.

212 Pierwsze Stowarzyszenie Profesjonalnych Wywiadowców Gospodarczych utworzono w 1986 r. w Stanach Zjednoczonych, jako *Society of Competitive Intelligence Professionals* (SCIP). Pierwotnie nazywało się ono *Society of Competitor Intelligence Professionals*, czyli stowarzyszenie profesjonalistów z dziedziny informacji o konkurencie. Jednak pojęcie „konkurent" okazało się mało precyzyjne, gdyż podejmowane działania wywiadowcze dotyczą także innych dziedzin jak np.: finansów, gospodarki, strategii, technologii itp. W związku z tym słowo *competitor* (konkurent) zastąpione zostało słowem *competitive* (konkurencja). Chodzi zatem o szeroko rozumianą działalność wywiadowczą, umożliwiającą przedsiębiorstwu zdobycie przewagi konkurencyjnej. Zatem różnorodność form tej działalności może być szeroko stosowana jest wtedy pominięta. Szerzej: B. Martinet, Y.M. Marti, *Wywiad gospodarczy…*, s. 312.

213 P. Hamilton, *Wywiad gospodarczy*, Warszawa 1971, s. 29-30. Tytuł oryginału: *Espionnage and Subversion Industriel Society*, London 1967.

Ważne jest uzasadnienie pozyskania wiedzy co do tych operacji, a mianowicie poznanie przyszłych planów gospodarczych rządu określonego kraju stwarza możliwości uzyskania dużych korzyści finansowych. Informacja o planach udzielenia pożyczki krajowi, czy innej firmie, mającej w tym względzie istotne potrzeby, daje przedsiębiorcom możność wcześniejszego zorganizowania agencji i biur obsługi, które umożliwią wyrobienie dobrej pozycji startowej do kolejnych transakcji. Podobnie przedstawia się sprawa poznania planów innej firmy, dotyczących opanowania przez nią jakiejś nowoczesnej czy wyspecjalizowanej dziedziny. Wczesne poznanie tych planów umożliwia rozpoznanie i zajęcie właściwej propozycji nabywczej i cenowej. Nowa, zasobna w kapitał firma, nawet z niewielkim udziałem w nowej produkcji rynkowej, może uzyskać sposoby na pokonanie głównego konkurenta, choćby nawet przez ustalenie i przejęcie jego kluczowej kadry.

Jednakże praca wywiadu gospodarczego nie polega jedynie na penetracji konkurencyjnej firmy. Po rozpoznaniu osobowym kadry konkurencji, jej zwyczajów i zasobów, nowa firma może zaproponować korzystniejsze warunki finansowe i możliwość awansu.

Kolejną, również dawno stosowaną metodą jest próba opanowania rynku poprzez sprzedaż towaru ze stratą. W tej samej kategorii mieści się ustalanie głównych nabywców towarów konkurencji i pozyskanie ich nawet poprzez istotne obniżenie ceny. Utrata klientów stanowi istotny cios dla konkurencyjnej firmy, która może to traktować nawet jako przegraną w swoistej wojnie psychologicznej. Czasem jest już za późno, aby przekonać się, że na wolnym rynku można zyskać dobrą pozycję, a można również ją stracić. Wszystko zależy nie tylko od towaru, jego jakości, formy dostawy i ceny, lecz również od rodzaju i sprawności obsługi. W tych kwestiach niezbędny staje się operatywny wywiad gospodarczy, który będzie w stanie dostrzec słabości i wykazać je firmom planującym zająć dominującą pozycję. To tylko niektóre elementy przydatne do wytworzenia klimatu dla atrakcyjnej oferty i uzyskania sukcesu biznesowego.

Nie ulega wątpliwości, że w dzisiejszym świecie odbywa się stały transfer wiedzy, umiejętności, kompetencji. Wymagają one profesjonalnej klasyfikacji, analizy, syntezy i wnioskowania. Należy to do profesjonalnych i wyspecjalizowanych w określonych kategoriach, analityków informacji. Niektóre kraje wykorzystują najnowsze technologie dla potrzeb wszelkiego rodzaju wywiadów. Natomiast kraje o największym potencjale ekonomicznym i militarnym budują swoje superwywiady.

W dzisiejszym świecie dociera do nas coraz więcej informacji, ale wydaje się za uzasadniony pogląd, że wiemy coraz mniej. Brakuje nam czasu na zdobycie wiedzy, jej uporządkowanie, aby była pogłębiona i kompleksowa. Prawdziwą wagę problemów ocenia wyspecjalizowany analityk określonego ściśle rodzaju informacji: kryminalnej, gospodarczej, finansowej, demograficznej itp. Ten specjalista dociera do faktów, odkrywa istotę zdarzeń, aby przekazać sprawdzoną wiedzę. Tylko taka wiedza daje bezpieczeństwo i pewność działania. Wszystkie kraje prowadzą systematyczne działania mające na celu zabezpieczenie swoich interesów. Dominującą pozycję w zbieraniu informacji zajmują służby specjalne, które tylko z podsłuchów zbierają i analizują 100 mld informacji miesięcznie.

System inwigilacji prowadzonej przez USA ma służyć walce z terroryzmem, ale szpiegowane, czy podsłuchiwane są również kraje sojusznicze, także UE, a także Niemcy, Francja i Polska.

Przepływ większości informacji w sieci powoduje zacieranie się różnic pomiędzy legalnym działaniem wywiadu gospodarczego a nielegalnym działaniem w ramach szpiegostwa gospodarczego. Dochodzi do takich sytuacji w skali międzynarodowej, że Brazylia, Meksyk, Francja i Niemcy zażądały od USA wyjaśnień, dlaczego są szpiegowani ich prezydenci i inni dostojnicy. Nie ważne są formy i metody podsłuchu, czy jest to podsłuch tematyczny czy hasłowy obejmujący określone terminy. Istotą jest podsłuchiwanie sojuszników. Czynią to nawzajem wszystkie wywiady.

Zaciera się również metodyka zdobywania informacji, a klasycznym tego przykładem jest działalność hakerów. Haker penetruje każdy system, każdy komputer, każde urządzenie mobilne i każdą instytucję – im bardziej jest chroniona tym odczuwa on większy pęd do zdobycia informacji.

Nastaje okres deregulacji wielu zawodów. Jednakże w wielu zawodach wymagany jest najwyższy profesjonalizm. Dotyczy to przykładowo takich specjalizacji jak: wywiadowca kryminalny, wywiadowca gospodarczy, analityk innych specjalistycznych informacji.

Analizując zagadnienie metodyki zdobywania informacji przez różnorodne wywiady nie można nie dostrzegać narastających zagrożeń występujących we współczesnym świecie:

- militarne jest zagrożeniem stałym i narastającym bardziej niż w poprzednich latach, a niestabilność bezpieczeństwa w wielu regionach świata jest obecnie największa;
- imigracyjne, nasilające się z Afryki i Azji. W Europie towarzyszy temu niepokój w postaci lęku przed obcymi.

Największe współczesne wyzwania, silnie związane z bezpieczeństwem informacji, można rozważać w wielu grupach problemowych, a przykładowe to:

1. problemy ekonomiczne – nowe kraje przejawiają zainteresowanie nasilaniem produkcji i eksportu, przejmowanej z wielu dotychczas tradycyjnych krajów;
2. zagrożenie energetyczne, które może być dużym źródłem konfliktów z uwagi na brak nowych źródeł energii;
3. bezpieczeństwo informacyjne – związane z totalnym stosowaniem podsłuchów przez USA. Takie działania oprócz wielu aspektów negatywnych zapewniają poważny rozwój współczesnych technologii. (Przykładowo, rząd USA dysponuje w Kalifornii 12 największymi na świecie komputerami, które rozwiązują najtrudniejsze zagadnienia). Istotą jest problem wyścigu o dominację w zakresie opanowania cyberprzestrzeni zagrożonej nie tylko kradzieżą informacji, lecz cyberterroryzmem;
4. silna konkurencja o zasoby mineralne. Jeśli przyjąć, że co 100 lat następuje przełom w tej kwestii, to szacuje się, że minęło już 70 lat;
5. doskonalony wciąż dostęp do infrastruktury i umożliwienie dostaw towarów. Przykładowo w celu usprawnienia planuje się sieć komunikacyjną od Brukseli po Władywostok i Pekin;
6. nasilają się występujące nierówności we współczesnym świecie na tle powszechnego prawa do rozwoju;
7. istotne jest zdominowanie gospodarki światowej przez system finansowy, który jednak nie zapewnia bezpieczeństwa, (szacuje się, że l% ludzi ma 46% bogactwa światowego);

8. terroryzm jest zjawiskiem rozpoznanym, a jego zapobieganie wymaga nadal dużych nakładów;
9. nastąpił istotny wzrost gospodarczy oraz istotne przesunięcie produkcji z Zachodu na Wschód, który dąży do pozycji dominującej;
10. przestępczość zorganizowana, a szczególnie cyberprzestępczość wprawdzie zmienia formy, ale nie jest zagrożeniem globalnym. Nasila się zapotrzebowanie na cudze informacje zarówno w skali mikro, jak i w ramach agresywnych działań międzynarodowych;
11. wśród występujących zagrożeń jednym z najważniejszych zagadnień jest bezpieczeństwo informacji, a informacji gospodarczej w szczególności.

Z klasycznej pozycji literatury na temat wywiadu gospodarczego jasno wynika konieczność doceniania wagi omawianego zagadnienia, a mianowicie: *Rozważania o wywiadzie gospodarczym jako czynniku przewagi konkurencyjnej stały się powszechne, gdy przedsiębiorstwa podjęły walkę konkurencyjną na rynkach międzynarodowych, poznając nowe przyczyny sukcesów i porażek własnych oraz doznawanych przez ich konkurentów. Z analizy tych przyczyn wynika, że aby osiągnąć trwałą przewagę konkurencyjną, nie wystarczy dobry produkt, znakomity marketing, kreatywność sprzedawców czy charyzmatyczny szef. Okazuje się, że trzeba przede wszystkim poznać i zrozumieć uwarunkowania oraz reguły gry konkurencyjnej, a także strategie graczy i ich silne oraz słabe strony. W efekcie pojawiło się pojęcie wywiadu gospodarczego*[214]. Podstawą każdego wywiadu jest uzyskanie informacji niezbędnych w funkcjonowaniu przedsiębiorstwa.

Niewiele zmieniło się od okresu, w którym prof. Mirosław Kwieciński w swojej rozprawie habilitacyjnej, a jednocześnie jednej z pierwszych polskich monografii na temat wywiadu gospodarczego, napisał: *Trzeba wyeliminować fałszywe pojmowanie wywiadu gospodarczego w dotychczasowej praktyce zarządzania, które utożsamia wywiad gospodarczy ze szpiegostwem gospodarczym. Jest to efekt traktowania wywiadu gospodarczego jako zjawiska, które jest wdzięcznym tematem artykułów publicystycznych dla nie zawsze znających się na jego istocie autorów, ale także jako zjawiska otoczonego swoistym nimbem tajemniczości, a więc nie do końca właściwie pojmowanym przez menedżerów. Stan taki jest wynikiem luki edukacyjnej, wywiad gospodarczy bowiem jest zagadnieniem bardzo rzadko ujmowanym, nie mówiąc już o przedmiocie, w programach kształcenia przyszłych menedżerów*[215].

Wywiad gospodarczy to trudna i złożona dziedzina wiedzy z uwagi na obszerny i interdyscyplinarny charakter zagadnienia. Wywiad gospodarczy stanowi bowiem skrzyżowanie różnych dziedzin i kompetencji nie tylko z zakresu prawa, kryminalistyki i kryminologii, organizacji i zarządzania, ekonomii, finansów, socjologii, psychologii, etyki oraz informatyki, lecz również bankowości i ubezpieczeń, a także szeregu dyscyplin technicznych, które stają się niezwykle istotnym przedmiotem analiz. Właśnie interdyscyplinarne i kompleksowe spojrzenie na zagadnienie wywiadu gospodarczego stwarza podstawę do racjonalnego interpretowania zachodzących zjawisk gospodarczych. Takie podejście może stanowić najlepsze źródło nie tylko do analizo-

214 B. Martinet, Y.M. Marti, *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji,* Warszawa 1999, s. 9. Francuskie wydanie tej pracy to: *L'intelligence economique – Les yeux et les oreilles de l'entreprise*, Paris 1995.

215 M. Kwieciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa-Kraków 1999, s. 9, 10.

wania i interpretowania informacji gospodarczych, lecz również do rozwoju i bezpieczeństwa w funkcjonowaniu przedsiębiorstwa.

Wciąż jeszcze zdarza się, że pojęcia wywiadu i szpiegostwa gospodarczego, są używane zamiennie. Przez wywiad gospodarczy należy rozumieć działania zmierzające do uzyskania informacji o innych podmiotach gospodarczych, a pozyskanie tych informacji realizowane jest metodami dopuszczalnymi przez normy prawne oraz zgodnie z zasadami etyki.

Natomiast w przypadku szpiegostwa gospodarczego mamy do czynienia z agresywnymi działaniami zmierzającymi do osiągnięcia tego samego celu, jednakże przy użyciu prawnie niedozwolonych środków, najczęściej poprzez przechwytywanie korespondencji, kradzież dokumentacji, korupcję pracowników konkurencyjnego przedsiębiorstwa, zatrudnianie agentów jako pracowników, stosowanie wszelkich form podsłuchu i różnych form obserwacji.

Wiadomo już, że sukcesy analityków informacji gospodarczej sprzyjają postępowi firmy, a nawet umożliwiają modernizację poprzez podejmowanie najbardziej trafnych decyzji dla przedsiębiorstwa. Zapewne z tego względu profesjonalna prognoza już z początku lat 90. XX wieku przewidywała, że: każdy pracownik będzie wywiadowcą na rzecz swojej firmy i tego typu zadania będą zapisane w zakresie obowiązków, po odpowiednim przygotowaniu personelu[216].

W pogoni za klientem, wykonaniem zamówionych produktów i pieniądzem nie zawsze pamięta się, że niezbędna jest wiedza, czyli cenna informacja. Zdobywaniem i analizowaniem profesjonalnych informacji zajmuje się profesjonalny wywiad gospodarczy. Ta dziedzina wiedzy ma charakter interdyscyplinarny. Wykorzystuje zatem dla swoich potrzeb rozmaite narzędzia właściwe innym dyscyplinom, korzystając w ten sposób z ich bogactwa i różnorodności wypracowanych i już sprawdzonych sposobów postępowania.

Niezwykle istotne jest podkreślenie, że zarówno w definicji, jak i w swych metodach, wywiad gospodarczy jest pojęciem syntetycznym. Jednakże, aby mógł stać się praktyką uznaną i przyjętą w przedsiębiorstwie, musi opierać się na jasno określonej organizacji[217].

Na skutek wielu różnorodnych czynników prawnych i społeczno-ekonomicznych, omówionych tylko częściowo w tej pracy, na przełomie XX i XXI wieku wywiad gospodarczy wszedł w fazę intensywnego rozwoju. Wśród uwarunkowań tego zjawiska można stwierdzić, że na tle rozwijającej się gospodarki i konkurencji, sprawdzanie wiarygodności klientów i partnerów transakcyjnych stało się obowiązkiem wynikającym z procedur dotyczących bezpiecznego funkcjonowania przedsiębiorstwa.

## 2. Z historii i współczesności wywiadu gospodarczego

Od niepamiętnych czasów człowiek podglądał bliźniego, aby uzyskać w ten sposób pewne korzyści. Robili to zwykli ludzie, rolnicy, kupcy, a także królowie, wodzowie i inni przywódcy – czy to dla zaspokojenia własnej ciekawości, czy też osiągnięcia rozmaitych korzyści – by zdobyć władzę, kraj lub podbić inny naród.

Jak wykazuje historia, nie było plemienia czy wspólnoty społecznej, które nie posługiwałyby się wywiadem. Już w czasach biblijnych Mojżesz wyprawiał zwiadow-

216 B. Martinet, Y.M. Marti, *Wywiad gospodarczy…*, s. 325.

217 M. Kwieciński, *Wywiad gospodarczy* .. wyd. cyt., s. 82.

ców do ziemi kananejskiej, by ci rozpoznali mocne i słabe strony jej mieszkańców. Wiele potęg starożytnego świata, tj. Grecja, Rzym, Persja czy Chiny, również pozostawiło po sobie liczne ślady wykorzystywania wywiadu[218].

Z dostępnych przekazów historycznych trudno określić datę powstania wywiadu. W IV wieku przed naszą erą teoretyk sztuki wojennej z Chin Sun-zi w pracy pt. *Sztuka wojenna* podkreślał, że *...uprzednia znajomość rzeczy jest tym czynnikiem, który umożliwia władcy i dobremu dowódcy uderzać, zwyciężać i brać łupy.*

Mówiąc żartem pierwszym szpiegiem gospodarczym był mitologiczny Prometeusz, który (bez licencji i opłaty) wykradł ogień bogom z Olimpu i ofiarował go ludziom. Został za to surowo ukarany – przykuty do skały w górach Kaukazu był torturowany przez orły wydzierające mu wątrobę. Opowieść dotyczy zbrodni i kary, ale historia i legendy pouczają, że najpilniej strzeżone tajemnice były wykradane. Przykładowo, Chińczykom skradziono niezwykle chronioną tajemnicę produkcji jedwabiu, czyli najbardziej eleganckiej i luksusowej tkaniny kilku epok.

Powszechnie uważa się, że szpiegostwo gospodarcze jest działaniem tak starym jak rodzaj ludzki i – jak wykazuje historia – nie było plemienia lub wspólnoty społecznej, które by się nim nie posługiwały w każdej epoce. W starożytności, jak i w naszych czasach pierwszą decyzją państwa po ukonstytuowaniu się jest tworzenie instytucji informatorów, rozgałęzionej na sposób systemu nerwowego i stworzonej dla działania zarówno w kraju, jak i za granicą. Te regularne źródła informacji stanowią podstawę polityki i przyszłych zamierzeń każdego rządu.Za udowodnione uważa się przekazy historyczne, które wskazują, że ten rodzaj szpiegostwa jest tak stary, jak ludzkość. Już od najdawniejszych czasów ludzie usiłowali przyswoić sobie nowe lub bardziej doskonałe technologie w sposób najłatwiejszy, tzn. po prostu kradnąc je temu, kto je posiadał. Natomiast podkreślenia wymaga specyficzna cecha wywiadu gospodarczego, w odróżnieniu od wojskowego i politycznego, mianowicie że niejednokrotnie jego działania skierowane są przeciwko konkurencyjnym firmom w tym samym państwie.

Przez cztery wieki różne wywiady usiłowały wykraść tajemnicę „greckiego ognia" wynalezionego w Konstantynopolu. Dopiero Arabowie posiedli tajemnicę tej, na owe czasy, broni totalnej.

Egipcjanie na 2000 lat przed naszą erą wynaleźli tzw. niebieską ceramikę. Tajemnicę produkcji skutecznie chroniono. Dopiero wynalazek współczesnych inżynierów francuskich doprowadził do wyjaśnienia tej skomplikowanej technologii.

Największa wojna wywiadów gospodarczych rozpętała się wokół porcelany, którą od tysiącleci produkowali Chińczycy. Doceniano jej niezwykłe właściwości: delikatność, a równocześnie trwałość. Sposób wytworzenia przez stulecia pozostawał nierozpoznany. Tajemnica produkcji przeniknęła jednak z Chin do Korei, a stąd, na kilka lat przed naszą erą – do Japonii. Produkowana przez Japończyków porcelana nie była jednak tak dobra jak chińska. Stąd rzemieślnicy japońscy jeszcze w XVIII wieku udawali się do Chin, aby podpatrzeć, w czym tkwi źródło sukcesu.

Europa nie znała sposobu produkcji porcelany. Dopiero w 1712 r. jezuita francuski udał się do Chin i w korespondencji przesyłanej do Francji dał dokładny opis produkcji porcelany z kaolinu. Udało mu się również przemycić próbki surowca. W kilkadziesiąt

218 Szerzej: E. Cilecki,, *Penetracja rynków zagranicznych: wywiad gospodarczy*. Warszawa, s. 76-92. Także: L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy. Historia i współczesność. Kraków 2005,* s. 11-24

lat później, w Sevres, Francuzi zaczęli produkować piękną porcelanę, wykorzystując własne pokłady kaolinu[219].

W Polsce za organizatora wywiadu na szeroką skalę uznaje się Bolesława Chrobrego. Był on zawsze dobrze poinformowany o tym, co dzieje się na dworze niemieckim. Na Rusi podobną funkcję pełniło otoczenie polskie księcia Świętopełka i jego żony; pod zarzutem spiskowania przeciwko księciu Włodzimierzowi znalazł się w więzieniu biskup Reinbern. Zarzutem szpiegostwa obarczył Thietmar wysłannika Bolesława Chrobrego – opata Tuni220.

Już w XVl-wiecznej Wenecji sporządzono czarną listę nieuczciwych kupców. W 1841 r. grupa kupców nowojorskich, kilkakrotnie oszukanych przez niewypłacalnych odbiorców skupionych wokół Lewisa Tapmana, założyciela The Mercantile Agency, zorganizowała sieć korespondentów, którzy odwiedzali firmy, opisywali je i rozmawiali z dostawcami. Wkrótce robili to już nie tylko na własny użytek – udostępniali dane tym, którzy za nie płacili.

W latach 20. XX wieku wykorzystywano bardzo szeroko wywiad ofensywny za granicą w postaci prywatnych biur detektywistycznych i wywiadowczych. Świadczyły one usługi wszystkim zainteresowanym, osobom prawnym i instytucjom lub firmom, każdemu kto tylko gotów był zapłacić. Sprzedawano informacje handlowe, spadkowe, a w zależności od zamówienia również z zakresu wywiadu gospodarczego. Podobny charakter miała organizacja występująca pod nazwą *Kartell der Auskunftei Bürgel* (kartel wywiadowczy), zajmująca się zbieraniem informacji handlowych w Niemczech i za granicą. Centrala jej mieściła się Akwizgranie. Organizacja ta posiadała ok. 300 filii. I tak filia w Gdańsku prowadziła wywiad ekonomiczny na Polskę, Wolne Miasto Gdańsk, ZSRR, Finlandię, Łotwę, Litwę i Estonię[221].

Niemcy dla celów wywiadu gospodarczego na Wschodzie powołali w Królewcu tzw. *Wirtschaftsinstitut fur Russland und die Oststaaten*, który według danych Oddziału II Sztabu Głównego Wojska Polskiego w 1927 r. miał do dyspozycji w Polsce 300 agentów gospodarczych. Stosowaną metodą pracy było umieszczanie rezydentów w stałych punktach zagranicznych w charakterze przedstawicieli i agentów firm handlowych. Wraz z informacjami zbieranymi w sposób tajny, rezydenci opracowywali wszelkie dostępne informacje gospodarcze z prasy, publikacji naukowych, politycznych, gospodarczych czy handlowych[222].

Nawet mały udział Stanów Zjednoczonych w pierwszej wojnie światowej zadziałał ożywczo na przemysł i spowodował dalsze wzbogacenie *się*. Wraz z rozwojem przemysłu rozwijał się wywiad. Był to wywiad odmienny od wojskowego, ale żyjący jego tradycją i metodami działania wywiad przemysłowy. Na uwagę zasługuje Ulmont O. Cumming, agent-weteran, szef amerykańskiej firmy wywiadowczej założonej w 1927 r., który opublikował pamiętniki dotyczące okresu międzywojennego. Twierdził, że prowadził w tym czasie 27.853 sprawy z dziedziny wywiadu i kontrwywiadu przemysłowego. Już wówczas, na co warto zwrócić uwagę, nie przejmował się etyczną stroną swej pracy. Jako wywiadowca przemysłowy pracował dla kilku najbardziej szanowanych kancelarii adwokackich Stanów Zjednoczonych, a także dla 15 wielkich towarzystw przemysłowych.

219 L. Bajer**,** *Wywiad gospodarczy,* Warszawa 1979, s. 10.

220 M. Biskup (red.) *Historia dyplomacji polskie***j,** Warszawa 1982, s. 86.

221 W. Kozaczuk**,** *Bitwa o tajemnice. Służby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939***,** Warszawa 1977, s. 89.

222 I. Krasuski**,** *Stosunki polsko-niemieckie 1918-1925,* Poznań 1962, s. 22.

W 1934 r. rząd amerykański powołał specjalny komitet dla zbadania całokształtu sytuacji w amerykańskim przemyśle zbrojeniowym. Okazało się, że sam komitet posługiwał się materiałami pochodzącymi z bardzo podejrzanych źródeł. Komitet zainteresował się szczególnie łodziami podwodnymi firmy *American Electric Boat Company* i jej angielskiego wspólnika koncernu *Vickers*. Jak zeznał na procesie Herbert Alten, przedstawiciel grupy *Driggs,* właśnie z powodu wywiadowczej działalności stracił olbrzymie zamówienie w Turcji dla *Vickersa"* [223].

W latach międzywojennych w USA pojawia się także nowy rodzaj wywiadu, wywiad podatkowy. Była to rozgałęziona siatka sterowana przez ministerstwo finansów USA. Chętnie zatrudniała pracowników-amatorów, którzy otrzymywali 10% od każdego wykrytego przestępstwa podatkowego. Wbrew pozorom nie było to zajęcie bezpieczne tym większe, przestępstwa podatkowe popełniają zazwyczaj osoby czy przedsiębiorcy dobrze sytuowani, w tym przestępcy zorganizowani. Właśnie za nie są pociągani do odpowiedzialności karnej, gdyż inne przestępstwa trudno jest im udowodnić. Dotyczy to m.in. często przywoływanego, słynnego gangstera Al Capone, któremu policja nie potrafiła nic udowodnić poza tym, że nie płacił podatków w odpowiedniej wysokości.

Wywiad podatkowy rozwinął się tak dalece w USA, że w 1938 roku ministerstwo skarbu wydało wewnętrzne zarządzenie zabraniające jego agentom zakładania podsłuchu telefonicznego. Mimo tego zakazu podsłuch był nadal praktykowany.

Wywiad przemysłowy w USA rozwijał się w miarę wzrostu nakładów na badania techniczne, a także w miarę postępującej w międzywojennym okresie koncentracji kapitału oraz rozrastania się poszczególnych koncernów. Proces ten najlepiej ilustrują następujące dane z tego okresu. Przykładowo, w 1939 r. dwieście firm przemysłowych miało w swych rękach 3/5 wszystkich kapitałów i 1/2 całej produkcji w USA. W 1945 r. już tylko 100 wielkich koncernów wytwarzało 1/3 produkcji przemysłowej kraju i zatrudniało 1/5 ogółu pracujących. W tym procesie wywiad i kontrwywiad także odegrały swoją rolę. Z dostępnych przekazów wynika iż tylko potentaci okradali się nawzajem[224].

Wydaje się, że istnieje uzasadnione przekonanie, iż wielkie koncerny różnymi metodami walczą o nowe technologie, ale jeśli jakieś odkrycie zagraża ich aktualnej produkcji, ich aktualnym interesom handlowym – potrafią zablokować wynalazkowi drogę na rynek, a w razie konieczności nie cofną się przed zniszczeniem wynalazcy. Mają przecież potężne środki w ręku.

Po drugiej wojnie światowej Amerykanie wdrożyli nową metodę, znaną jako tzw. drenaż mózgów, czyli ściąganie najwybitniejszych specjalistów z całego świata. W istotny sposób zasilili oni amerykańską naukę.

Począwszy od drugiej połowy XX wieku obserwujemy nasilenie działalności wszystkich rodzajów wyspecjalizowanych instytucji zajmujących się gromadzeniem informacji. Doprowadziło to do powstania nowych, wyspecjalizowanych firm, a także do nowych kierunków działania, w tym przede wszystkim szpiegostwa gospodarczego. Na tym tle warto zwrócić uwagę na działania politycznego wywiadu gospodarczego państw socjalistycznych, który był istotnym elementem unowocześniania gospodarki. Działania tego wywiadu były niezwykle cenne z uwagi na embargo dotyczące nowoczesnych technologii. Szczególnie penetrowane były: USA, Japonia oraz Repu-

223 L. Bajer, *Wywiad gospodarczy.* Warszawa 1979, s. 148.

224 Tamże.

blika Federalna Niemiec. W tym ostatnim kraju straty z powodu szpiegostwa gospodarczego wynosiły 5-8 miliardów marek rocznie, gdy na cele badawcze wydawano około 5 miliardów.

Na tym tle wiele krajów podjęło zabezpieczające działania prawne. Pierwsza ustawa o ochronie informacji niejawnych, a szczególnie przeciwko szpiegostwu gospodarczemu została uchwalona w Kalifornii w 1963 roku. Jednakże zastosowano ją dopiero w trzy lata później. Konieczność przeciwdziałania nasilającym się zagrożeniom uwidoczniła się w niektórych krajach zaostrzeniem odpowiedzialności karnej za szpiegostwo gospodarcze. Przykładowo, w USA zaostrzono odpowiedzialność karną przewidzianą w ustawie federalnej z 1968 roku za kradzież tajnych informacji przemysłowych. Od 1996 roku sprawca tego rodzaju przestępstwa może być skazany na karę pozbawienia wolności do lat 15 i grzywnę do 10 mln dolarów.

Powszechnie wiadomo, że wywiad gospodarczy ma długą historię, jednakże jego podstawy teoretyczne zaczęto tworzyć dopiero w połowie XX wieku a rozwój literatury przedmiotu datuje się po roku 1980. Do tego czasu w większości przedsiębiorstw związanych z konkurencją produkcji czy handlu ograniczano się jedynie do wyszukiwania informacji z dostępnych źródeł. Wywiad gospodarczy był mylony z inną dyscypliną praktyki i nauki, jaką jest szpiegostwo gospodarcze. Nie mógł zatem mieć istotnego wpływu na istotne decyzje strategiczne. Rozwój kapitalizmu z początkiem XX wieku spowodował wzrost walki konkurencyjnej, jednakże dopiero w latach 70. XX w. w krajach rozwiniętych przemysłowo, zaczęto istotnie doceniać zagadnienie jakości planowania i działania strategicznego. Zaczęto zatem stopniowo wprowadzać wywiad gospodarczy w struktury przedsiębiorstwa. W tym okresie ukazało się kilka znaczących pozycji literatury omawiających tematykę konkurencji i konkurentów. Wyróżnia się tu praca Michaela E. Portera *Strategia konkurencji: Metody analizy sektorów i konkurentów* z 1980 roku, która uważana jest za fundament nowoczesnego, współczesnego wywiadu gospodarczego. Praca ta rozpoczęła nowy etap na drodze ewolucji tej dziedziny nauki. *Podobno od tego okresu w wielu* przedsiębiorstwach zaobserwowano gwałtowny rozwój struktur wywiadowczych. Pojawiło się również pilne zapotrzebowanie na literaturę zajmującą się analizą rynku, konkurentów oraz zdobywaniem i wykorzystaniem wiedzy w procesach decyzyjnych. Warto podkreślić powszechny pogląd, że od tego okresu nastąpił naukowy rozwój wywiadu gospodarczego, który trwa nadal.

Zdaniem prof. Mirosława Kwiecińskiego intensywny rozwój wywiadu gospodarczego jako dziedziny biznesu datuje się od czasu opublikowania pracy Leonarda Fulda[225], który w 1979 r. założył Fuld & Company, jedną z pierwszych firm konsultingowych zajmujących się wywiadem gospodarczym. Organizacja ta nadal prowadzi szkolenia, udziela konsultacji na potrzeby określonych klientów lub organizacji[226]. W latach 80.-90. XX wieku, zgodnie z potrzebami środowiska zaczęły powstawać stowarzyszenia wywiadowców gospodarczych. Zaczęto organizować szkolenia i konferencje naukowe[227]. Dopiero w latach 1988-2000 nastąpił istotny rozkwit literatury

225 M. Kwieciński, *Wywiad…*, s. 29. Szerzej: http://www.fuld.com

226 A. H. Walle, *From marketing research to competitive intelligence: useful generalization or loss of focus?* Management Decision, 1999, nr. 37, s. 520.

227 Jedna z pierwszych konferencji naukowych w Polsce była: *Wywiad gospodarczy. Teoria i praktyka*, która odbyła się 30 września 1999 roku w hotelu Gromada w Warszawie. Szerzej: J.W. Wójcik, *Wywiad gospodarczy – wybrane problemy kryminologiczne* w: materiały cytowanej konferencji.

przedmiotu, a wywiad gospodarczy przyjął swoją obecną formę. Nie ulega wątpliwości, że sprzyjał temu rozwój gospodarczy, rozwijające się problemy konkurencji, a także rozwój Internetu, a zatem łatwiejszy dostęp do elektronicznych baz danych. To wówczas zaczął się rodzić rynek bezpieczeństwa informacji i biznesu. Powstały wówczas pierwsze profesjonalne wywiadownie gospodarcze, a przykładowo: Info-Credit i InfoNet w 1990 r. oraz Infocredit, Dun and Bradstreet Poland i Creditreform Polska w 1992 roku – dysponujące informacjami jawnymi. Zaczęły powstawać również agencje detektywistyczne, które uzyskują informacje metodami niejawnymi, jak obserwacja czy podsłuch. Powstały również firmy headhunterskie, czyli tzw. łowcy głów.

Warto podkreślić, że termin „wywiad gospodarczy" nie stanowi bezpośredniego tłumaczenia z języka angielskiego. Został on niejako dopasowany do *Competitive Intelligence* jako jego polski odpowiednik. Jednakże skojarzenie tych dwu pojęć w rozprawie habilitacyjnej prof. Mirosława Kwiecińskiego[228], było istotną inspiracją dla polskiej literatury przedmiotu i zwróciło uwagę wielu środowisk biznesowych, a także naukowych, na tę nową dziedzinę związaną z bezpieczeństwem biznesu. Świadczą o tym m.in. organizowane konferencje naukowe. Przykładowo: Wszechnica Polska Szkoła Wyższa w Warszawie oraz Fundacja Instytut Wywiadu Gospodarczego w Krakowie zorganizowały w dniu 25 maja 2017 roku Ogólnopolską Konferencję Naukową pn. Wywiad i kontrwywiad w teorii i praktyce biznesu, która skupiła wielu przedstawicieli zainteresowanych środowisk. W konferencji udział wzięło szereg przedstawicieli nauki i praktyki z różnych obszarów nauki i biznesu m.in.:

- menadżerów planujących wdrożyć narzędzie wywiadu i kontrwywiadu gospodarczego,
- analityków życia gospodarczego i politycznego,
- specjalistów w zakresie zarządzania informacją i bezpieczeństwem biznesu,
- pracowników administracji publicznej odpowiedzialnych za bezpieczeństwo i zarządzanie kryzysowe,
- nauczycieli akademickich,
- osób, dla których sprawy bezpieczeństwa biznesu są obszarem szczególnego zainteresowania.

Wygłoszone referaty i dyskusja dotyczyła przede wszystkim:

- aktualnych problemów dotyczących znaczenia i możliwości wykorzystania wywiadu i kontrwywiadu w teorii i praktyce działania biznesu oraz służb specjalnych;
- rozwoju teorii i praktyki wywiadu i kontrwywiadu gospodarczego (biznesowego, konkurencyjnego, technologicznego, handlowego, ekonomicznego, naukowego i in.);
- upowszechnienia doświadczeń z ujawnionych spraw z zakresu szpiegostwa gospodarczego w praktyce śledczej;
- wymiany poglądów na temat przyszłości wywiadu i kontrwywiadu gospodarczego jako współcześnie uniwersalnej metody działania wobec aktualnych wyzwań charakteryzujących się:
  - ✦ nasiloną konfrontacją w biznesie i polityce,
  - ✦ cyberprzestępczością i cyberterroryzmem,
  - ✦ wadliwymi działaniami w zakresie ochrony informacji,
  - ✦ masowymi ruchami migracyjnymi,

228 M. Kwieciński, *Wywiad…*, s. 30.

✦ podziałem świata biznesu i polityki na różnorodne opcje biegunowe itp.

W wyniku dyskusji zmierzano do określenia:

- współczesnych i perspektywicznych zagrożeń bezpieczeństwa biznesu,
- systemowych możliwości przeciwdziałania zagrożeniom bezpieczeństwa biznesu przez administrację rządową i podmioty gospodarcze,
- czynników warunkujących optymalne funkcjonowanie wywiadu i kontrwywiadu gospodarczego,
- kierunków zmian w działaniach wywiadu i kontrwywiadu z perspektywy ewolucji środowiska bezpieczeństwa biznesu.

Ponadto, organizatorzy zapowiedzieli:

- ukierunkowanie doboru tematyki i prelegentów stworzenie platformy do wymiany poglądów,
- położenie nacisku na aplikacyjność rozważanych problemów i rozwiązań,
- stworzenie okazji do wzmocnienia kontaktów, dyskusji oraz integracji środowiska,
- wydawania materiałów konferencji w formie monografii,
- organizowanie kolejnych konferencji naukowych[229].

## 3. Definicja wywiadu

Wywiad, a wywiad gospodarczy w szczególności, jest stary jak ludzkość. Każda epoka, od rzymskiej do napoleońskiej, stosowała sztukę wywiadowczą, wyprzedzając kunsztem wiele innych dziedzin kierowania państwem. Współcześnie również w życiu każdego państwa wywiad odgrywa ważną rolę. Stąd, przez pojęcie „wywiadu" rozumie się *jedną z podstawowych metod zbierania informacji, jak i badania opinii publicznej polegającą na przeprowadzeniu odpowiednio ukierunkowanych rozmów lub badań naukowych*[230]. Wywiad może mieć charakter jawny lub tajny. Jest to pojęcie ogólne. Natomiast w działalności służb wywiadowczych wywiad to *...'specjalny, zazwyczaj państwowy organ, którego zadaniem jest nielegalne zdobywanie niedostępnych innymi sposobami informacji o politycznych, gospodarczych, wojskowych i innych działaniach kraju będącego przedmiotem zainteresowania*[231].

Termin wywiad to szerokie pojęcie, zawierające przynajmniej kilkanaście definicji, a więc:

1. wywiad (jako instytucja państwowa w formie służby specjalnej) – to instytucja państwowa zajmująca się działalnością wywiadowczą. Ogólnie wywiad dzieli się pod względem celów, a przykładowo: polityczny (zdobywanie informacji politycznych), gospodarczy (zdobywanie danych handlowych i technicznych), wojskowy (zdobywanie informacji o organizacji), uzbrojeniu i liczbie wojsk itp.
2. wywiad (rozmowa) – rozmowa dziennikarza z jakąś osobą; rozmowa jest publikowana w czasopiśmie lub prezentowana w radiu czy telewizji;

229 https://www.google.pl/earch?dcr=0&source=hp&ei=Jed-WtK3JtCckwXIz53gCA&q=sprawozdanie+z+ogólnopolskiej+konferencji+naukowej+wywiad+i+kontrwywiad+w+teorii+i+praktyce+biznesu&oq(dostęp 10.02.2018)

230 *Encyklopedia Powszechna PWN*, Warszawa 1987, s. 808.

231 *Encyklopedia szpiegostwa*, Praca zbiorowa, Warszawa 1995, s. 243.

3. wywiad (jako metoda badawcza) – metoda badawcza stosowana m.in. w kryminologii, kryminalistyce, socjologii, psychiatrii i psychologii, jako jedna z podstawowych metod zbierania określonych informacji i badania opinii publicznej polegająca na przeprowadzaniu odpowiednio ukierunkowanych i planowych rozmów;
4. wywiad (medyczny) – informacje od chorego na temat jego subiektywnego odczucia obecnego i przeszłego stanu zdrowia, oraz czynników ryzyka;
5. wywiad diagnostyczny – metoda badawcza w psychologii;
6. wywiad gospodarczy – metoda pozyskiwania informacji o formach i metodach gospodarowania konkurencji;
7. biały wywiad – podstawowa metoda pracy wywiadowczej, polegająca na pozyskiwaniu i analizowaniu ogólnie dostępnych informacji. Znany jest także termin „szary" wywiad jako pośredni pomiędzy białym a czarnym wywiadem;
8. czarny wywiad – metoda pracy wywiadowczej polegająca na pozyskiwaniu i analizowaniu informacji chronionych.

Wraz z rozwojem nauki i techniki nastąpiła specjalizacji i profesjonalizacja oraz rozwój działań wywiadowczych. Pojawiły się różne dziedziny wywiadu gospodarczego, a prawdopodobnie wcześniej szpiegostwo gospodarcze. Systematycznie rozbudowują się służby wywiadowcze prywatne i specjalne państwowe. Występuje różnorodność w nazewnictwie różnych dziedzin wywiadu[232] i profesjonalizacja wywiadowców gospodarczych. Jednakże większość ekspertów czy detektywów unika terminów wywołujących negatywne skojarzenia, zdecydowanie unikając terminu „szpiegostwo" i używa bardziej nobliwego określenia „wywiad gospodarczy" czy „wywiad wśród konkurencji". Taka terminologia jest myląca dla osób, nie znających przepisów prawnych w omawianym zakresie.

Przeglądając różnorodne publikacje naukowe i popularnonaukowe można spotkać zróżnicowane nazewnictwo dotyczące wywiadu, a szczególnie wywiadu gospodarczego, który określany jest również jako: naukowo-techniczny, technologiczny, handlowy, konkurencyjny, finansowy, ekonomiczny, naukowy, strategiczny. Uwidacznia się również określanie wywiadu gospodarczego jako wywiad biznesowy, a także: konkurencyjny, rynkowy, geopolityczny, itp. Przykładowo, organizatorzy Forum Strategicznego Wywiadu Biznesowego zorganizowanego 17 września 2015 r. przez Akademię Leona Koźmińskiego w Warszawie, określili zakres swoich zainteresowań w ramach wywiadu biznesowego jako:

- cykl wywiadowczy i rodzaje produktów wywiadowczych,
- źródła wywiadowcze i metody pozyskiwania informacji,
- metody analizy informacji, analizy wywiadowczej, analizy ilościowej,
- raportowanie i komunikacja wyników działań wywiadowczych,
- ocena wiarygodności biznesowej przedsiębiorstw i osób,
- technologie informatyczne wspierające działania wywiadowcze,

232 Jak: agresywny i tu rodzaj jak np.: technologiczny, handlowy, konkurencyjny, biznesowy ekonomiczny, naukowy, wojskowy, strategiczny czy inny np. sportowy. Warto jednak pozostać przy terminie wywiad gospodarczy, który jest najstarszym i najbardziej powszechnym terminem, a ponadto obejmuje swoim znaczeniem wszystkie pozostałe określenia.

- budowa, zarządzanie, rozwój komórek i zespołów wywiadowczych,
- budowanie kultury dzielenia się wiedzą w organizacji,
- systemy wczesnego ostrzegania i symulacje typu *war game*,
- kontrwywiad biznesowy,
- metody dziennikarstwa śledczego i analizy śledczej.
- znaczenie, priorytety, korzyści z wywiadu biznesowego,
- prawne i etyczne granice wywiadu biznesowego.

Z powyższego wykazu wynika, że zakres terminologii wywiad biznesowy jest identyczny z terminem wywiad gospodarczy. Zatem terminy te mogą być używane zamiennie. Natomiast eksperci z zakresu tej tematyki powinni znać zagadnienia wywiadu biznesowego: strategii i analiz, marketingu, *public relations*, sprzedaży, rozwoju biznesu, zakupów, inwestycji, fuzji i przejęć, badań i rozwoju produktów i usług, zarządzania ryzykiem, audytu, finansów, kontrolingu, windykacji, zasobów ludzkich oraz pracowników będących etatowymi pracownikami wywiadu biznesowego[233].

Można się jedynie domyślać, ze względu na brak definicji, iż określenie wywiadu z dodatkiem agresywny, może oznaczać szpiegostwo gospodarcze. Ta terminologia ma jedynie związek z kierunkiem zainteresowania. Brak jest natomiast danych co do etyki takiej działalności, pomimo że każdy powinien mieć orientację, iż wywiad gospodarczy opiera się na czynach prawnie dozwolonych, a szpiegostwo gospodarcze wykorzystuje wszelkie możliwe także zabronione środki działania i jest karalny z art. 23 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[234].

Terminy wywiad gospodarczy i szpiegostwo gospodarcze są niejednokrotnie mylone lub stosowane zamiennie. Czynią to nawet tacy eksperci jak agenci CIA w swoich publikacjach[235].

Istnieje jednak przekonanie, że mimo iż działalność komórek wywiadowczych w firmach amerykańskich z reguły uchodzi za etyczną, nie ma zgodności co do tego, kiedy i jak często przedsiębiorcy przekraczają granice przyzwoitości. W kręgu znawców panuje opinia, że operacja wertowania przeznaczonej na śmietnik dokumentacji Microsoftu zlecona przez korporację Oracle to niechlubny wyjątek. Zdaniem ekspertów handlowych, przedsiębiorcy skrupulatnie przeglądają witryny internetowe rywali, a także dokumentację biur patentowych. Czasem jednak posuwają się jeszcze dalej, np. robią zdjęcia konkurencyjnych fabryk. Typowe jest analizowanie Internetu przy wykorzystywaniu nowoczesnego oprogramowania do szybkiego przeszukiwania baz danych, które umożliwia odnalezienie powiązań między strzępami informacji na temat konkurencji.

Od dawna wiadomo, że prawie w każdej dużej amerykańskiej firmie istnieje biuro wywiadowcze. Natomiast duże przedsiębiorstwa z oddziałami w dużym kraju lub za granicą mają oddziały wywiadowcze niemal we wszystkich rozproszonych po całym świecie placówkach zagranicznych. Specjalne zespoły bacznie obserwują rywali, tropią fuzje, podglądają nowe technologie, a nawet analizują morale w firmach, które są ich klientami.

233 www.kozminski.edu.pl/swb/(3.09.2015)

234 T. jedn. Dz. U. z 2003 r. Nr 153, poz. 1503.

235 D.R. Clarridge, *Po prostu szpieg,* Warszawa 2001, s. 340. (Tytuł oryginału: *A Spy for all Seasons. My life in the CIA*).

## 4. Wywiad państwowy a wywiad gospodarczy

Systematycznie rozbudowują się służby wywiadowcze państwowe, a także następuje dalsza profesjonalizacja zespołów wywiadowców gospodarczych. Warto zatem dokonać podstawowej analizy zagadnienia podobieństw i różnic zachodzących pomiędzy siecią wywiadu państwowego a gospodarczego. W wywiadzie państwowym zatrudnieni są oficerowie wywiadu, których podstawową ideą działania jest zasada patriotyzmu. Werbowani mogą być zachęcani obietnicą podróży zagranicznych i emocji związanych z wykonywanymi tajnymi czynnościami wywiadowczymi. Szkolenia wywiadowców państwowych odbywają się w wyspecjalizowanych ośrodkach szkoleniowych, jednakże niektórzy oficerowie są tak zakonspirowani, że odbywają szkolenie w trybie indywidualnym. Ma to na celu zapewnienia im maksymalnego bezpieczeństwa. Natomiast ich działalność polega przede wszystkim na tajnym rozpracowywaniu określonych osób oraz zdobywaniu tajnych materiałów, także o charakterze wojskowym czy obronnym. Lojalność w przypadku wywiadu państwowego obowiązuje wobec państwa i narodu.

Sieć wywiadu państwowego powstaje z mocy ustawy. Najczęściej organizowane są dwie państwowe służby wywiadowcze w zakresie bezpieczeństwa wewnętrznego i zewnętrznego. Przykładowo, w Polsce działają Agencja Wywiadu (AW) i Agencja Bezpieczeństwa Wewnętrznego (ABW) jako służby cywilne oraz Służba Wywiadu Wojskowego (SWW) i Służba Kontrwywiadu Wojskowego (SKW) jako służby wojskowe. Natomiast w Wielkiej Brytanii istnieją trzy główne organizacje wywiadowcze: *Military Intelligence, Departament Five* (MI 5) do spraw kontrwywiadu na terytorium Wielkiej Brytanii; *Military Intelligence, Departament Six* (MI 6), często nazywana Tajną Służbą Wywiadowczą *(Secret Intelligence Service)* zajmująca się szpiegostwem za granicą; i wreszcie Rządowe Centrum Łączności *(Government Communications Headquarters* – GCHQ) odpowiedzialna za zabezpieczenie informacji przeznaczonych dla rządu brytyjskiego oraz przechwytywanie ich z innych krajów. Stany Zjednoczone mogą poszczycić się najpotężniejszymi i największymi budżetami służb wywiadowczych na świecie. Cztery najważniejsze z nich to Centralna Agencja Wywiadowcza (CIA), zajmująca się szpiegostwem za granicą; Agencja Bezpieczeństwa Narodowego (NSA) zajmująca się wywiadem elektronicznym (Elint) oraz łamaniem kodów; Narodowy Urząd Rozpoznania *(National Reconnaissance Office* – NRO) nadzorujący działanie satelitów szpiegowskich oraz Agencja Wywiadowcza Obrony *(Defence Intelligence Agency* – DIA), koordynująca operacje wywiadowcze armii lądowej, marynarki wojennej i sił powietrznych. Kontrwywiadem w USA zajmuje się Federalne Biuro Śledcze (*Federal Bureau of Investigation* – FBI). Francja ma dwie organizacje wywiadowcze: *Direction General de Sécurité Exterieur* (DGSE), zajmującą się – podobnie jak MI 6 i CIA – akcjami szpiegowskimi poza granicami kraju, oraz *Direction de la Surveillance du Territoire* (DST), odpowiedzialną za sprawy kontrwywiadu w kraju. Także Izrael ma dwie organizacje wywiadowcze: *Mossad Le Aliyah Beth* (zajmującą się wywiadem i służbami specjalnymi, a także odpowiedzialną za szpiegostwo za granicą) oraz *Shin Beth* zajmującą się sprawami bezpieczeństwa i kontrwywiadu, odpowiedzialną za bezpieczeństwo w kraju. Natomiast małe państwa mają tylko jedną służbę[236].

236 J. Rusbridger, *Gra wywiadów. Iluzje i pozory szpiegostwa międzynarodowego*, Warszawa 1993, s. 26-50.

Niezbędne jest zwrócenie uwagi na wywiad wojskowy, który ma specyficzne znaczenie obronne. Na podstawie jawnego źródła informacji, jakim jest Raport o działaniach żołnierzy i pracowników b. Wojskowych Służb Informacyjnych oraz wojskowych jednostek organizacyjnych realizujących zadania w zakresie wywiadu i kontrwywiadu wojskowego przed wejściem w życie ustawy z 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych w zakresie określonym w art. 67 ust. 1 pkt 1-10 ustawy z 9 czerwca 2006 r. – Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz ustawę o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego oraz o innych działaniach wykraczających poza sprawy obronności państwa i bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polskiej[237] - można zdecydowanie określić, że w okresie opracowywania wspomnianego dokumentu w wywiadzie wojskowym rozróżniano dwa podstawowe źródła zdobywania informacji i materiałów wywiadowczych, a mianowicie źródła osobowe i bezosobowe. Ze względu na charakter, wspomniane źródła dzielono na oficjalne i nieoficjalne, tajne (poufne) lub jawne.

Do źródeł osobowych zaliczano wszelkie kontakty pracowników kadrowych wywiadu z osobami współpracującymi świadomie lub nieświadomie z wywiadem wojskowym. Prócz agentów i informatorów pozyskanych do współpracy z wywiadem, potencjalnymi nośnikami osobowych źródeł informacji są między innymi: środowiska wojskowe kraju zainteresowania wywiadowczego, urzędnicy instytucji cywilnych, dziennikarze, personel techniczny i administracyjny w przemyśle (głównie zbrojeniowym), handlowcy i inne osoby mające dostęp do informacji interesujących wywiad, a ponadto pracownicy attachatów wojskowych i innych placówek, którymi interesowano się w miarę potrzeb.

Natomiast do źródeł nieosobowych zaliczano przede wszystkim: resortowe i uczelniane biblioteki specjalistyczne, biblioteki publiczne i wojskowe, prasę codzienną, księgarnie ogólne i specjalistyczne (geograficzne, topograficzne, techniczne), pokazy i wystawy wojskowe i ogólne (branżowe), ćwiczenia i manewry wojskowe, pokazy i parady wojskowe, audycje telewizyjne i radiowe, konferencje i sympozja oraz pokazy filmów o tematyce wojskowej.

Cytowane źródło ujawnia sposoby zdobywania informacji i materiałów. Zatem wywiad wojskowy, wykorzystując dostępne mu siły i środki, stosował wówczas różnorodne sposoby zdobywania informacji i materiałów wywiadowczych. Do najczęściej stosowanych sposobów zaliczono:

1. prowadzenie rozmów;
2. obserwację własną;
3. penetrację rynku wydawniczego oraz zakup materiałów i sprzętu objętych embargiem;
4. podsłuch osobisty i przy pomocy urządzeń nagrywających;
5. nasłuch radiowy;
6. kradzieże i wynoszenie tajnych materiałów;
7. fotografowanie obiektów wywiadowczych.

Niektóre wyżej wymienione sposoby zdobywania informacji i materiałów mogą być łączone, na przykład:

237 Zob. http://www.iniejawna.pl/pomoce/przyc_pom/raport.pdf (dostęp: 18.06.2014 r.), s. 260-261.

- prowadzenie rozmów i obserwacja, a także
- obserwacja i fotografowanie obiektów wywiadowczych.

Prowadzenie rozmów określono jako jeden z podstawowych sposobów zdobywania informacji. Sposób ten z reguły stosują wszyscy pracownicy zagranicznego aparatu wywiadowczego, a więc pracownicy kadrowi, współpracownicy, agenci i informatorzy świadomi. Wyniki rozmów zależą od wielu okoliczności, a przede wszystkim od: warunków i sytuacji, stopnia przygotowania wywiadowczego, elokwencji i wiedzy, znajomości danego języka oraz doboru rozmówcy i umiejętności wyboru tematu rozmów itp.

Autorzy cytowanego Raportu podkreślają, że drogą obserwacji własnej można zdobyć wiele interesujących i wartościowych informacji wywiadowczych. Sposób ten stosowany jest przez wszystkich członków zagranicznych ogniw wywiadowczych.

Obserwacja może być prowadzona gołym okiem lub przy użyciu przyrządów optycznych. Prowadzenie obserwacji jest zwykle bezpieczniejsze, niż prowadzenie rozmowy na tematy wojskowe lub odnoszące się do konkretnego obiektu. Obserwacja ma także ujemne strony, gdyż w jej trakcie można ustalić tylko zewnętrzne cechy obiektu lub fragmentaryczne dane jakiegoś zdarzenia (zjawiska), które muszą być potwierdzone przez inne źródła.

Wartość informacji uzyskanych drogą obserwacji zależy przede wszystkich od: należytego przygotowania wywiadowczego i fachowego, umiejętności wykorzystania środków technicznych, warunków terenowych, pory dnia i warunków meteorologicznych oraz od stopnia przygotowania się do wykonania danego zadania.

Obserwację można prowadzić z jednego lub kilku miejsc w terenie, z okna hotelu, wieży obserwacyjnej lub z innego stałego obiektu, z samochodu w ruchu, samolotu komunikacyjnego, pociągu, roweru, statku pasażerskiego, motorówki itp. Ponadto podkreśla się, że penetracja rynku wydawniczego, zakup materiałów i sprzętu objętych embargiem ma duże znaczenie w pracy wywiadowczej.

Zespoły wywiadu gospodarczego zazwyczaj powstają na zapotrzebowanie określonego przedsiębiorcy, w trakcie poszukiwania różnorodnych kontaktów zawodowych, naukowych, osobistych, towarzyskich itp.

Wywiad gospodarczy nie jest rejestrowany z wyjątkiem tych jednostek, które z tego powodu prowadzą działalność gospodarczą. W niektórych krajach działają stowarzyszenia wywiadowców gospodarczych. Różnice wynikające z funkcji i obowiązków wywiadu państwowego i wywiadu gospodarczego opracowali B. Martinet, Y.M. Marti pod koniec XX wieku i z niewielkimi zmianami są aktualne i zamieszczone w poniższej tabeli.

Działalność wywiadowcy gospodarczego jest działalnością jawną, a jego lojalność odnosi się do pracodawcy, zgodnie z postanowieniami umowy o pracę, kodeksem pracy, a także regułami etycznymi obowiązującymi w danej branży.

Podsumowując znaczenie terminu wywiad warto zwrócić uwagę na dwa podstawowe znaczenia tego terminu. W pierwszym oznacza organizację, instytucję najczyściej służbę państwową, zaspokajające istotne, dyktowane racją stanu potrzeby informacyjne władz. Organizacje wywiadowcze, często z dość daleko idącymi analogiami do służb państwowych, tworzą także niektóre przedsiębiorstwa lub ich związki. W znaczeniu drugim termin wywiad oznacza działalność, ukierunkowaną przede wszystkim na pozyskiwanie informacji. Działalność organizacji wywiadowczej może być nasta-

wiona na pozyskiwanie (przetwarzanie, wykorzystywanie) informacji politycznych, wojskowych czy ekonomicznych. Mówimy wtedy o wywiadzie politycznym, wojskowym i ekonomicznym. Dziedziny aktywności wywiadowczej mogą być także określane inaczej, np. terytorialnie lub poprzez wskazanie typu rozpoznawanych obiektów, obszarów czy innych organizacji[238].

**Sieć wywiadowcza państwa a sieć wywiadowcza przedsiębiorstwa**

| **Sieć wywiadowcza państwa** | **Sieć wywiadowcza przedsiębiorstwa** |
|---|---|
| Lojalność wobec państwa | Umowa o pracę<br>Klauzula o zakazie konkurencji |
| Lojalność wobec zwierzchników | Prawo decydowania i zgłaszania sprzeciwu<br>Lojalność podwójna: wobec zwierzchników i partnerów sieci |
| Regulacje państwowe | Reguły klubowe ustalane kolektywnie |
| Działanie nie ograniczane. Racja stanu | Obowiązek przestrzegania norm prawnych i etycznych |
| Logika tajności | Logika komunikacji |
| Staranna selekcja kadr | Nabór przez „dokooptowywanie” |
| Zatrudnianie tajnych informatorów | Klienci, dostawcy, banki, partnerzy i sojusznicy przedsiębiorstwa, naukowcy, eksperci itp. |
| Brak wpływu na sposób wykorzystania informacji | Sprzężenie zwrotne między dostawcą a użytkownikiem informacji |
| Działalność zawodowa na całe życie | Jeden z etapów kariery zawodowej<br>Działalność możliwa do wykonywania w ramach innego zawodu |

Źródło: B. Martinet, Y.M. Marti, *Wywiad ....,* s. 61.

Z punktu widzenia kryminalistyki wywiad to istotna część rozpoznania środowiskowego i osobowego**.** W tym znaczeniu wywiad to operacyjna, czyli pozaprocesowa metoda uzyskiwania informacji podczas prowadzenia rozmowy z inną osobą.

Uzyskiwanie wiadomości może zostać przeprowadzone w sposób jawn**y** lub ukryty tak, że udzielający odpowiedzi nie będzie wiedział kim jest interlokutor, a tym bardziej jaki jest cel tej konwersacji.

Najczęściej w działalności wywiadowczej wykorzystywane są jawne informacji, czyli takie, które nie są chronione przez dysponenta, mamy wówczas do czynienia z tzw. wywiadem „białym**”.** Jeżeli w toku działań wywiadowczych dociera się do źródeł niejawnych, czyli chronionych przez ich posiadacza i stosuje się metody nielegalne w świetle obowiązującego prawa, mamy wówczas do czynienia z wywiadem „czarnym” czyli szpiegostwem. Jednakże J. Konieczny, znakomity znawca przedmiotu podkreśla: *doświadczenie uczy, że praktyka wywiadowcza, przybierając czasem czystą biel lub czystą czerń występuje także we wszystkich możliwych odcieniach szarości, znajdujących się pomiędzy wspomnianymi biegunami[239].*

238 J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu* , Warszawa 2004, s. 145, 146.
239 Tamże, s. 146.

W celu uzyskania obiektywnych lub potwierdzonych informacji w ramach wywiadu pomocna może być obserwacja. Ten rodzaj rozpoznania jest często stosowany w działaniach kryminalistycznych.

Obserwacja to taka koncentracja uwagi na określonym miejscu, rzeczy lub osobie, która prowadzona jest najczęściej w celu dokonania rozpoznania badanego zjawiska lub zapewnienia ochrony wskazanemu obiektowi. Według Wikipedii obserwacja naukowa to proces uważnego i celowego spostrzegania; rezultatem obserwacji naukowej są spostrzeżenia naukowe. Wartość poznawcza metody obserwacyjnej polega na opisie zjawisk, od którego często zaczynają się badania naukowe[240].

Realizowanie różnorodnych form obserwacji prawie najczęściej wymaga posługiwania się wyspecjalizowanym sprzętem wspomagającym – kamerą, noktowizorem, termowizją i innymi środkami technicznymi.

W definicji wywiadu państwowego należy rozumieć szereg różnych stanowisk, które zajmują osoby związane z tą służbą realizując zadania różnorodne, typowe dla tych służb, a przykładowo:

- oficerowie wywiadu, tj. funkcjonariusze działający niejawnie,
- sieć agentów, tj. funkcjonariuszy na etacie, działających pod przykrywką (z fikcyjną tożsamością), czy
- sieć tajnych współpracowników działających w konspiracji.

## 5. Poglądy na definicje i formy wywiadu gospodarczego

Termin ten jest trudny do zwięzłego określenia, albowiem zarówno wywiad gospodarczy, jak i kontrwywiad gospodarczy obejmują interdyscyplinarną problematykę z przewagą zarządzania, administracji, różnych dziedzin prawa, ekonomii, finansów, socjologii, psychologii, kryminologii, kryminalistyki, informatyki, a także etyki i bezpieczeństwa biznesu.

Zdefiniowanie wywiadu gospodarczego przynosi istotne trudności nie tylko metodyczne, lecz również terminologiczne dotyczące jego zakresu. Zatem według najpopularniejszego źródła informacji, Wikipedii, wywiad gospodarczy to działania zmierzające do uzyskania informacji o innych podmiotach gospodarczych zgodnie z prawem, ze źródeł ogólnie dostępnych np. rejestrów sądowych i ewidencji przedsiębiorstw, publikatorów urzędowych, prasy, katalogów branżowych itd.[241] Definicja może być zatem związana z kierunkiem zainteresowań badawczych.

Według T. Wojciechowskiego *wywiad gospodarczy to profesjonalne zdobywanie i analizowanie informacji o określonych segmentach rynku, funkcjonujących na tym rynku podmiotach, ich osiągnięciach technicznych, projektach działań i pozycji ekonomicznej*[242]. Profesjonalna metodyka działania pozwala na zdobycie takich informacji, które mogą służyć zleceniodawcy do sprecyzowania strategii postępowania przedsiębiorstwa, koncernu, a w niektórych przypadkach, państwa w uzyskaniu lub utrwaleniu jego wpływów na danym rynku. W swoim działaniu wywiad gospodarczy posługuje się określonymi formami, metodami i środkami dla uzyskania niezbędnych informacji, zgodnie z obowiązującym stanem prawnym.

240 https://pl.wikipedia.org/wiki/Obserwacja_(metoda_badawcza)(5.08.2015)
241 http://pl.wikipedia.org/wiki/Wywiadownia_gospodarcza(30.12.2011)
242 T. Wojciechowski, *Wywiad gospodarczy*, Firma 1991, nr 7 – 8.

Według rozszerzonej definicji Francuskiego Generalnego Komisariatu do Spraw Planowania Gospodarczego wywiad gospodarczy (ang. *Competitive Intelligence*) to zespół działań polegających na poszukiwaniu (gromadzeniu), przetwarzaniu i rozpowszechnianiu (w celu wykorzystania) informacji przydatnej podmiotom gospodarczym, prowadzony zgodnie z prawem, z zachowaniem wszelkich możliwych gwarancji niezbędnych dla ochrony zasobów (majątku) przedsiębiorstwa. Z rozpowszechnianiem informacji wiąże się podejmowanie pewnych działań (aktów oddziaływania) mających na celu wpływ na otoczenie przedsiębiorstwa (np. konkurencyjne, prawne), które zbliżone są do powszechnie pojmowanego lobbingu[243].

M. Kwieciński zauważa, iż współczesne rozumienie nazwy „wywiad gospodarczy" dotyczy zasadniczo jednego z instrumentów zarządzania przedsiębiorstwem zwłaszcza zaś w przedmiocie zwiększenia jego konkurencyjności. Stosowanie tego określenia rozpoczęto z początkiem lat osiemdziesiątych XX wieku. Zresztą w różnych formach pokrewnych (wywiad organizacyjny, wywiad konkurencyjny, wywiad marketingowy, itd.).

Szeroka definicja pozwala na niemal całkowite ujęcie tego terminu. Zatem *wywiad gospodarczy jest zespołem działań polegających na uzyskiwaniu, przetwarzaniu i wykorzystywaniu informacji przydatnych organizacjom gospodarczym. Jego zadaniem jest rozpoznawanie rynków, metod analizowania konkurencji i partnerów, rozpoznawania ich kultury, zamierzeń i zdolności ich realizacji, Jako podstawowe funkcje wywiadu gospodarczego wylicza się: identyfikację w ramach działania w otoczeniu przedsiębiorstwa, analizowanie zagrożeń i szans rozwoju, doskonalenie firmowego dorobku naukowego, technicznego, technologicznego i organizacyjnego*[244].

Szczegółowe definiowanie zasad wywiadu gospodarczego, *Business Intelligence* – BI (wywiadu biznesowego), który jak powszechnie wiadomo jest istotnym elementem zarządzania strategicznego organizacji oraz *Competitive Intelligence* (wywiadu konkurencji) wymaga dalszych badań, które przekraczają ramy tego opracowania. Niezbędne jest jednak przytoczenie określenia *Business Intelligence* według Benjamina Gilada, a mianowicie: *Efektywna analiza konkurencji powinna polegać na próbie wczesnego odczytywania trendów i zmian na rynku, spełniać funkcje wczesnego ostrzegania. Nie może ona zapobiec niespodziewanemu wprowadzeniu nowego produktu, pojawieniu się nowego konkurenta, przejęciu, wykupieniu lub innym strategicznie istotnym ruchom na rynku, które były skrzętnie ukrywane przed opinią publiczną. Ze względu na to, że BI nie używa metod szpiegowskich jest karygodnym oczekiwać, że będzie przewidywała te specyficzne wydarzenia. (...) Efektem pracy komórki BI są przypuszczenia co do oczekiwanych zmian, kreślenie możliwych scenariuszy, przewidywanie kolejnych kroków, ale nie konkretnych decyzji*[245]. Ten autor określił cele *Business Intelligence* jako:

1. zwiększenie i zabezpieczenie udziału w rynku,
2. poznanie sił i słabości konkurencji, a szczególnie analiza tych elementów, które świadczą w czym konkurencja jest lepsza i jakie posiada w tym względzie wartości,

243 Euvre collective du Commissariat General du Plan, *Intelligence Economique et strategie des entreprieses,* La Documentation Francaise, Paris 1994. (Cytuję za M. Kwiecińskim, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa, Kraków 1999, s. 30 i 160.)

244 M. Kwieciński, *Wywiad gospodarczy, wyd. cyt.,* s. 29-31

245 B. Gilad, *Business Intelligence System: A New Tool for Competitive Advantage, Amazon 1988*, s. 19.

3. przygotowanie na ewentualne niespodzianki,
4. uczenie się od konkurencji, gdyż jest to najtańsza metoda zdobywania wiedzy[246].

W tym omówieniu brakuje jednakże problemu rozpoznawania, prognozowania i zasad działania w trakcie sytuacji kryzysowej, która niejednokrotnie związana jest zarówno z prowadzeniem biznesu, jak i działaniami w ramach wywiadu gospodarczego czy kontrwywiadu gospodarczego..

Można przyjąć na potrzeby tej pracy, że wywiad gospodarczy to takie złożone, korzystne i prawne działanie na rzecz przedsiębiorstwa, które angażuje specjalistów posiadających odpowiednie kwalifikacje. Jednym z podstawowych zadań sprawnie funkcjonującej jednostki wywiadu gospodarczego jest ochrona informacji strategicznych przedsiębiorstwa, czyli profesjonalna działalność kontrwywiadowcza.

## 6. Kierunki i rodzaje wywiadu gospodarczego

Na szczególną uwagę zasługują działania i osiągnięcia wywiadu gospodarczego, zwany niekiedy wywiadem konkurencji, który określany jest jako pozyskiwanie informacji na temat gospodarki przedsiębiorstw i państw. Polega on przede wszystkim na uzyskiwaniu lub potwierdzaniu informacji dotyczących sytuacji prawnej i finansowej wybranych przedsiębiorstw na zlecenie innych podmiotów gospodarczych w celu zmniejszenia ryzyka współpracy gospodarczej lub też dla podjęcia odpowiednich kroków dla odzyskania należności.

Wywiad gospodarczy, którym zajmują się wyspecjalizowane biura detektywistyczne czy firmy, w szczególności firmy windykacyjne, a także analitycy informacji gospodarczych i finansowych zatrudniani przez konsorcja przemysłowe, może być skierowany zarówno na firmy, jak i na osoby prywatne w zakresie pozyskiwanie informacji na temat gospodarki przedsiębiorstw i państw.

Przedmiotem zainteresowań wywiadu gospodarczego są najczęściej:

1. dane dotyczące działalności firmy, jak np.: bilanse, zyski, kredyty i wierzytelności,
2. rachunki bankowe i prowadzone na nich operacje,
3. rodzaje transakcji, listy klientów, listy dostawców i odbiorców;
4. zakres i rodzaje produkcji czy usług;
5. wyniki badań, wynalazki produkcyjne, wszelkie dane na temat postępu naukowo-technicznego i rozwoju przedsiębiorstwa;
6. prognozy oraz plany na przyszłość.

Podstawowym zakresem zainteresowania wywiadu gospodarczego jest zdobywanie informacji gospodarczej, jak np. o nowych technologiach wdrażanych w firmach konkurencyjnych, w celu podjęcia kroków prewencyjnych dla zachowania lub uzyskania odpowiedniej, czyli konkurencyjnej, pozycji rynkowej.

Niezbędne jest akcentowanie różnic pomiędzy dwoma niejednokrotnie mylonymi pojęciami. Wywiad gospodarczy należy odróżnić od szpiegostwa, przez które rozumie się próbę uzyskania dostępu do tajnych informacji przy użyciu prawnie niedozwolonych środków. Jednakże informacje pozyskiwane przez wywiad gospodarczy mogą

246 Takie cele BI podkreśla już od dawna wielu autorów. Por.: T. Majcherek, *Cele i zadania oraz metody pracy komórek wywiadu gospodarczego*. Referat wygłoszony na konferencji pt. Wywiad gospodarczy. Teoria i praktyka. Warszawa dnia 30 września 1999 roku.

być również wykorzystywane przez wywiady różnych krajów zarówno w celach gospodarczych, jak i wojskowych w celu zmniejszenia ryzyka współpracy gospodarczej lub też dla podjęcia odpowiednich kroków dla odzyskania należności[247].

Należy jednak mieć na uwadze, że wywiad gospodarczy zajmuje się zbieraniem i gromadzeniem, a także analizowaniem informacji, które cechuje walor aktualności. Oznacza to zbieranie danych o faktach, wydarzeniach, planach i zamierzeniach określonych organizacji np. konkurencyjnych firm. Celem tego działania jest przede wszystkim wnioskowanie na podstawie zebranych danych. Uzyskane informacje dostarczane są własnemu kierownictwu (firmy, koncernu) w celu czasowego wyprzedzenia konkurencji w podejmowaniu optymalnych decyzji gospodarczych.

Już w latach 80. XX wieku Amerykanie uważali, że słowo *competitive,* czyli konkurencja, obejmuje szeroko rozumianą działalność wywiadowczą, umożliwiającą zainteresowanemu przedsiębiorstwu podejmowanie odpowiednich przedsięwzięć w celu zdobycia przewagi konkurencyjnej. Z tego względu niektórzy posługują się terminem wywiad konkurencji. Różne źródła wskazują, że wszelkie formy konkurencji i wywiadu gospodarczego stosowano już w starożytności.

Współczesna sytuacja ekonomiczna oraz niektóre efekty rozpoznania światowych służb specjalnych wyraźnie wskazują, że aktualne zagrożenia powodowane są niezwykle aktywnymi działaniami wywiadów gospodarczych na tle walki konkurencyjnej czy zmowy cenowej.

Wywiad gospodarczy według Wikipedii to pozyskiwanie informacji na temat gospodarki przedsiębiorstw i państw. Polega na uzyskiwaniu, przetwarzaniu i udostępnianiu informacji dotyczących sytuacji prawnej, kadrowej, handlowej, finansowej i ekonomicznej przedsiębiorstw, na zlecenie innych podmiotów gospodarczych w celu szacowania ryzyka współpracy, zdobywania przewagi konkurencyjnej i unikania strat lub odzyskiwania należności. Termin wywiad gospodarczy jest często niesłusznie utożsamiany z pojęciem szpiegostwo gospodarcze" lub kojarzony z tajnymi działaniami służb państwowych.

W polskim języku biznesowym zaczęto stosować dosłowne tłumaczenia nazw angielskich lub francuskich, choć często oznaczają one odmienne formy zdobywania i przetwarzania informacji mających znaczenie biznesowe. Wśród odmian pojęcia wywiad gospodarczy" najczęściej wymienia się:

*Competitive Intelligence,* czyli wywiad konkurencyjny, koncentruje się głównie na pozyskiwaniu, analizowaniu i przekazywaniu informacji o konkurencji i wszelkich możliwościach dotyczących jej funkcjonowania *na rynku, a zwłaszcza jej produktach i klientach. Terminem pochodnym do Competitive Intelligence* jest

Market Intelligence (wywiad rynkowy) ukierunkowany jednak na badanie rynku i aspektów konkurencyjnych 4P marketingu mix (tj. produkt, cena, promocja, miejsce; ang. *product, price, place, promotion*).

Business Intelligence, ewoluując z systemów wspomagania decyzji z lat 60. XX w, jest obecnie zestawem określonych metod i procesów, które przy pomocy technologii informatycznych przekształcają różnorodne dane ilościowe w użyteczne informacje, wykorzystywane w celu skuteczniejszego podejmowania decyzji strategicznych i operacyjnych. Z Business Intelligence związane są bezpośrednio terminy, *data mining*, hurtownie danych, *benchmarking*, *dashboards*, KPI oraz analityka predyktywna i proskrypcyjna.

247 Por. http://pl.wikipedia.org/wiki/Wywiad_gospodarczy(14.12.2011)

*Economic Intelligence* dotyczy procesów zarządzania zdobytymi informacjami ekonomicznymi w makro skali, co oznacza zrozumienie przepływu zasobów finansowych i niefinansowych wewnątrz danych krajów lub globalnych organizacji, polityki reinwestowania i prowadzenia inwestycji zagranicznych oraz zasobów i zdolności produkcyjnych, a także innych kwestii, które mogą wyjaśniać możliwości do produkcji aktywów.

*Due Diligence* (dosłownie: należyta staranność) stanowi zespół kompleksowych i pogłębionych analiz danego podmiotu gospodarczego z dostarczonych uprzednio informacji, pod względem jego sytuacji prawnej i podatkowej, zarządzania strukturą organizacji i kapitałem ludzkim, potencjału technologicznego oraz kondycji handlowej i finansowej w celu identyfikacji ryzyk i możliwości, przed podjęciem negocjacji związanych z transakcją kapitałową, np. przed podpisaniem umowy przejęcia przedsiębiorstwa.

*Commercial Intelligence* – wywiad handlowy lub komercyjny, jest najstarszą i najbardziej zaawansowaną oraz wszechstronną formą legalnego i oficjalnego zbierania, analizy i udostępniania informacji o podmiotach gospodarczych, ich działalności oraz funkcjonowaniu w otoczeniu, w tym informacji o konkurencji i kondycji handlowej, sytuacji prawnej i powiązaniach, a także innych danych, istotnych dla działalności gospodarczej.

Jak wynika z powyższych definicji, *Business Intelligence*, *Economic Intelligence* i *Due Diligence*, nierzadko tłumaczone jako wywiad gospodarczy (biznesowy lub ekonomiczny), nie są ściśle rozumianym wywiadem gospodarczym, lecz analityką biznesową, ekonomiczną, finansową, prawną, itp. *Competitive Intelligence* jest natomiast rodzajem wywiadu, w którym najłatwiej można przekroczyć granicę pomiędzy legalnymi i etycznymi działaniami a szpiegostwem gospodarczym.

Wywiadem gospodarczym zajmuje się wiele podmiotów gospodarczych i zapewne osób fizycznych. Najczęściej wymienia się wyspecjalizowane wywiadownie gospodarcze, a także firmy detektywistyczne czy windykacyjne. Informacje pozyskiwane przez wywiad gospodarczy mogą być również wykorzystywane przez wywiady różnych krajów np. w celach wojskowych[248].

Chociaż dostrzegane są istotne problemy w zdefiniowaniu wywiadu gospodarczego, to jednak panuje względna zgoda co do tego, że można dobrze określić jego zalety funkcjonalne dla wewnętrznych potrzeb przedsiębiorstwa. Zatem wywiad gospodarczy można pojmować jako:

1. dyscyplinę naukową – dziedzinę badawczą,
2. nową dziedzinę biznesu;
3. praktyczne działanie – zespół działań, proces wykonywania następujących po sobie czynności, dostarczający wiarygodną i rzetelną informację;
4. narzędzie zarządzania – narzędzie wzrostu konkurencyjności, element wczesnego ostrzegania, funkcję organizacyjną, system informacji, środek wspomagania decyzji;
5. przydatną informację – produkt procesu wywiadowczego;
6. klucz do sukcesu i dominacji firmy nad konkurencją[249].

248 http://pl.wikipedia.org/wiki/Wywiad_gospodarczy(25.03.2015)

249 http://www.ujk.edu.pl/infotezy/ojs/index.php/infotezy/article/view/16/40(25.03.2015)

Przedsiębiorstwo czy organizacja może prowadzić, w zależności od tematyki pozyskiwanych informacji i jej przeznaczenia, wywiady o: klientach, personelu, strategii marketingowej, badaniach, sprzedaży, produktach, usługach, promocji, dystrybucji, cenach, Internecie. A ponadto zajmować może się wywiadem: naukowo-technicznym (dla rozwoju badań naukowych), technologicznym (rozwój nowoczesnych technologii), konkurencyjnym (podnoszenie wartości przedsiębiorstwa), strategicznym (planowanie strategii przedsiębiorstwa), finansowym (kapitał i akcje), handlowym, medialnym itp.[250]

Najważniejszym celem zbierania informacji gospodarczych jest zdobycie danych o nowoczesnych technologiach oraz szybkie ich wdrożenie w cykle produkcyjne. Odmienne natomiast są zadania wywiadu ekonomicznego, zwanego czasami wojskowym, który rozpoznaje potencjał ekonomiczny określonego państwa, czy organizacji i jego wpływu na możliwości obronne kraju.

Stosowanym terminem, posiadającym swoje zaplecze prawne i naukowe, jest penetracja rynków zagranicznych. Określając schematycznie uwarunkowania strategiczne dotyczące penetracji rynków najczęściej odnosi się je do marketingowego systemu informacji, które ogólnie rzecz biorąc pochodzą ze źródeł o charakterze czynników wewnętrznych i zewnętrznych[251]. Zatem czynniki wewnętrzne są związane z różnymi zasobami organizacji, na przykład: rzeczowymi, finansowymi, ludzkimi. Istnieją w postaci raportów, sprawozdań, informacji o zamówieniach, sprzedaży, cenach itp. Wśród czynników zewnętrznych wyróżnić należy ekonomiczne (rynkowe), technologiczne, prawne i kulturowe. Funkcjonują one przede wszystkim w postaci informacji o konkurentach (producentach tych samych lub substytucyjnych produktów), rynkach zaopatrzeniowych (konkurencyjnych), konsumentach (ich przyzwyczajeniach, stylu życia) nabywcach instytucjonalnych (przyjętych przez nich strategiach i planowanych technologiach), kooperantach, polityce kredytowej (banków i ich produktów, form działalności) oraz polityce państwa.

Funkcje penetracji rynków, bez względu na to czy są to rynki krajowe czy zagraniczne, określa się jednoznacznie jako:

- ukierunkowujące zainteresowania (np. określonym rynkiem, branżą, firmą, organizacją, towarem);
- informacyjne w zakresie uzyskiwania danych o interesujących zdarzeniach czy zjawiskach, występujących na rynku lub dotyczące określonych osób;
- weryfikujące zasoby wiedzy o zaistniałych zdarzeniach lub posiadanych informacjach, co umożliwia podjęcie trafnej decyzji, w zakresie wiarygodności danych o kliencie, na przykład zwiększenia zaufania do klienta czy odmowy współpracy z nierzetelną firmą;
- ochronne i zabezpieczające w odniesieniu do własnej firmy czy konkretnego zdarzenia, np. umowy czy kontraktu, a w tym również ochrony tajemnicy produkcji, tajemnicy przedsiębiorstwa, tajemnicy handlowej lub danych marketingowych.

Wszystkie powyższe funkcje przydatne są w zbieraniu informacji przez wywiad gospodarczy lub w działaniach kontrwywiadowczych. W tym zagadnieniu brakuje jednakże problemu rozpoznawania, prognozowania i zasad działania w trakcie sytuacji

250 A. Moryś, *Geneza i ewolucja wywiadu gospodarczego*. Część pierwsza http://www.ujk.edu.pl/infotezy/ojs/index.php/infotezy/article/view/15/33(25.03.2015)

251 E. Cilecki, *Penetracja rynków zagranicznych. Wywiad zagraniczny*, Warszawa 1997, s. 12, 13.

kryzysowej, która niejednokrotnie związana jest zarówno z prowadzeniem biznesu, jak i działaniami w ramach wywiadu gospodarczego czy kontrwywiadu gospodarczego.

Trudno dokładnie określić, jakie są rodzaje, czy jak sklasyfikować wywiad gospodarczy. Wielu specjalistów mówi o wywiadzie gospodarczym nazywając go wywiadem o konkurentach, konkurencji lub konkurencyjnym. Inni mówią o wywiadzie ekonomicznym, a jeszcze inni uznają wywiad gospodarczy jako ogół, a w nim wywiad konkurencyjny, wywiad ekonomiczny, wywiad przemysłowy lub technologiczny. W podgrupach tych rozróżniają następnie między innymi wywiad o produktach/usługach, wywiad o strategii marketingowej, wywiad o personelu, wywiad finansowy, wywiad o promocji, wywiad o cenach, a także wywiad o klientach, wywiad o Internecie, wywiad w zakresie benchmarkingu i inne[252]. Jak widać, w stosunkowo młodej dziedzinie, jaką jest wywiad gospodarczy, trudno mówić o jednolitym nazewnictwie. wszystko zależy od autorskiego ujęcia.. Jednakże działania profesjonalnego wywiadowcy gospodarczego, pozostają takie same, bez względu na to, która z przedstawionych nazw została użyta.

A zatem wywiad ogólnie dzieli się na bardziej szczegółowe rodzaje:

1) ze względu na podmioty realizujące czy pole zainteresowania:
   - wywiad państwowy – stosowany przez i na zlecenie danego państwa w celach obronnych;
   - wywiad niepaństwowy – stosowany przez inne podmioty (np. przedsiębiorstwa) w celach komercyjnych i w odpowiedzi na ich prywatne potrzeby;
2) ze względu na zakres zainteresowań:
   - **w**ywiad wszechstronny, który stale i szeroko kontroluje i analizuje aktualną sytuację, konkurencję, itp. Jako wszechstronny, czyli nie ma zdefiniowanych potrzeb i kierunków informacyjnych;
   - wywiad ukierunkowan jest wyraźnie określony na konkretne i potrzebne informacje;
3) ze względu na metody pozyskiwania informacji, czyli:
   - **w**ywiad biały, który polega na zdobywaniu informacji w sposób całkowicie jawny. Nie dotyczy informacji tajnych, poufnych i chronionych w inny sposób;
   - wywiad czarny jest przeciwieństwem wywiadu białego i może być zdefiniowany jako szpiegostwo. Polega na gromadzeniu informacji chronionych i wykorzystuje się do tego celu wszystkie możliwe środki, a w szczególności nielegalne czynności operacyjne. Takie czynności mogą być wykonywane jedynie przez policję i służby specjalne w ramach prawem przewidzianej procedury.

W obrębie wywiadu państwowego można wyróżnić:

- wywiad polityczny – zdobywanie informacji politycznych dotyczących obcego kraju, np. ukształtowanie i struktura stronnictw partyjnych, rozkład stanowisk rządowych, osoby przywódców politycznych, podatność na propagandę itp.;
- wywiad wojskowy – zdobywanie informacji dotyczących bezpieczeństwa militarnego danego kraju, jak np. organizacja, uzbrojenie, liczba i rodzaj wojsk, struktura

252 M. Kwieciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa, Kraków 1999, s. 29, 30.

sił zbrojnych, stan i proces modernizacji, osiągnięcia naukowe w dziedzinie obronności itp.;

- wywiad naukowo-techniczny – zdobywanie informacji oraz dokumentacji z zakresu światowych osiągnięć naukowo-technicznych, np. nowy sprzęt, wynalazki, nowe technologie, badania naukowe, badania farmaceutyczne itp.;
- wywiad ekonomiczny – zdobywanie informacji o potencjale gospodarczym danego państwa, np. zasoby surowców, słabe punkty, możliwość nacisku gospodarczego, produkcja, dystrybucja, poziom konsumpcji itp.;
- wywiad gospodarczy – zdobywanie informacji o krajowych i zagranicznych podmiotach gospodarczych, np. dane handlowe i techniczne, sytuacja prawna i finansowa, produkcja, sposoby dystrybucji, technologia, struktura, pracownicy itp.[253]

Wywiad gospodarczy stosowany przez przedsiębiorstwa prowadzony jest na mniejszą skalę niż wywiad państwowy (w tym wywiad gospodarczy państwowy). Wywiad gospodarczy przedsiębiorstw koncentruje się przede wszystkim na otoczeniu (rynek, trendy, konkurenci, konsumenci, dostawcy itp.), w którym dana firma funkcjonuje i prowadzi działania wywiadowcze mając na uwadze aktualne potrzeby i cele.

Bez względu na rodzaj wywiadu gospodarczego jest to przede wszystkim:

1) szeroki proces pozyskiwania, gromadzenia, a także przetwarzania i rozpowszechniania informacji;
2) ukierunkowane podejmowanie przedsięwzięć mających na celu wywieranie wpływu na otoczenie dla realizacji strategicznych planów własnego przedsiębiorstwa;
3) wydawanie zdecydowanej walki ze szpiegostwem gospodarczym.

Planowanie rodzaju zastosowania wywiadu zależy przede wszystkim od określonych potrzeb przedsiębiorstwa. Brak właściwego planowania dezorganizuje pracę komórki wywiadowczej i niejednokrotnie nie jest ona w stanie właściwie spełniać swoich zadań, które polegają przede wszystkim na wyprzedzeniu konkurencji. Natomiast dobrze zaplanowane i profesjonalnie wykonane działania doprowadzą do zarówno do sukcesu, jak i wielu oszczędności.

M. Kwieciński podkreśla, że nie zawsze powinien być stosowany niezwykle pracochłonny wywiad wszechstronny, a raczej należy wykorzystywać działania ukierunkowane (wywiad ukierunkowany na określone zagadnienie), czyli takie, które polega na dokładnym określeniu poszukiwanego celu[254]. Zatem kwestią kluczową pozostaje właściwe sformułowanie pytań przez zleceniodawcę, a przykładowo:

- klarownie i zrozumiale określenie i uzasadnienie poszukiwanych informacji. Niejednokrotnie sprzyja to na doprecyzowanie badanej sytuacji;
- sformułowanie potrzeby informacyjnej w postaci konkretnego pytania;
- sformułowane pytanie musi być nie tylko precyzyjne, ale także specyficzne (np. kto w miejscowości A będzie naszym konkurentem?);
- trzeba określić znaczenie informacji, którą chce się uzyskać. Czy oczekuje jej przełożony? Czy wiąże się z nowym i ważnym projektem? co już wiadomo na ten temat?;
- warto określić przypuszczalne prawdopodobieństwo uzyskania trafnej odpowiedzi na zadany problem.

253 A. Moryś, *Geneza i ewolucja wywiadu gospodarczego*. Część pierwsza http://www.ujk.edu.pl/infotezy/ojs/index.php/infotezy/article/view/15/33

254 Szerzej: M. Kwieciński, *Wywiad gospodarczy…,* s.35-38.

- jeśli zatrudnieni będą podwykonawcy należy dopilnować, aby pytania nie zostało zniekształcone;
- trzeba upewnić się, czy istotą badań jest informacja czy jej źródło. Najlepiej osobiście korzystać z dostępnych źródeł[255].

Każdy rodzaj stosowanego wywiadu gospodarczego wymagać może rutynowych oraz specjalistycznych działań kontrwywiadowczych o charakterze tajnym, jak i jawnym. Przykładem mogą być działania prowadzone przez państwowy wywiad naukowo-techniczny, który jak dość powszechnie wiadomo w latach 70. i 80. XX wieku intensywnie wspomagał polską gospodarkę w wielu dziedzinach, a szczególnie w zakresie informacji o różnorodnych nowoczesnych technologiach stosowanych w krajach zachodnich. Przedsięwzięcia kontrwywiadowcze mogą dotyczyć ochrony własnych technologii i wynalazków, jak i zdobytych w innych krajach czy przedsiębiorstwach.

Praktycy ze służb wywiadowczych wielu krajów dysponują w tej mierze wieloma przykładami, o których w zasadzie milczy literatura przedmiotu.

Przykładem celowości działań kontrwywiadowczych mogą być skutki wizyty kontrahentów zagranicznych w jednej z polskich fabryk; ta wizyta doprowadziła do rozpoznania przez jednego z gości najnowszej technologii strzeżonego produktu, który był akurat na taśmie produkcyjnej. Następnie okazało się, że zagraniczne służby intensywnie szukały sposobu zdobycia tej strzeżonej wciąż technologii[256].

Nie tylko wywiadowca, czy analityk informacji, lecz również przeciętny obserwator dostrzega, że wszelkiego rodzaju wywiady i służby specjalne najbardziej są zainteresowane nowoczesną technologią i wszelkiego rodzaju wynalazkami.

## 7. Wywiad gospodarczy jako zjawisko o charakterze ponadnarodowym

W ostatnich latach wyraźnie uwidacznia się różnica wpływów i interesów instytucji oraz wielkich organizacji w różnych państwach. Skutkuje to m.in. działaniami wywiadowczymi o charakterze gospodarczym. W związku z tym na światowych rynkach dostrzegamy następujące zjawiska:

- w polityce wielu państw dominuje preferowanie, a nawet nasilanie działalności wywiadowczej o charakterze ekonomicznym;
- niektóre organizacje gospodarcze nie szczędzą nakładów i wysiłków w celu zdobywania nowych technologii czy licencji w sposób nieoficjalny, a ponadto nieuczciwie je rozpowszechniają poprzez piractwo itp.;
- ukierunkowanie organizacji gospodarczych na działalność wywiadowczą uwarunkowane jest wieloma czynnikami. Jednakże wyczerpujące przedstawienie i uzasadnienie tego problemu byłoby możliwe dopiero po przeprowadzeniu złożonych badań socjokryminologicznych;
- polskie organizacje gospodarcze, nie tylko przemysłowe, również finansowe, są poddawane różnorodnym działaniom i naciskom w celu wyparcia ich z rynku. Podobne tendencje uwidaczniają się w stosunkach pomiędzy niektórymi znaczącymi firmami polskimi;
- polskie organizacje gospodarcze, finansowo-bankowe, handlowe i inne są zmuszo-

255 Szerzej: A.P. Garrin, R. Berkman, *The Art of Being Well Informed*, New York 1996, 23-32.

256 K. Dubiński. I. Jurczenko, ***Być szpiegiem*****,** Warszawa 1994, s. 24-25.

ne do zaostrzenia zasad bezpieczeństwa związanego z ochroną swoich interesów. Nie budzi również wątpliwości teza, że działania te wymagają obecnie najwyższego profesjonalizmu;

- niezwykle opłacalne stają się inwestycje biznesowe związane z przygotowywaniem profesjonalistów organizujących wywiad gospodarczy[257].

Gospodarka rynkowa, obok wielu pozytywnych elementów, zniosła również monopol na naukę i praktykę w dziedzinie wywiadu czy kontrwywiadu gospodarczego. W rywalizacji wolnorynkowej w zasadzie każda informacja o konkurencji, o produktach czy usługach, o nowym rodzaju działalności, które w powiązaniu z wieloma elementami dotyczącymi możliwości i potrzeb własnej firmy – posiada niezwykle istotne znaczenie. Wszystkie one wzbudzają czyjeś zainteresowanie nie tylko z marketingowego czy handlowego punktu widzenia.

Zasadne są rozważania na temat uwarunkowań i czynników, które przyczyniły się do powstania i rozwoju wywiadu gospodarczego, zarówno w Polsce jak i na świecie. Są to przede wszystkim:

- technologia – wykorzystywana jest na każdym etapie procesu wywiadowczego. Postęp technologiczny w dziedzinie technologii informacyjnych (IT), mediów elektronicznych, systemów transmisji danych itp. usprawnił metody gromadzenia, przetwarzania, udostępniania i ogólnego operowania informacją;
- społeczeństwo informacyjne – podniosło rangę i zagwarantowało dostęp do informacji. Państwo, które dąży do osiągnięcia statusu społeczeństwa informacyjnego musi się rozwijać m.in. technologicznie, dzięki czemu dostarcza wywiadowi gospodarczemu środków, by ten mógł być prawidłowo realizowany;
- rynek informacji – umożliwia handel informacją co jest źródłem utrzymania wywiadowni gospodarczych, a także pozostałych podmiotów oferujących dostęp do niej. Bez rynku ogólnodostępnych informacji legalne ich pozyskiwanie nie byłoby możliwe, a wywiad gospodarczy straciłby sens na rzecz szpiegostwa;
- demokracja – odpowiedni ustrój polityczny gwarantuje swobodę, wolność słowa i dowolność działania. Państwo poprzez odpowiedni system prawny gwarantuje obywatelom m.in. dostęp do informacji publicznej, daje możliwości i określa granicę działania wywiadowców gospodarczych;
- kapitalizm – przejście z gospodarki planowanej na rynkową otworzyło drogę inwestorom, przedsiębiorcom i zainicjowało konkurencję – w monopolu, gdy przedsiębiorstwa nie rywalizują, informacje wywiadowcze są zbędne[258].

We współczesnym biznesie jest czymś oczywistym wcześniejsze rozpoznanie partnera transakcyjnego. Zwykle już w negocjacjach okazuje się, że konkurencja jest dobrze przygotowana do trudnych rozmów, dysponując np. pełną wiedzą o najważniejszych członkach zarządu spółki, z którą planuje współpracę. Tak więc znane są nie tylko nazwiska partnerów, lecz również ich życiorysy i zainteresowania. Najczęstsza jest znajomość rodzajów i form produkcji, rodzaju wyposażenia i ostatnio zawartych kontraktów

257 J.W. Wójcik, *Wywiad gospodarczy a prawna ochrona informacji*, Warszawa 2000, s. 9.

258 A. Moryś, *Geneza i ewolucja wywiadu gospodarczego.* http://www.ujk.edu.pl/infotezy/ojs/index.php/infotezy/article/view/15/33(13.01.2012)

# Rozdział 5

# Rozpoznane metody działania w ramach szpiegostwa gospodarczego

## 1. Postęp technologiczny jako bodziec dla wywiadów i szpiegów

W literaturze przedmiotu wyraźnie zaznacza się, że zarówno szpiegostwo gospodarcze, jak i wywiad gospodarczy zyskały na znaczeniu w XX wieku. Lawinowy rozwój postępu technicznego, powstanie tzw. rynku wynalazków spowodowało, że zaczęto stosować wszelkie dostępne środki, legalne i nielegalne, dla zdobywania informacji. Najcenniejsze z nich dotyczyły wdrożonych wynalazków, planów poczynań konkurencji, strategii marketingu oraz wprowadzania na rynek nowych towarów. Plan kampanii reklamowych, pomysł reklamowy – także przedstawia określoną wartość, którą można wyliczyć w pieniądzach, a więc można także sprzedać, kupić, w ostateczności nawet ukraść. Kiedy jednak nie daje się kupić i nie udaje się namówić do zdrady pracowników firmy, wtedy pozostaje tylko jedno wyjście, a mianowicie posłużenie się techniką wywiadowczą.

Wydaje się za w pełni uzasadnione twierdzenie, że ważniejsze od szpiegowania politycznego jest jednak szpiegostwo gospodarcze. Wszystkie, nie tylko europejskie rządy, polecają swym służbom wywiadowczym, aby dla nich pracowały i zapewniały przewagę w gromadzeniu danych o najnowszych zdobyczach naukowych, czy np. planowanych wielkich międzynarodowych kontraktach. W czasach narastającego kryzysu gospodarczego czy bezrobocia proceder szpiegowania z roku na rok nasila się. Przykładów w tej mierze jest wiele, szczególnie z okresu końca XX wieku np. niezwykle sprawny i agresywny wywiad francuski w kwietniu 1994 roku dzięki podsłuchiwaniu rozmów telefonicznych szefów koncernu Siemensa nieomal wydarł, jak się wydawało przesądzony już, miliardowy kontrakt z Koreą Południową na pociąg dużej prędkości.

Doceniając wagę informacji jako podstawy rozwoju przedsiębiorstwa, już w latach 90. XX w. lansowano zasadę: *Każdy pracownik jest wywiadowcą na rzecz swojej firmy*[259].

Rozpoznanym osiągnięciom wywiadów gospodarczych wielu państw dużą uwagę poświęca się w mediach, a także w literaturze naukowej czy popularnonaukowej, także na konferencjach naukowych. Wiele pozycji z lat 80. i 90.

259 Tak przewidywała profesjonalna prognoza z przełomu lat 80. i 90. XX wieku opracowana przez francuskich ekspertów wywiadu gospodarczego, która przewidywała, że oprócz innych ważnych postanowień, tego typu zadania będą zapisane w zakresie obowiązków pracowników firm, po odpowiednim przygotowaniu personelu. Szerzej: B. Martinet, Y.M. Marti, *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji,* Warszawa 1999, s. 325.

XX wieku omawia działalność i efekty MI 5 i MI 6. Można nawet spotkać się z poglądem, że co do tych służb nie ma już czego a także w literaturze naukowej czy popularno-naukowej, także na konferencjach naukowych. Wiele pozycji z lat 80. I 90. XX wieku omawia działalność i efekty MI 5 i MI 6. Można nawet spotkać się z poglądem, że jeśli idzie o te służby, to nie ma już czego utajniać[260].

Powojenne sukcesy wywiadowców gospodarczych czy szpiegów gospodarczych różnych krajów można tylko częściowo wyliczać, gdyż nie wszystkie zostały upublicznione – chociażby ze względów na tajemnicę przedsiębiorstwa czy bezpieczeństwo państwa lub informatorów. Wymieńmy przynajmniej niektóre z nich:

- z laboratorium w Cambridge w Wielkiej Brytanii skradziono dokumentację techniczną na produkcję kolorowych telewizorów;
- z firmy lakierniczej pod Londynem skradziono 150 kilogramów dokumentów zawierających technologię produkcji farb i politury odpornej na wysoką temperaturę;
- z francuskiego pieca hutniczego, w trakcie procesu technologicznego, skradziono próbki specjalnego szkła;
- Japończycy jeszcze pod koniec XIX wieku nie mieli własnych stoczni. Większość statków zamawiali w stoczniach niemieckich i angielskich. Przez okres 20 lat byli klientami stoczni Clyde. Wysyłali tam swoich inżynierów i rozpoznawali szczegóły przemysłu stoczniowego. Zdarzało się, że zamawiali statek a następnie rezygnowali lub zmieniali zamówienie. W efekcie okazało się, że niektóre statki Japończycy sami kończyli i wodowali. Kiedy Japończycy złożyli kolejne zamówienie na budowę drobnicowca, Szkoci spodziewali się kolejnych manipulacji. Rzeczywiście, zamawiający zrezygnowali z realizacji, a w stoczni japońskiej odbyło się wodowanie bliźniaczego statku. W trakcie uroczystości statek przewrócił się do góry dnem. Sprytni Szkoci opracowali specjalną, fałszywą dokumentację, którą z całą premedytacją udostępnili szpiegom gospodarczym. W wielu innych, skutecznych przedsięwzięciach znane było patriotyczne zaangażowanie Japończyków, które umożliwiło zdobycie wielu osiągnięć światowej myśli naukowo-technicznej. Swoje zdobycze udoskonalali do tego stopnia, że nawet sami wynalazcy mieli trudności z rozpoznaniem swego dzieła. Jednakże nie wszystkie poczynania wywiadów kończą się sukcesami. Przekonali się o tym nie tylko Japończycy.
- na wystawie lotniczej w Le Bourget pod Paryżem w 1973 roku Francuzi po raz pierwszy zaprezentowali Concorde'a. Bliźniaczy model prezentowali Rosjanie pod marką Tupolew. Niezwykłe podobieństwo spowodowało, że model rosyjski nazwano „Concordzki". W czasie pokazów rosyjski model uległ katastrofie. Dobrze poinformowani twierdzą, że Francuzi od początku projektowania samolotu mieli świadomość obecności rosyjskich wywiadowców. Z tego powodu przygotowali dwie dokumentacje, z których jedna była przeznaczona na użytek konkurencji czyli rosyjskiego wywiadu;
- w 1995 roku głośna sprawa pięciorga Amerykanów dotyczyła tajnych operacji rozpoznawczych w ramach szpiegostwa gospodarczego we Francji i próby przekupienia wysokich urzędników z otoczenia premiera. W odpowiedzi CIA oświadczyła, że nie zajmuje się wykradaniem tajemnic francuskim koncernom i przekazywaniem ich prywatnym amerykańskim firmom;

260 Szerzej: J. Rusbridger, *Gra wywiadów. Iluzje i pozory szpiegostwa międzynarodowego*, Warszawa 1993, s. 26.

- w 1997 r. Hsu Kailo, dyrektor tajwańskiej firmy farmaceutycznej, został aresztowany za kradzież dokumentacji leku stosowanego w onkologii, produkowanego przez Bristol-Myers Squibb. Azjata zapłacił 400 tys. USD za lek, którego opracowanie kosztowało 15 mln USD.
- w 1997 r. Steven L. Davis trafił na 2,5 roku do zakładu karnego za próbę kradzieży projektu nowej maszynki do golenia Mach3 firmy Gilette.
- jedną z sensacji 1998 roku były informacje wywiadowcze przekazane firmie British Aerospace, które przyczyniły się do wygrania przetargu na dostawę samolotów szkolno-bojowych Hawk do Indonezji. Wcześniej uzyskano dokładne dane na temat warunków, jakie zaoferowała francuska firma konkurencyjna – potentat zbrojeniowy Dassault.

Z początkiem XXI wieku, wobec szybkiego rozwoju nowoczesnych technologii, wykradane konkurencji tajemnice nabrały większej wagi i ceny:

- W 2003 r. dwóch menedżerów z Boeinga zostało aresztowanych za wyniesienie projektu programu rakietowego dla *US Air Force* z siedziby koncernu Lockheed Martin. Wartość kontraktu opiewała na 2 mld USD.
- Chiński producent samochodów Cherry Q zdobył w maju 2005 r. wartą 100 mln USD dokumentację Chevroleta Sparks produkowanego przez General Motors.
- W marcu 2005 roku zatrzymano szpiega przemysłowego w Ericssonie, którym okazał się 26-letni Węgier, podejrzany o uzyskanie tajnych informacji z zakresu obronności Szwecji. Dane uzyskał po włamaniu się do systemu informatycznego Ericssona. Tłumaczył, że chciał wykazać braki w zabezpieczeniach i liczył, że Szwedzi zatrudnią go w swojej firmie.
- W maju 2005 policja izraelska zatrzymała 20 osób, w tym członków władz czołowych firm w kraju, w związku ze skandalem na tle szpiegostwa gospodarczego. Media izraelskie określiły skandal jako aferę bez precedensu. Wśród osób zatrzymanych znalazło się 11 prywatnych detektywów podejrzewanych o nielegalne zdobycie w okresie 18 miesięcy wielu ważnych dokumentów i zdjęć i przekazanie ich klientom. W areszcie znaleźli się również szefowie: telewizji satelitarnej Yes, operatorzy łączności komórkowej Cell-Com, Pelephone, Mayers oraz importer pojazdów Volvo, Honda i Jaguar. Wszyscy są podejrzani o zdobywanie informacji poprzez włamywanie się do cudzych systemów informatycznych. Zleceniodawcy szpiegostwa korzystali z usług 9 firm detektywistycznych. Długotrwałe śledztwo prowadziły policje Izraela, Wielkiej Brytanii, Niemiec oraz Interpol. Skandal świadczy o zaciekłej walce konkurencyjnej, która mogła mieć bardzo poważne skutki dla gospodarki Izraela.
- W 2006 roku aresztowano trzech nielojalnych pracowników, którzy zażądali 1,5 mln USD za najpilniej strzeżoną tajemnicę koncernu Coca-Cola. Była to receptura nowego produktu, który jeszcze nie ujrzał światła dziennego, wzór jego opakowania i kilka łyków na spróbowanie. Zdobycie receptury nowego produktu Coca-Coli nie było trudne. Wyniosła ją w torebce Joya Williams, jedna z pracownic administracyjnych. Oprócz niej, prokuratura oskarżyła o kradzież tajemnicy handlowej dwie inne osoby. Sprawę ujawnił koncern PepsiCo, do którego zgłosili się złodzieje. Poinformował o tym FBI oraz konkurenta jednocześnie oświadczając,

że rywalizacja może być czasami ostra, ale musi być także uczciwa. Coca-Cola podziękowała za przekazanie informacji, a jednocześnie zdecydowała, że zaostrzy procedury bezpieczeństwa[261].

- W 2007 roku anonimowe źródło w brytyjskiej prasie podało, że korzystając z olbrzymiej ilości danych wykradzionych McLarenowi, Fernando Alonso i zespół Renault zdobyli tytuły mistrzów świata w 2006. Wykradzione dane podobno zawierały 780 szkiców technicznych McLarena przygotowanych na 2006 i 2007 rok. Według źródła „były to dokładne i kompletne plany samochodów", czyli w sporcie, w którym decydują ułamki sekund, rzecz bezcenna, warta dziesiątki, jeśli nie setki milionów dolarów. Właściwe pliki zostały wgrane i wykorzystane w systemie komputerowym Renaulta.
- W jednej z francuskich firm inżynieryjnych zauważono, że podczas oprowadzania po zakładzie grupy przedstawicieli firmy azjatyckiej jeden ze zwiedzających bardzo często się pochylał, żeby zawiązać sznurowadło. W efekcie podczas każdego z tych postojów podnosił z podłogi malutkie skrawki metalu i potem przyklejał je do taśmy umocowanej wewnątrz krawata. Miały one zostać potem poddane analizie – już w firmie szpiega z często rozwiązującymi się sznurowadłami.
- Z firmy Wakefield Shirt Company skradziono rewelacyjny produkt – niemnącą się koszulę. Firmie Minnesota Mining and Manufacturing Company wydarto tajemnicę produkcji taśmy do klejenia. Szpiedzy gospodarczy, rekrutujący się z różnych firm i koncernów, kradną sobie nawzajem prototypy nowych modeli telewizorów, magnetowidów, próbki szkieł, makiety nowych modeli samochodowych. Od kiedy zaczęła funkcjonować komputeryzacja na skalę przemysłową, szpiedzy gospodarczy zaczęli dokonywać kradzieży informacji zawartych w komputerach[262], w których obecnie przechowuje się wszelkie ważne informacje, a więc dokumenty techniczne, prace naukowe, opisy patentów, dane dotyczące obrotów handlowych i zamierzeń eksportowych, kierunków zainteresowań gospodarczych itd.
- Zdaniem Waltera Opfermana, szefa biura wywiadowczego w Badenii-Wirtembergii, ok. 20% małych i średnich niemieckich firm stało się obiektem szpiegostwa. A to wynika jego zdaniem z chińskich dążeń, by w 2020 r. prześcignąć USA i stać się największą gospodarką na świecie.
- Przedstawiciele Motorolli przyznają, że dzięki wywiadowi wśród konkurencji korporacja dokonała wielu istotnych zmian wewnątrz firmy, a także nawiązała współpracę z nowymi partnerami,
- Obowiązująca w USA ustawa o szpiegostwie gospodarczym z 1996 r. wyraźnie stanowi, że kradzież tajemnic handlowych jest przestępstwem federalnym. Jednak Departament Sprawiedliwości przyznaje, że w latach 1996-1999 były tylko 22 przypadki postawienia firmy w stan oskarżenia na podstawie zapisów tej ustawy. Wydaje się, że łatwiej jest badać straty. W jednej z często cytowanych analiz

261 Recepturę Coca-Coli opracował farmaceuta John Stith Pemberton z Atlanty. Nazwę napoju i jego charakterystyczne logo wymyślił jego wspólnik i księgowy Frank Robinson. Obecnie Coca -Cola jest obecna w ok. 200 krajach. W Polsce produkcja na licencji ruszyła w 1972 roku. Dwadzieścia lat później koncern rozpoczął bezpośrednią działalność w naszym kraju. Coca-Cola Poland Services oraz Coca-Cola HBC zatrudniają w Polsce łącznie 3 tys. osób. Jednakże recepturę zna tylko kilka osób. Szerzej:http://pl.wikipedia.org/wiki/Coca-Cola(18.03.2015)

262 L. Bajer, *Wywiad gospodarczy*, wyd. cyt, s. 76.

stwierdza się, że w wyniku kradzieży danych tysiąc spółek badanych przez magazyn „Fortune" poniosło w 1999 r. straty w wysokości 45 mld USD.

- Niemieckie źródła podają, że w 1994 r. wykryto przeszło 1000 przypadków działalności agentów gospodarczych w przedsiębiorstwach RFN. Większość zakładów i firm, w obawie przed konkurencją, woli nie przyznawać się, że ich tajemnice dostały się w obce ręce. Po upadku żelaznej kurtyny i przeciwstawnych bloków nastąpiła eskalacja szpiegostwa gospodarczego. Nowe techniki informacyjne dają tu wręcz nieograniczone możliwości, znikoma też jest szansa wpadki agenta. Jeżeli teoretycznie każdy może włamać się do ewidencji danych CIA, co udowadniają komputerowi piraci, to co dopiero mówić o działaniach profesjonalistów. Szczególną aktywność wykazywały wywiady byłego Bloku Wschodniego.
- Według niemieckiego Urzędu Ochrony Konstytucji z początkiem XXI wieku tylko Węgry, Czechy i Słowacja chwilowo zrezygnowały ze szpiegostwa gospodarczego. Natomiast za bardzo aktywny uważa się w Niemczech wywiad polski, a największe zaangażowanie przejawiają Rosjanie. Wywiad rosyjski, dysponujący potężnym wyposażeniem i szpiegowskim *know-how* umacnia kontakty z osobistościami życia politycznego i gospodarczego, aby wykorzystać je dla swoich celów, często bez ich wiedzy. Równocześnie szpiedzy pod przykrywką dyplomacji próbują rozszerzać stosunki przekraczające oficjalne ramy polityczne i gospodarcze (wspólne spędzanie urlopów, uczestnictwo w prywatnych przyjęciach z okazji imienin, urodzin, połączone z dawaniem drogich prezentów itp.) Podkreślić przy tym należy, że poprawa stosunków między Niemcami a krajami b. ZSRR spowodowała ostrożniejsze postępowanie przy zdobywaniu informacji gospodarczych, co pozwoliło uniknąć powikłań dyplomatycznych.
- W 1995 r. aresztowano 2 naukowców USA, którzy usiłowali sprzedać genetycznie zmienione komórki, tj. ludzki hormon – erytropetynę, podobno najbardziej dochodowy produkt przemysłu biotechnologicznego. Powodował przyspieszenie tworzenia czerwonych ciałek krwi, stanowił środek pomocny w dializie nerek, w zwalczaniu AIDS i był przydatny w chemioterapii.
- Dziennik „Suddeutsche Zeitung" z marca 1996 r. twierdził, iż według rozeznania niemieckich służb specjalnych jedna trzecia spośród 500 rosyjskich dyplomatów przebywających stale w Niemczech wykonuje wyłącznie zadania związane z pracą wywiadu (dla porównania np. w Wielkiej Brytanii jest tylko 35 rosyjskich dyplomatów). Do tego doliczyć należy parę tysięcy współpracowników wywiadu, działających bezpośrednio w gospodarce, w około 2500 niemiecko-rosyjskich firmach, współzarządzanych często przez oficerów służb specjalnych. Prasa niemiecka zwracała uwagę na to, że próby penetracji gospodarki kraju podejmują również szpiedzy z Kazachstanu, Ukrainy, Syrii, Libii i Iranu[263].
- W naszej branży wszyscy szpiegują wszystkich. Właściwie jest to już uważane za formę współpracy – żartował były prezes General Motors na Europę Nick Reilly. Ale już nie było mu do śmiechu, kiedy pracownik GM Europa Jose Ignacio Lopez zwolnił się i przeszedł do Volkswagena z pudłami pełnymi tajnych dokumentów.

Nie ulega wątpliwości, że szpiedzy gospodarczy stosują wszystkie, także niedozwolone metody działania, czyli takie, którymi mogą posługiwać się służ-

263 E. Cilecki, *Penetracja rynków,* wyd. cyt. s 117.

by specjalne i wywiad państwowy, a przykładowo: podsłuch, podgląd obiektu, werbowanie tajnego współpracownika, kontrola korespondencji i inne.

## 2. Najgłośniejsze sprawy o szpiegostwo gospodarcze

W literaturze przedmiotu występuje uzasadnione przekonanie, że z wywiadu gospodarczego wyodrębniło się szpiegostwo gospodarcze. Terminy te bezpodstawnie występują przemiennie. Podstawowe cele, a przede wszystkim niektóre bezprawne formy działania zespołów szpiegostwa gospodarczego są równoznaczne z popełnieniem przestępstwa.

Zdobyte informacje służą zleceniodawcy do precyzowania strategii postępowania zarówno państwa, a przede wszystkim przedsiębiorstwa, koncernu, w uzyskaniu lub utrwaleniu jego wpływów na danym rynku. W swoim działaniu wywiad gospodarczy posługuje się określonymi formami, metodami i środkami dla uzyskania niezbędnych informacji[264]. A podstawową cechą wywiadowcy jest brak konfliktu z prawem.

Szpiegostwo gospodarcze określane również jako przemysłowe polega na zdobywaniu zaawansowanych technologii oraz szybkie ich wdrażanie w cyklach produkcyjnych. Przedmiotem zainteresowania są zazwyczaj informacje niejawne;ich nielegalne zdobycie zagrożone jest karą pozbawienia wolności. W działaniu stosuje się nielegalne środki właściwe służbom specjalnym jak np.: werbowanie współpracowników, wywiad elektroniczny, nagrywanie rozmów, tajne fotografowanie, stosowanie podsłuchu i podglądu, kopiowanie dokumentów itd.

Inne zadania stoją przed wywiadem ekonomicznym zwanym również wywiadem wojskowym, który ma za zadanie rozpoznawanie potencjału ekonomicznego i jego wpływu na możliwości obronne kraju. Zakres zainteresowań obejmuje całokształt produkcji, dystrybucji i konsumpcji. Osiągnięcia tego wywiadu umożliwiają wnioski dotyczące zakresu produkcji i dystrybucji oraz poziomu konsumpcji, a nawet analizy poziomu gospodarczego danego kraju. Wywiad ekonomiczny jest o tyle skomplikowany, że jego działanie nie wywołuje – np. w okresie pokoju – natychmiastowych skutków ujemnych. Kieruje swe zainteresowania na obiekty zarówno o strategicznym znaczeniu, jak węzły komunikacyjne, środki łączności, media i wiele innych, które z pozoru nie mają wiele wspólnego z obronnością kraju, są jednakże niezbędne do funkcjonowania zarówno wojska, jak i ludności[265].

W latach 70. XX w. zakres profesjonalnych zainteresowań rozszerzył się z wywiadu gospodarczego na bardziej ukierunkowany wywiad naukowo-techniczny. W Polsce ukierunkowano zainteresowania wywiadu na uzyskiwanie informacji oraz dokumentacji z zakresu światowych osiągnięć naukowo-technicznych. Wywiad uczestniczył w pościgu za technologiami, za niedostępnym lub zbyt drogim sprzętem, za chronionymi wynalazkami, a także za dokumentacją techniczną[266].

Każdy rodzaj wywiadu gospodarczego wymaga rutynowych albo specjalistycznych działań kontrwywiadowczych o charakterze tajnym, jak i jawnym.

264 T. Wojciechowski, *Wywiad gospodarczy,* wyd. cyt.
265 Por. Z. Bagiński, *Wywiad,* Warszawa 1975, s. 68-69.
266 Tamże.

Przykładem mogą być działania prowadzone przez państwowy wywiad naukowo-techniczny, który jak powszechnie wiadomo w latach 70. I. 80. XX wieku intensywnie wspomagał polską gospodarkę w wielu dziedzinach, a szczególnie w zakresie informacji o różnorodnych nowoczesnych technologiach stosowanych w krajach zachodnich. Wymagało to jednak niezwykle starannej ochrony kontrwywiadowczej zakładów, do których trafiały zdobyte technologie.

Przedsięwzięcia kontrwywiadowcze dotyczą ochrony własnych technologii i wynalazków, jak i tych zdobytych w innych krajach czy przedsiębiorstwach.

Wizyta kontrahentów zagranicznych w jednej z polskich fabryk farmaceutycznych doprowadziła do rozpoznania przez gości najnowszej technologii strzeżonego produktu. Otóż goście zorientowali się, że cykl produkcyjny pewnego specyfiku, który był akurat na taśmie produkcyjnej, jest wierną kopią starannie strzeżonego na Zachodzie. Następnie okazało się, że zagraniczne służby intensywnie szukały, jaką drogą, podległego im zakładu, wydostała się strzeżona technologia[267].

Różnorodne zagadnienia związane z działalnością szpiegów politycznych, militarnych, ekonomicznych i gospodarczych przedstawiają media w wielu krajach. Państwa zachodnie od lat wzajemnie szpiegują się na polu gospodarczo-produkcyjnym, a faktom tym nadaje się szeroki rozgłos.

Nie trzeba być specjalistą, by zorientować się, że praktycznie wszystkie państwa szpiegują się wzajemnie. Prawdziwa eksplozja informacji na ten temat miała miejsce pod koniec XX wieku. Piętnowane jest wzajemne szpiegowanie się sojuszników, co warto zilustrować przykładami[268]. Wymienia się afery związane ze szpiegostwem gospodarczym Japonii, Niemiec i Francji w USA w latach 70. i 80. W 1997 r. Niemcy wydaliły dyplomatę USA usiłującego uzyskać od wysokich funkcjonariuszy informacje dotyczące najnowszych technologii, osiągnięć produkcyjnych, handlowych i technologicznych.

W Stanach Zjednoczonych po 1990 r. zanotowano wręcz eksplozję szpiegostwa przemysłowego, wymierzonego przeciwko amerykańskim korporacjom, co miało zmusić rząd do reorganizacji jednostek kontrwywiadowczych. Wskazuje się na przypadki szpiegostwa m.in. ze strony Francji, Włoch, Niemiec, Chin oraz Rosji i innych państw powstałych po rozpadzie byłego ZSRR. Media amerykańskie twierdzą nawet, że USA powinny „odpłacać tym samym". Uzasadnione wydaje się twierdzenie, że rosyjskie zagrożenie wywiadowcze jest dziś tak samo poważne, jak w czasach zimnej wojny[269].

Federalne Biuro Śledcze (FBI) postawiło Niemcom zarzut, że należą do grupy 23 państw, które wykorzystują swoje służby specjalne do prowadzenia szpiegostwa gospodarczego. Podobno tylko w 1997 r. gospodarka amerykańska z tego tytułu poniosła straty w wysokości ok. 300 mld dolarów[270]. Do mediów przedostały się także informacje o sporach między USA i Izraelem, związanych z działalnością szpiegowską Izraela w USA.

---

267 K. Dubiński. I. Jurczenko**,** *Być szpiegiem***,** Warszawa 1994, s. 24-25.

268 Wiele uwagi temu zagadnieniu poświęcili autorzy R. i M. Taradejna, w pracy pt. *Ochrona informacji w działalności gospodarczej, społecznej i zawodowej oraz w życiu prywatnym,* Warszawa 2004, s, 312-322.

269 S. Walczak**,** *Spadkobiercy KGB***,** „Rzeczpospolita" z 26 stycznia 2000 r.

270 R. Hoffman, *Niewidzialna ręka amerykańskiej agencji. Świat w szpiegowskiej siatce***,** „Trybuna" z 27 października 1999 r**.**

Z kolei amerykańska CIA podczas ONZ-towskiej konferencji na temat rozwoju ekonomicznego w latach 70. szpiegowała delegacje innych państw, aby zdobyć szczegóły prawdziwych pozycji negocjacyjnych innych krajów. Jak wynika z odtajnionego raportu CIA, dzięki tym informacjom Amerykanie uzyskali na konferencji wszystko, co chcieli, bo ich negocjatorzy doskonale wiedzieli, komu i co proponować[271].

Tajemnica bankowa zawsze wzbudza duże zainteresowanie. A zarzut szpiegostwa na rzecz brytyjskiego wywiadu MI-6 postawiono m.in. urzędnikowi Banku Federalnego we Frankfurcie nad Menem, który to bank finansuje niemiecki rząd. Podobno ujawnione informacje pozwoliły Brytyjczykom na zastosowanie taktyki nacisku na Niemcy i korzystne rokowania z innymi państwami Unii Europejskiej. Także w Niemczech ujawniono fakt szpiegostwa przemysłowego obywatela Hiszpanii, byłego menadżera Opla i Volkswagena oraz trzech jego współpracowników. Natomiast z początkiem roku 2000 ujawniono działalność szpiegowską w Niemczech siedmiu dyplomatów tureckich.

W 1995 r. głośna była afera związana z wydaleniem przez Francję, pod zarzutem szpiegostwa gospodarczego, grupy dyplomatów amerykańskich. Fakt ten miał podobno doprowadzić do zakłóceń we współpracy służb specjalnych obu państw w zwalczaniu terroryzmu i nielegalnego handlu bronią. Natomiast kontrwywiad nowozelandzki udaremnił niecodzienną akcję szpiegów ChRL, którzy próbowali wykraść z Nowej Zelandii dzieło tamtejszych botaników – jabłonkę Róża Pacyfiku, której owoce mogą mieć dużą przyszłość rynkową.

Pod koniec ubiegłego wieku media podjęły szeroką akcję informacyjną o działalności amerykańskiej Agencji Bezpieczeństwa Narodowego (*National Security Agency* – NSA) i o prowadzonym przez nią ośrodku Echelon, zajmującym się totalnym podsłuchiwaniem za pomocą sieci około 120 satelitów szpiegowskich. Podsłuchiwane są wszelkiego rodzaju elektroniczne środki masowej komunikacji, tj. od rozmów telefonicznych, przez faksy, pagery, pocztę e-mail, sieć Internetu, łączność satelitarną i światłowodową a kończąc na specjalnych połączeniach przy zastosowaniu bardzo zaawansowanej techniki.

Sama idea szpiegowania na masową skalę pochodzi jeszcze z czasów II wojny światowej, a rozwinięto ją w latach 60. wraz z rozwojem Echelonu, tj. systemu globalnej sieci wywiadu elektronicznego, który powstał z inicjatywy USA, by wspólnie z sojusznikami, na masową skalę gromadzić i analizować rozmowy telefoniczne, faksy, e-maile i transfery plików[272]. Pierwsze informacje na

271 B. Węglarczyk, *Jak wygląda szpiegostwo końca XX wieku? Świat równoległy*, „Gazeta Wyborcza" z 31 stycznia 2000 r.

272 Echelon to globalna sieć wywiadu elektronicznego. System powstał przy udziale Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii i jest zarządzany przez amerykańską służbę wywiadu NSA. Później dołączyły inne państwa, głównie europejskie. Echelon posiada w całym świecie urządzenia techniczne do przechwytywania (podsłuch) wiadomości w kanałach telekomunikacji. System gromadzi i analizuje transmisje fal elektromagnetycznych przez urządzenia elektroniczne z całego świata – urządzenia telekomunikacyjne, IT, faksy, e-maile, transfery plików, rozmowy telefoniczne, komputery, radary, satelitów rozpoznawczych, s. telekomunikacyjnych itp. System gromadzi i przetwarza miliardy przekazów elektronicznych na dobę. Jest to tylko niewielki ułamek całej komunikacji elektronicznej, gdyż jedynie w USA wykonuje się prawie 4 mld samych tylko rozmów telefonicznych na dobę. Zebrane lokalnie informacje z całego świata przesyłane są do centrali w Fort Meade, gdzie znajduje się główna siedziba NSA. Superkomputery dokonują analizy materiału, dostosowanej do regionu, tworzą słownik haseł, stanu materiału i algorytm szyfrowania.

ten temat pojawiły się już w 1988 r., a później temat wracał wraz z kolejnymi skandalami. Echelon miał być wykorzystany m.in. do podsłuchiwania ważnych osobistości jak np. księżnej Diany czy sekretarza generalnego ONZ. Prawdopodobnie dzięki informacjom zdobytym za pomocą tego systemu ujawniono korupcję podczas przetargu na samoloty dla Arabii Saudyjskiej, w efekcie czego kontrakt stracił europejski Airbus. W marcu 2000 r. James Woolsey Jr, już wtedy były dyrektor CIA, ironizował broniąc się przed zarzutami szpiegowania Europejczyków. Napisał wówczas w „The Wall Street Journal": „My musimy was kontrolować, bo bierzecie łapówki".

Teraz Europa grzmi, że sojusznicy nie powinni wzajemnie podsłuchiwać swych przywódców. Chce także – na wniosek Francji i Niemiec – wynegocjować z Waszyngtonem pakt podobny do tego, jaki USA podpisały z Wielką Brytanią, Australią, Kanadą i Nową Zelandią. Chodzi o tzw. *Five Eyes*, czyli umowę ścisłej współpracy, której sentencją jest stwierdzenie, że zamiast szpiegować się nawzajem, kraje te wspólnie szpiegują innych.

Podsłuchem komunikacji telefonicznej, faksowej, telegraficznej i komputerowej zajmuje się także brytyjska *Government Communications Headquartes* (GCHQ). Natomiast niemiecki wywiad BND prowadzi pod Frankfurtem nad Menem stację podsłuchową – Rahab, która systematycznie nagrywa rozmowy telefoniczne z USA i włamuje się do amerykańskich systemów komputerowych. Na uwagę zasługuje fakt, że niemiecki Trybunał Konstytucyjny w Karlsruhe uznał w 1999 r., że niemieckie służby specjalne mogą legalnie podsłuchiwać międzynarodowe, bezprzewodowe rozmowy telefoniczne, chociaż miałoby to dotyczyć nie tylko walki z terroryzmem.

Niezwykle trafnie ujął to zagadnienie Bartosz Węglarczyk, który pisze: *W świecie równoległym wszyscy szpiegują więc wszystkich. CIA od lat wspiera amerykański przemysł, podsłuchując firmy z Europy. Francuzi szpiegują amerykańskie koncerny w Afryce i Azji. Brytyjczycy pilnują poczynań Francuzów. Ci ostatni mają olbrzymią siatkę wywiadowczą w Jugosławii, której wywiad interesuje się z kolei np. Rumunią i Bułgarią. Tajne służby bułgarskie zbierają informacje w Grecji na temat zamierzeń rządu tego kraju wobec Macedonii. Grecy oczywiście szpiegują Turków, zaś ci pilnują Armenii, Iraku i Syrii w sojuszu z Izraelem. Izraelski Mossad także szpieguje wszystkich, nie wyłączając swych najbliższych sojuszników Amerykanów"*[273].

W problematyce politycznej nie należy zapominać o walce konkurencyjnej, która rozgorzała od momentu wprowadzenia gospodarki rynkowej w byłych krajach socjalistycznych. Naszym specjalistom nie brakuje pomysłów, a wykorzystywani są nie tylko byli pracownicy służb specjalnych. Wśród różnorodnych metod, najczęściej stosowane są klasyczne. Zdarza się również niezwykle uzdolniona sprzątaczka – informatyk[274].

Współcześnie rosyjscy szpiedzy mają zdobywać przede wszystkim informacje, wzmacniające kartę negocjacyjną Kremla w sprawach energetyki czy bez-

System Echelon był m.in. prawdopodobnie bezpośrednim źródłem informacji o korupcji przy wartym 6 miliardów dolarów przetargu na samoloty dla Arabii Saudyjskiej. W efekcie ogłoszenia NSA przetarg stracił europejski Airbus. Dla ułatwienia pracy szpiegowskiej systemu Echelon władze amerykańskie obłożyły embargiem niektóre techniki szyfrowania http://pl.wikipedia.org/wiki/Echelon(12.03.2015)

273 B. Węglarczyk, *Jak wygląda szpiegostwo* . wyd. cyt.

274 M. Przewoźniak, E. Mazurków, *Pomysłowy szpieg przemysłowy. Sprzątaczka-informatyk kradła dane konkurencji,* Życie Warszawy z 17 listopada 2003 r.

pieczeństwa. Od tego typu wyspecjalizowanych szpiegów roi się też w biznesie i ośrodkach badawczych. Ich zadaniem jest wykradanie informacji i technologii, które mogą pomóc Rosji nadrobić zaległości wobec Zachodu. Głęboko infiltrowane są również międzynarodowe instytucje, takie jak OBWE czy Rada Europy, a także centra naukowe i uniwersytety, gdzie podobnie jak w czasach ZSRR opłacani przez Kreml naukowcy występują w obronie rosyjskich interesów.

W wielu kręgach politycznych dominuje pogląd, że najbardziej jaskrawym przypadkiem działania rosyjskich szpiegów w sprawach gospodarczych jest gazociąg północny, który udało się zbudować dzięki przeciągnięciu na stronę Kremla byłego kanclerza Niemiec Gerharda Schroedera i byłego premiera Finlandii Paavo Lipponena.

W przypadkach, w których zawodzi lobbing i przekupstwo, rosyjskie służby sięgają po stare metody: szantaż, zastraszanie i. uwodzenie[275]. Kolejne aresztowania rosyjskich szpiegów w wielu krajach ukazują olbrzymią skalę rosyjskiej agentury na Zachodzie, a jej głównym celem jest zdobywanie informacji o charakterze gospodarczym. Jednakże na posiedzeniu Federalnej Służby Bezpieczeństwa Władimir Putin oświadczył, że rosyjski kontrwywiad w 2014 roku. położył kres działalności 52 kadrowych funkcjonariuszy i 290 agentów obcych służb specjalnych działających w Rosji.

Warto dodać, że w październiku 2012 roku FBI wykryło rosyjską siatkę szpiegów gospodarczych, których działalność polegała na nielegalnym kupowaniu elektronicznych komponentów dla rosyjskich instytucji wojskowych i wywiadowczych. Prokuratura federalna oskarżyła 11 osób, z których aresztowano 8 obywateli rosyjskich, a pozostałe 3 osoby przebywają w Rosji. Zdaniem prokuratury w całą operację zaangażowane były firmy mające siedzibę w Houston (Arc Electronics) i Moskwie (Apex System). Właściciel i szef Arc Electronics Alexander Fishenko został oskarżony o działalność w charakterze tajnego agenta rosyjskich władz w Stanach Zjednoczonych. Fishenko urodził się w Kazachstanie, a obywatelstwo amerykańskie uzyskał w 2003 r. Przedmiotem szpiegostwa gospodarczego były nowoczesne urządzenia mikroelektroniczne warte 50 mln USD, których nie wolno sprzedawać za granicę bez zgody urzędów amerykańskich. Urządzenia te mają zastosowanie przede wszystkim w radarach i systemach naprowadzania rakiet. Zdaniem prokuratury szpiedzy usiłowali wykorzystać amerykański wolny rynek, by ukraść amerykańskie technologie dla rosyjskiego rządu. Przeszukania dokonane przez FBI w siedzibie Arc Electronics doprowadziły do zabezpieczenia dokumentów spakowanych w 18 pudłach. Moskwa odrzuca zarzuty Amerykanów twierdząc, że nielegalna dostawa urządzeń elektronicznych do Rosji nosi jedynie charakter kryminalny i nie jest związana z działalnością wywiadowczą[276].

W jednej z najgłośniejszych afer w Polsce nieznani sprawcy usiłowali, przy pomocy podrobionych przepustek, wynieść z poznańskiej fabryki Volkswagena plany modelu Caddy Maxi, który miał być wkrótce produkowany w tej fabryce.

W 2004 roku rozpoznano największą ze spraw toczących się przeciwko złodziejom własności intelektualnej i myśli technicznej rozpracowywanych w

275 Szerzej: W. Lorenz, *Kreml stawia na szpiegów*, „Rzeczpospolita" z dnia 7-9 kwietnia 2012 r.
276 *FBI rozbiło rosyjską siatkę szpiegowską*, „Rzeczpospolita" z 4 października 2012 r.

okresie ostatnich kilkunastu lat przez policję i prokuraturę. Sprawa dotyczyła grupy inżynierów z firmy Fazos S.A., należącej do giełdowej grupy Famur. Wspomniani inżynierowie, a w tym długoletni pracownik Fazosu, który pełnił tam funkcje m.in. prokurenta spółki i pełnomocnika zarządu ds. projektów, odeszli do konkurencyjnego przedsiębiorstwa. W zameldowaniu organom ścigania podano wartość zabranych projektów i programów komputerowych na ponad 6 milionów złotych. Po dwóch latach, tj. w maju 2006 roku, postawiono wspomnianym pracownikom m. in. następujące zarzuty:

1. ujawnienie i wykorzystanie informacji, z jakimi zapoznali się w związku z wykonywaną pracą,
2. przerobienie dokumentacji technicznej poprzez usunięcie z rysunków założeniowych danych właściciela praw autorskich i wstawienie danych nowego pracodawcy,
3. naruszenie majątkowych praw autorskich poprzez skopiowanie na nośniki komputerowe rysunków dokumentacji technicznej,
4. uzyskanie bez właściwej zgody cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej,
5. paserstwo dotyczące powyższych programów i przedmiotów.

Według Instytutu Bezpieczeństwa Biznesu sprawa Fazosu, najgłośniejsza tego typu w Polsce, to jednak tylko wierzchołek góry lodowej, gdyż handlowanie informacjami strategicznymi przedsiębiorstw jest dość nagminne. Nie ma właściwie branż, których by to nie dotyczyło. Obecnie nasila się także problem wycieku istotnych dla bezpieczeństwa danych z firm logistycznych i transportowych. Kradnie się wszystko np.: projekty maszyn, urządzeń, procesów technologicznych, strategii marketingowych, dane klientów, wyniki sprzedażowe, treści umów. Aktualnie wydaje się, że każda, nawet najbardziej błaha informacja, znajdzie swojego nabywcę[277]. Typowe sprawy to np.:

- w dużej firmie z branży IT kierownictwo zauważyło częste przypadki zwalniania się najlepszych przedstawicieli handlowych. Po przeprowadzeniu analizy informacji zawartych w firmowych komputerach udało się ustalić, że jeden z pracowników administracji firmy przekazał wyniki handlowców konkurencji. A ta podkupywała tych z największymi sukcesami;
- w innej sprawie nielojalny pracownik przekazywał konkurencji informacje na temat ofert przetargowych za pomocą popularnej gry *on-line* „OGame", gdzie występuje opcja wysyłania wiadomości do innych graczy;
- sprawa kradzieży danych z Urzędu Miasta w Siemianowicach Śląskich, w której sprawca i ochroniarz w jednej osobie, podczas nocnej zmiany wyniósł komputer z wydziału komunikacji i więcej się nie pojawił.

Z problematyką szpiegostwa przemysłowego boryka się coraz więcej polskich firm. Konsekwencje finansowe nielojalności pracowników sięgają nawet setek milionów złotych, działalność taka niesie niewielkie zagrożenie karą pozbawienia wolności. Przykładowo, w Stanach Zjednoczonych szpiegostwo jest traktowane jak poważne przestępstwo. Siergiejowi Alejnikowi, który ukradł kod komputerowy należący do

277 W. Chmielarz http://niwserwis.pl/artykuly/szpiegostwo-przemyslowe-duzy-zysk-niskie-kary.html(14.11.2013)

banku Goldman Sachs, grozi kara 15 lat pozbawienia wolności, natomiast dwaj inżynierowie, którzy wykradli tajemnice handlowe firmy oponiarskiej Goodyear, mogą zostać skazani nawet na 10 lat. Póki w Polsce nie będziemy traktować sprawy równie poważnie, firmy stale będą narażone na straty spowodowane przez nielojalnych i nieuczciwych pracowników.

Według niesprawdzonych informacji aktualnie w Polsce za 200-250 tys. zł. istnieje możliwość zdobycia sprawozdania finansowego spółki giełdowej, zanim zostanie ono upublicznione.

## 3. Handel informacjami strategicznymi

Handlowanie informacjami strategicznymi przedsiębiorstw jest nagminne i ujawniane w wielu krajach świata. Nie ma właściwie branż, czy kraju których by to nie dotyczyło. Obecnie nasila się np. problem wycieku istotnych dla bezpieczeństwa danych z firm logistycznych i transportowych Kradnie się wszystko: projekty maszyn, urządzeń, procesów technologicznych, strategii marketingowych, ale także dane klientów, wyniki sprzedażowe, treści umów.

Niektóre sprawy są szczególnie niepokojące. Wciąż jeszcze w wojsku pamięta się przygodę szefa sztabu, gen. Tadeusza Wileckiego, z lat 90. XX w., który wchodząc do gabinetu, bardzo się zdziwił, że sprzątaczka dokładnie przegląda papiery na jego biurku. Kiedy spytał ją, co robi, odpowiedziała po rosyjsku, że została zatrudniona przez firmę zewnętrzną i porządkuje mu biurko[278].

Kradzieże na tzw. sprzątaczkę były swego czasu bardzo popularne. Firmy wysyłały do konkurencji dobrze opłacane kobiety, które zatrudniały się tam np. jako sprzątaczki i pod pozorem prowadzenia prac porządkowych kradły dane i dokumenty. Sprzątnięcie gabinetu zajmuje nie więcej niż 10 minut. Pozostałe pół godziny można spokojnie przeznaczyć na włamanie się do komputera szefa firmy bądź założenie podsłuchu.

Według szacunkowych danych straty polskich firm z powodu wycieku strategicznych danych czy tajemnic przedsiębiorstwa szacowane są nawet na 360 milionów dolarów rocznie. Branże, które są narażone na działania wywiadu czy konkurencji, to przede wszystkim IT, bankowość, motoryzacja. Wiadomo, że ucierpiały z tego powodu PZU i KGHM, kilka banków, znaczący producent sprzętu oświetleniowego, firmy IT oraz producent sprzętu górniczego Famur, który oficjalnie wycenił swoje straty na 6 mln zł.

W mediach angielskich wiele uwagi poświęca się informacjom dotyczącym działalności byłych funkcjonariuszy MI6, którzy zasilają profesjonalne wywiadownie gospodarcze i są angażowani do zdobywania tajemnic gospodarczych dla największych brytyjskich korporacji. Na liście krajów objętych działalnością prowadzonego przez MI6 wywiadu gospodarczego znajduje się m.in. Francja, Niemcy, Włochy, Hiszpania i Szwajcaria. Nie jest ona natomiast prowadzona w czterech państwach, z którymi Wielka Brytania zawarła porozumienia o wymianie informacji wywiadowczych, tj. w Stanach Zjednoczonych, Kanadzie, Australii i Nowej Zelandii.

278 D. Walewska, *Sprzątaczka, czyli Bond po polsku*, „Rzeczpospolita" 9-11 listopada 2013 r.

Uzyskiwane przez wywiad informacje przekazywane są największym brytyjskim bankom i firmom przemysłowym, takim jak British Aerospace, BP czy British Airways - niekiedy za pośrednictwem tzw. The Hackluyt Foundation, w której zarządzie zasiadają dyrektorzy generalni i prezesi wielkich korporacji, byli wysokiej rangi przedstawiciele MSW i emerytowani, również wysokiej rangi pracownicy MI6. Przykładowo pismo „Sunday Business" twierdzi, że MI6 pomogła British Aerospace wygrać przetarg na dostawę samolotów szkolno-bojowych Hawk do Indonezji, przekazując tej firmie warunki, jakie zaoferował jej francuski konkurent Dassault[279].

## 4. Atrakcyjny rynek badawczo-rozwojowy w Polsce

Zagrożenia polskiego przemysłu i ośrodków badawczo-rozwojowych są oczywiste. Przykłady w tym zakresie to chociażby zagraniczna wędrówka w 1991 roku planów polskich kopalń z wielkością zasobów i jakością złóż, a także listy 10 tysięcy największych polskich przedsiębiorstw z ich aktualnym stanem finansowym, planami inwestycyjnymi, stanem zatrudnienia i kooperantami. Czy zostały wykorzystane przy prywatyzacji przez zagranicznych inwestorów?

Cudzoziemcy przyjeżdżający do Polski w latach siedemdziesiątych i osiemdziesiątych wykazywali wiele inicjatywy w zdobywaniu informacji gospodarczych, np.

- przedstawiciel jednego z koncernów chemicznych RFN, przebywający na kongresie naukowym w Polsce, usiłował wykorzystać swój pobyt do zbierania informacji o nowych procesach technologicznych w fabryce barwników;
- inny przedstawiciel przemysłu niemieckiego usiłował zebrać informacje o wynalazku dotyczącym metody produkcji farby do sitodruku;
- handlowiec z Meksyku zbierał informacje na temat procesu technologicznego przy budowie statków w stoczni w Szczecinie;
- przedstawiciele niemieckiej firmy Aktiengesselschaft wręczyli łapówkę pracownikowi Zakładów Rafinerii i Petrochemii w Płocku za przekazanie informacji o ofertach firm konkurencyjnych i danych techniczno- technologicznych projektu kontraktu;
- w czasie prowadzonych negocjacji z firmami amerykańskimi w sprawie zakupu licencji, przedstawiciele polskiego przemysłu nawiązali prywatne kontakty z niektórymi przedstawicielami amerykańskiej firmy, którym przekazali szereg danych o ofertach konkurentów;
- przedstawiciele niemieckiej firmy Aktiengesselschaft zaproponowali pracownikowi działu inwestycji w jednym z przedsiębiorstw łapówkę za udostępnienie cen, informacji o ofertach firm konkurencyjnych oraz danych techniczno-technologicznych projektu kontraktu sprzedanej instalacji prototypowej;
- przedstawiciel firmy niemieckiej nawiązał kontakt z pracownicą stoczni remontowej „Gryf" w Szczecinie, która przekazała mu informacje dotyczące prac remonto-

279 E. Bieńkowska-Higgins, *Agent James Bond w biznesmena przemieniony*, „Rzeczpospolita" z 16 października 1998 r.

wych na statkach, warunków negocjacyjnych i kontraktowych za remonty statków dla różnych zagranicznych armatorów.

W Polsce ukierunkowano zainteresowania wywiadu na uzyskiwanie informacji oraz dokumentacji z zakresu światowych osiągnięć naukowo-technicznych. Wywiad uczestniczył w pościgu za technologiami, za niedostępnym lub zbyt drogim sprzętem, za chronionymi wynalazkami i dokumentacjami[280].

Osiągnięcia polskich służb specjalnych w zakresie wywiadu gospodarczego nie odbiegają od norm światowych. Zdobycie nowych, interesujących nas technologii znacznie obniża koszty prac naukowo-badawczych**.** Powszechną normą stała się bardzo niebezpieczne przekonanie, że łatwiej wykraść nową technologię i ją usprawnić lub po prostu kradzioną sprzedać. Tego rodzaju praktyki stosowane na świecie są sprzeczne z zasadami ochrony własności intelektualnej[281]. Polscy specjaliści, a szczególnie polski wywiad nie odbiegają od światowych standardów. Świadczą o tym oficjalnie podawane sukcesy polskiego wywiadu. Przykładowo, w 1989 roku polski wywiad zdobył dokumentację wartości około 500 mln USD. Natomiast średnio rocznie przekazywał polskiej gospodarce około 800 rozwiązań technologicznych i dokumentacji pozwalającej na usprawnienie bieżącej produkcji lub na wdrożenie nowoczesnych rozwiązań na miarę osiągnięć światowych z takich dziedzin jak na przykład: elektronika, biotechnologia, chemia, rolnictwo i przetwórstwo żywnościowe, energetyka oraz medycyna i ochrona zdrowia.

## 5. Metody Dalekiego Wschodu

Specyficzne, jak na metody wywiadowcze, ale stare i wypróbowane są sposoby działania stosowane przez niektóre narodowości, a szczególnie przez Chińczyków i Japończyków.

Jednym z najgłośniejszych przykładów szpiegostwa przemysłowego naszych czasów pozostaje na razie zatrzymanie w 2001 roku na chicagowskim lotnisku O'Hare Jin Hanjuan, chińskiej informatyczki, która miała w bagażu ponad tysiąc stron tajnych dokumentów wyniesionych z Motoroli, gdzie pracowała jeszcze dwa dni wcześniej. Była szpiegiem na rzecz Huawei[282]. Cały pakiet miał dla Motoroli wartość 600 mln USD.

W Chinach szpiegostwo przemysłowe było otwarcie popierane przez władze jeszcze 30 lat temu. Znalazło to wyraz w tzw. Projekcie 863[283]; postawiono na pozyskiwanie technologii, które jak najmniejszym kosztem pomogłyby się uniezależnić od firm zachodnich. Nie wiadomo, ile nowoczesnych rozwiązań od tego czasu zostało „wyeksportowanych" do Chin. Metoda została określona jako *tysiące ziarenek piasku*, które po złożeniu miały tworzyć plażę.

Cechą charakterystyczną tej i podobnych metod jest minimalizowanie profesjonalnych służb wywiadowczych, a maksymalizowanie wysiłku wszystkich obywateli, którzy mogą być przydatni.

280 K. Dubiński. I. Jurczenko. *Być szpiegiem***,** Warszawa 1994, s. 24-25.

281 J.W. Wójcik, *Kryminologia. Współczesne aspekty*, Warszawa 2014 cz. II s. 137-278.

282 Huawei Technologies Co., Ltd. – chińskie przedsiębiorstwo, założone w 1987 roku, specjalizujące się w produkcji urządzeń i rozwiązań telekomunikacyjnych oraz informatycznych.

283 Nazwa pochodzi od daty – trzeci miesiąc 1986 roku.

Wykorzystywanie turystów, studentów, stypendystów i długoletnich mieszkańców na obczyźnie – daje niezwykłe efekty. To stwierdzenie zawarte jest w opublikowanym 25 maja 1999 roku raporcie (liczącym 900 stron) komisji Chrisa Coksa jako specjalnej komisji Kongresu, z którego ujawniono tylko niektóre informacje. Okazuje się, że przez ponad 20 lat Chiny bez przeszkód zdobywały informacje o kluczowych tajemnicach militarnych Stanów Zjednoczonych. Jednakże najważniejszym stwierdzeniem raportu było uświadomienie wszystkim zainteresowanym bezradności amerykańskich służb specjalnych wobec chińskich wywiadowców, którzy nie są szpiegami. Liczbę tego rodzaju chińskich szpiegów określono na miliony, a jednocześnie stwierdzono, że nie mają oni nic wspólnego z profesjonalnym wywiadem.

Wśród wielu pouczających wniosków ważne jest stwierdzenie, że rola profesjonalnych agentów może okazać się minimalna, natomiast praca wszystkich tych, którzy mają dostęp do interesujących informacji, a którym nie można nic zarzucić – przynosi niezwykłe efekty.

Strategia chińskich służb specjalnych, jak ujawniono w cytowanym raporcie, polega na pozyskiwaniu drobnych informacji od jak największej liczby osób i składaniu tej mozaiki w jedną całość. Z tego względu chiński wywiad utrzymuje oraz systematycznie rozbudowuje kontakty z wielką liczbą potencjalnych informatorów, którzy są najczęściej: biznesmenami, menedżerami, inżynierami, naukowcami, stypendystami, studentami, ale również zwykłymi turystami. Po powrocie do kraju dzielą się oni swoimi spostrzeżeniami z pracownikami służb specjalnych. Po takich rozmowach powstają kolejne elementy mozaiki informacyjnej.

Wspomniany powyżej napływ informacji, składających się z najróżnorodniejszych danych zapewniają następujące źródła:

- chińscy studenci, których stała liczba w USA wynosi około 100 tysięcy,
- turyści i delegowani służbowo Chińczycy, którzy co roku odwiedzają USA w liczbie około 80 tysięcy osób,
- Amerykanie chińskiego pochodzenia, aktywni w różnego rodzaju sferach życia publicznego, których oblicza się na kilkanaście milionów osób.

Komisje Kongresu, CIA i FBI systematycznie prowadzą dochodzenia w celu ustalenia winnych ujawnienia najbardziej strzeżonych tajemnic ze strategicznych laboratoriów i przedsiębiorstw. Chodzi również o ustalenie sposobów omijania przepisów dotyczących zasad eksportu do Chin technologii o charakterze strategicznym.

Raport Coxa zaskoczył Amerykanów, chociaż części zawartych w dokumencie faktów wciąż nie podano do wiadomości publicznej[284]. Opublikowana część dobitnie szacowała ogrom strat poniesionych przez USA, a także uświadomiła wszystkim, jak bezradne są amerykańskie służby specjalne wobec działań chińskich „szpiegów", których liczba sięga milionów i którzy formalnie nie mają nic wspólnego z zawodowym wywiadem.

Komisja bez trudu ustaliła, że dwie amerykańskie firmy i kilka innych przedsiębiorstw dostarczyły Chinom technologie, które umożliwiły szybkie unowo-

284 K. Darewicz, *Szpiegostwo bez szpiegów*, „Rzeczypospolita" z 7 czerwca 1999 r.

cześnienie chińskich rakiet balistycznych, i że Pekin najprawdopodobniej dokonał modernizacji swego arsenału nuklearnego. Niemal jedna trzecia raportu jest poświęcona korporacjom Loral i Hughes. Produkowane przez nie satelity miały być umieszczone na orbicie przez chińskie rakiety nośne, ale wszystkie te rakiety, w latach 1992, 1995 i 1996, eksplodowały tuż po starcie, a satelity uległy zniszczeniu. Obie korporacje tak ochoczo pomagały Chińczykom w ustalaniu przyczyn katastrof, że w rezultacie dostarczyły im większość informacji, które chińska armia wykorzystała do modernizacji rakiet balistycznych.

Ustalono również, iż Pekin zdobył nie tylko plany głowic nuklearnych, ale i poznał tajniki budowy broni elektromagnetycznych, które mogą służyć do zwalczania z kosmosu satelitów, rakiet i łodzi podwodnych. Ponadto, Chińczycy uzyskali dane o niezliczonych detalach amerykańskiego uzbrojenia, od systemów naprowadzających dla myśliwców i czołgów, po laserowe urządzenia umożliwiające symulację eksplozji nuklearnych w warunkach laboratoryjnych i superszybkie komputery.

Opublikowane wyniki dochodzeń budzą szereg wątpliwości, przede wszystkim z uwagi na brak podejrzanych. Natomiast niektóre efekty strategii chińskich służb specjalnych ilustrują poniższe przykłady*:*

- dr Peter Lee, naukowiec pracownik laboratorium w Los Alamos, pochodzący z Tajwanu, w czasie dwóch legalnych wizyt naukowych w Chinach, zdaniem FBI, ujawnił ekspertom technikę laserowej symulacji eksplozji nuklearnych i konstrukcje radarów służących do wykrywania atomowych okrętów podwodnych. Na wspomniane badania amerykańskie ośrodki badawcze wydały kilkadziesiąt miliardów dolarów. Jednakże nie zdołano przedstawić mu jakichkolwiek zarzutów.
- Jeszcze bardziej żenująca dla amerykańskich służb specjalnych jest sprawa dr. Wen Ho Lee. Urodzony na Tajwanie, posiadający amerykańskie obywatelstwo naukowiec, przez dwadzieścia lat pracował w najtajniejszej Sekcji X laboratorium nuklearnego Los Alamos, które opracowało najnowocześniejszą zminiaturyzowaną głowicę atomową W-88. Dr Lee pewnie do dziś nie wzbudziłby podejrzeń, gdyby w 1988 roku pewien Chińczyk, podający się za agenta chińskiego wywiadu, nie przekazał agentowi CIA na Tajwanie dokumentów świadczących, że Chiny weszły w posiadanie tajemnic konstrukcyjnych wszystkich rodzajów amerykańskich głowic nuklearnych. Ale dopiero po kilku latach FBI rozpoczęło obserwację dr. Lee i po raz pierwszy poddało go przesłuchaniu. Naukowca aresztowano przedstawiając mu zarzuty, które dotyczyły działalności w latach 1993-1997. Dr Lee przekopiował z komputera w laboratorium Los Alamos na swój prywatny komputer dane o praktycznie wszystkich sekretach atomowych Stanów Zjednoczonych: detale konstrukcyjne głowic nuklearnych, kody służące do ich detonacji, wyniki próbnych eksplozji i szczegóły wykrytych w ich trakcie problemów oraz programy służące do konstruowania głowic i przeprowadzania testów. W tej sprawie doszło do wyroku skazującego jedynie na: 12 miesięcy aresztu domowego, 3000 godzin pracy społecznej na rzecz gminy i 20.000 USD grzywny.

Problemem było ustalenie metod działania. Dopiero współpraca komisji z FBI i CIA doprowadziła do ustaleń również w tym zakresie. Okazało się, że wiosną 1995 roku pewien Chińczyk przekazał rezydentowi CIA na Tajwanie kilkaset stron dokumentów zawierających między innymi informację, że chińska

armia znacznie wcześniej zdobyła projekt zminiaturyzowanej głowicy atomowej W-88 najnowocześniejszej w amerykańskim arsenale, w którą uzbrojone są rakiety D-5 wystrzeliwane z atomowych okrętów podwodnych Trident. Chińczycy poznali również budowę sześciu innych rodzajów głowic nuklearnych, w tym tzw. bomby neutronowej, czyli dopiero przygotowywanej do uzbrojenia amerykańskich rakiet głowicy W-70.

Prowadzone dochodzenie wykazało, że Chińczycy już od co najmniej 20 lat swobodnie zdobywali szereg cennych informacji. Jednakże trudno było zrozumieć, dlaczego przez tyle lat Chińczycy nie napotykali żadnych większych trudności przy zdobywaniu militarnych sekretów największego mocarstwa świata. W raporcie Coksa wymieniono wiele metod, jakie stosowali Chińczycy, by osiągnąć swój cel. Na liście tej brakuje zarzutów pod adresem chińskich szpiegów. To właśnie najlepiej wyjaśnia, dlaczego Pekinowi aż tak się powiodło.

Chińskie służby specjalne działają odmiennie niż zachodnie. Rola zawodowych agentów jest minimalna, bo na potrzeby wywiadu pracują wszyscy mogący mieć dostęp do interesujących informacji i każda z takich osób jest i poniekąd „szpiegiem", choć formalnie nie można jej tego zarzucić. Strategia chińskich służb specjalnych polega na pozyskiwaniu drobnych informacji od jak największej liczby osób i składaniu tych danych w całość. W tym celu chiński wywiad utrzymuje i rozbudowuje kontakty z ogromną liczbą potencjalnych informatorów – naukowców, inżynierów, biznesmenów, studentów, itp. Każdy z nich po powrocie z zagranicy do Chin dzieli się z pracownikami służb specjalnych swymi spostrzeżeniami i dokłada kolejny element do układanki.

Zważywszy na fakt, że tylko do Stanów Zjednoczonych przyjeżdża co roku służbowo około 80 tysięcy Chińczyków, a stale uczy się tu około 100 tysięcy chińskich studentów, zapewnia to Pekinowi ogromny, płynący nieprzerwanie strumień rozmaitych danych. Ponadto wywiad szczególnie dba o dogłębną infiltrację kilkunastomilionowej społeczności Amerykanów chińskiego pochodzenia, uczestniczących we wszystkich sterach życia USA. Toteż do zdobycia technologii takiego czy innego rodzaju amerykańskiego uzbrojenia mogło przyczynić się kilkudziesięciu, kilkuset lub nawet kilka tysięcy informatorów, a nie jeden czy dwóch zawodowych agentów.

W takiej sytuacji prawnej amerykańskie służby specjalne, jak się okazałobyły bezradne wobec zastosowanej strategii i nieprzygotowane do przeciwdziałania. Lee pozostaje ciągle na wolności, bo FBI nie jest w stanie postawić mu żadnych konkretnych zarzutów.

Wśród wielu sukcesów chińskich służb specjalnych wymienia się zdobycie:

- planów i technologii głowic nuklearnych, a w tym W – 88,
- tajemnic budowy broni elektromagnetycznych służących do zwalczania satelitów,
- szeregu tajemnic dotyczących nowoczesnych rakiet i łodzi podwodnych,
- licznych detali amerykańskiego uzbrojenia, od systemów naprowadzających dla myśliwców i czołgów, po laserowe urządzenia umożliwiające symulację eksplozji nuklearnych w warunkach laboratoryjnych;
- superszybkich komputerów, które niewątpliwie mają walory strategiczne.

## 6. Inne rozpoznane metody i zagrożenia

Poznając wybrane efekty działalności wszelkiego rodzaju wywiadów, trzeba chyba dać wiarę temu, co twierdzi były agent CIA, a mianowicie: *Działalność wywiadowcza jest jak pornografia: skryta i zakazana. Na pierwszy rzut oka sprawia wrażenie ekscytującej i ważnej, ale tak naprawdę jest niezwykle nudna. W miarę odkrywania się przed obserwatorem staje się mniej interesująca*[285].

Analiza literatury przedmiotu, a szczególnie informacji medialnych, prowadzi do interesujących wniosków. Nie ulega wątpliwości, że omawiane zagadnienie jest przedmiotem szerokiego zainteresowania zarówno mediów, jak i wielu środowisk społecznych. Nie są to informacje niejawne, lecz niektóre z nich były niejawne w przeszłości, a przykładowo:

- W 1997 roku FBI prowadziła ponad 700 dochodzeń o szpiegostwo przemysłowe, z których wynika istotna rola obcych firm i instytucji rządowych. Wykradano nie tylko dokumentacje związaną z nowymi wynalazkami i wyniki najnowszych prac badawczych, lecz również plany produkcyjne, marketingowe oraz listy klientów.
- Najnowsze kierunki zainteresowań wywiadów gospodarczych dotyczą biotechnologii, a szczególnie produkcji hormonów, osiągnięć genetyki i farmakologii.
- Wielkie organizacje nie żałują pieniędzy na zdobycie technologii produkcji nowych leków. Niejednokrotnie nie chodzi wcale o pomoc chorym, zdarza się, że celem tego działania zaborczych korporacji jest sprawowanie kontroli nad nowymi wynalazkami i technologiami.

Z wielu źródeł, nie zawsze oficjalnych wynika, że nie tylko USA ale i inne potęgi gospodarcze, walcząc o dominację ekonomiczną, Japonia, Niemcy, Francja i Wielka Brytania, są wspierane przez rządowe agencje gospodarcze.

Niemiecki kryminolog H. Cornwall w odniesieniu do wywiadu ZSRR podaje, że według jego informacji do roku 1980 ten wywiad uzyskał 4.502 wzorce różnego rodzaju sprzętu technicznego i 25.453 komplety dokumentacji technicznej dotyczącej nowych urządzeń. Działalność wywiadu ZSRR w postaci wspomnianych zdobyczy przyczyniła się do zaoszczędzenia 407,5 mln rubli, zainicjowała 200 nowych projektów oraz przyspieszyła zrealizowanie 1.458 projektów, nad którymi trwały prace naukowo-badawcze.

Podsumowując, można zatem stwierdzić, że osiągnięcia polskich służb specjalnych w zakresie wywiadu gospodarczego nie odbiegają od norm światowych. Zdobycie nowych, interesujących nas technologii znacznie obniża koszty prac naukowo – badawczych**.** Świadczą o tym oficjalnie podawane sukcesy polskiego wywiadu. Przykładowo, w 1989 roku polski wywiad zdobył dokumentację wartości około 500 mln USD. Rocznie przekazywał polskiej gospodarce około 800 rozwiązań technologicznych i dokumentacji pozwalającej na usprawnienie bieżącej produkcji lub na wdrożenie nowoczesnych rozwiązań na miarę osiągnięć światowych z takich dziedzin jak na przykład: elektronika, chemia, rolnictwo i przetwórstwo żywnościowe, energetyka oraz medycyna i ochrona zdrowia.

Duane R. Clarridge – autorytet w zakresie działań wywiadowczych w drugiej połowie XX wieku, długoletni agent CIA zamieścił kilka uwag na temat wywiadu gospodarczego w swojej książce pt. *Po prostu szpieg.* Ekspert ten uważa, że:

285 J. Rusbridger, *Gra wywiadów. Iluzje i pozory szpiegostwa międzynarodowego*, Warszawa 1993, s. 282.

*Wywiad gospodarczy jest kolejnym problemem tajnych służb, który stał się tematem publicznej debaty. Wywiad gospodarczy należy podzielić na dwie części. Jedna z nich to zwykły wywiad gospodarczy, czyli informacje, które pomagają rządowi federalnemu w negocjacjach handlowych z innymi krajami, stanowią dane dla Federalnego Banku Rezerw, dotyczące zmian kursów zagranicznych banków centralnych, zapewniają, że za granicą nie nastąpi jakiś niespodziewany przełom technologiczny itp. Informacje te nie pomagają bezpośrednio konkretnej gałęzi przemysłu czy przedsiębiorstwu, ale wspierają politykę rządu federalnego. W przeszłości tajne służby mogły być dumne z sukcesów odniesionych w tej dziedzinie.*

*Drugim składnikiem wywiadu gospodarczego jest szpiegostwo przemysłowe, którego zadaniem jest zbieranie informacji biznesowych (negocjacje kontraktowe, „tajemnice handlowe", procesy produkcji itp.). Ani CIA ani też żadna inna amerykańska agencja wywiadowcza nie jest zaangażowana w szpiegostwo przemysłowe. Ponieważ Francuzi, Izraelczycy, Rosjanie, Japończycy, Chińczycy i prawie wszystkie inne kraje dysponujące solidną bazą technologiczną są w to zaangażowane, niektórzy argumentują, że tajne służby także powinny to robić, dla wspierania amerykańskiego przemysłu. Tajne służby wystrzegają się tego typu działalności…* Przede wszystkim dlatego, że sukcesy amerykańskiego biznesu za granicą nie mają wpływu na bezpieczeństwo narodowe, a trudno byłoby sprawiedliwie przekazywać zyski amerykańskiemu biznesowi".[286]

Bardziej zwięźle przedstawia to zagadnienie De Marenches (szef francuskich tajnych służb w latach 1970-1981), zatem ekspert i praktyk, w swoich opublikowanych wspomnieniach pisze *Szpiegostwo we właściwym znaczeniu coraz bardziej koncentruje się na interesach i gospodarce oraz nauce i przemyśle. Jest ono niezmiernie korzystne. Umożliwia poznawanie metod stosowanych w innym kraju, których wynalezienie lub udoskonalenie zabrałoby całe lata i kosztowałoby nieraz miliony franków* [287].

Od kilku lat dostrzegane są narastające zagrożenia związane ze szpiegostwem gospodarczym, przemysłowym czy technologicznym. Z raportu Biura Dyrektora Krajowego Kontrwywiadu USA (*Office of the National Counterintelligence Executive*) dla Kongresu z 2011 roku pt. „Zagraniczni szpiedzy wykradają gospodarcze tajemnice USA w cyberprzestrzeni", obejmującego analizę działań szpiegowskich skierowanych przeciwko amerykańskiej gospodarce w latach 2009-2011 wynika, że cyberprzestrzeń z racji swoich unikalnych właściwości jest szczególnie podatna na akty cyberszpiegostwa. Dzisiaj liczącymi się aktorami w tym procederze są nie tylko państwowe służby specjalne, lecz przede wszystkim konkurencyjne przedsiębiorstwa, instytuty badawcze, uniwersytety, a także pojedynczy, wynajęci do konkretnego zlecenia hakerzy. Analizy wydarzeń na rynkach światowych wykazują, że cyberprzestrzeń sprzyja szpiegostwu przemysłowemu z kilku podstawowych powodów, a mianowicie:

1. trudniej jest wykryć sprawców operacji szpiegowskich;
2. sprawcą kradzieży informacji w cyberprzestrzeni może być pojedyncza osoba, słabe państwo albo niewielkie przedsiębiorstwo, na tyle zasobne jednak, aby wynająć

286 D.R. Clarridge, *Po prostu szpieg*, Warszawa 2001, s. 339, 340.

287 H. de Marenches, *Dans les secrets desprinces*, Paris 1986, s. 8.

zdolnego hakera będącego w stanie wykorzystywać złośliwe oprogramowania lub kraść wrażliwe informacje;

3. w cyberprzestrzeni trudniej o ustalenie prawdziwych motywów działania szpiegowskiego;
4. cyberprzestrzeń oferuje większe bezpieczeństwo sprawcom z wewnątrz danej organizacji, czyli nie ma potrzeby fizycznego spotkania pomiędzy skorumpowanym pracownikiem a „kupcem", co redukuje prawdopodobieństwo wykrycia;
5. ten rodzaj szpiegostwa jest szybszy i tańszy**,** a cyberprzestrzeń umożliwia niemal natychmiastowy transfer ogromnej ilości informacji[288].

W zgodnej opinii służb specjalnych USA i państw zachodnich, ale także wielkich korporacji, palmę pierwszeństwa w tym względzie dzierżą Chiny i Rosja. Z siedmiu przypadków szpiegostwa przemysłowego w 2010 roku, które miały miejsce w USA, sześć wiązało się z aktywnością Chin. Z napływających informacji wynika, że działania tych państw wykazują stałą tendencję wzrastającą.

Działalność w ramach szpiegostwa gospodarczego istotnie zagraża bezpieczeństwu, funkcjonowaniu i nowatorskim przedsięwzięciom wielu organizacji gospodarczych, przemysłowych, finansowych, naukowych i innych. Nie ulega wątpliwości, że penetrowane są szczególnie firmy z tzw. sektora nowoczesnej technologii, jak na przykład firmy informatyczne i jednostki naukowe oraz badawczo-rozwojowe.

Według Francuskiego Urzędu Ochrony Konstytucji lista dziedzin, którymi w 1989 roku interesowały się wywiady krajów socjalistycznych, w tym również wywiad polski, to obok technologii militarnych technologie dotyczące komunikacji lotniczej, kosmicznej, radarowej, technika laserowa, optyka oraz mikroelektronika. W ramach tej ostatniej dziedziny Polska zajmowała się głównie technologią półprzewodników, numerycznymi urządzeniami sterującymi i komputerami dużej mocy. Według tego samego źródła, polski wywiad w dziedzinie przemysłu chemicznego szukał przede wszystkim informacji na temat produkcji z tworzyw sztucznych oraz innych technologii o podwójnym zastosowaniu, tj. w sektorze cywilnym i wojskowym. Przykładem takiej technologii może być analizator spektralny fal dźwiękowych, który ongiś został legalnie zakupiony przez wywiad b. ZSRR. Natomiast po kilku latach okazało się, że znalazł on zastosowanie w tłumieniu szumów radzieckich okrętów podwodnych.

Nie ulega wątpliwości, że działalność w ramach szpiegostwa gospodarczego, przemysłowego czy naukowo technologicznego swoje zainteresowania ukierunkowuje na zdobywanie zaawansowanych technologii oraz szybkie ich wdrażanie w cyklach produkcyjnych. Szpiegostwo przemysłowe jest tak stare, jak ludzkość. Już od najdawniejszych czasów ludzie usiłowali przyswoić sobie nowe lub bardziej doskonałe technologie w sposób najłatwiejszy, tzn. po prostu kradnąc je temu, kto je posiadał. Specyficzną cechą szpiegostwa przemysłowego – w odróżnieniu od wojskowego i politycznego – bywa fakt, że często skierowane jest ono również przeciwko konkurencyjnym firmom w tym samym państwie. W swoim działaniu stosuje ono środki rzeczywistego szpiegostwa w postaci werbowania agentów, tajnego fotografowania, kopiowania dokumentów, podsłuchiwania ltd. Inne zadanie realizuje wywiad ekonomiczny (wywiad wojskowy), który rozpoznaje potencjał ekonomiczny i jego wpływ

288 M. Ciecierski, *Szpiegostwo przemysłowe opanowało cyberprzestrzeń* http://biznes.pl/wiadomosci/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen,5402264,news-detal.html(28.11.2014).

na możliwości obronne kraju. Na pojęcie to składa się całokształt produkcji, dystrybucji i konsumpcji. Na podstawie działalności wywiadowczej, ustalającej produkcję, sposoby dystrybucji oraz poziom konsumpcji wysnuwane są wnioski, jak cały organizm gospodarczy może funkcjonować w okresie zagrożenia, napięć, czy też w warunkach wojennych. Wywiad ekonomiczny jest o tyle skomplikowany, że jego działanie me wywołuje – np. w okresie pokoju – natychmiastowych skutków ujemnych. Kieruje swe zainteresowania na obiekty zarówno o kapitalnym znaczeniu, jak i zdawałoby się niewiele mające wspólnego z obronnością kraju, np. wodociągi. Jednak wodociągi w ogromnych aglomeracjach stanowią obiekt, który ma kapitalne znaczenie dla wywiadu ekonomicznego. Znać to miejsce i urządzenia, to mieć możliwość szybkiego zatrucia wody w całej sieci[289].

W Polsce ukierunkowano zainteresowania wywiadu na uzyskiwanie informacji oraz dokumentacji z zakresu światowych osiągnięć naukowo-technicznych. Wywiad uczestniczył w pościgu za technologiami, za niedostępnym lub zbyt drogim sprzętem, za chronionymi wynalazkami i dokumentacjami[290].

Rozmiary zagrożeń w latach 90. XX wieku dość dobrze rozpoznało amerykańskie towarzystwo bezpieczeństwa przemysłowego, które podaje, że ujawnione straty sięgały wówczas 300 mln USD w wyniku 1100 udokumentowanych i 550 prawdopodobnych przypadków szpiegostwa przemysłowego w kilku tysiącach największych firm USA. Ustalono, że szpiedzy przemysłowi otrzymują zlecenia z firm USA, Chin, Japonii, Francji i Wielkiej Brytanii. Okazało się, że przemysłowe firmy amerykańskie szpiegowane są również przez agencje rządowe Francji, Niemiec, Izraela, Chin i Korei Południowej[291].

W 1997 roku FBI prowadziła ponad 700 dochodzeń o szpiegostwo przemysłowe, z których wynika istotna rola obcych rządów. Wykradano nie tylko dokumentację związaną z nowymi wynalazkami i wyniki najnowszych prac badawczych, lecz również plany produkcyjne, marketingowe oraz listy klientów. Nic więc dziwnego, że prezydent Bill Clinton nakazał Centralnej Agencji Wywiadowczej traktować zbieranie informacji z zakresu wywiadu gospodarczego jako najważniejsze zadanie wywiadowcze okresu, który nastąpił po zimnej wojnie. Media w USA wspominają o tajnej dyrektywie prezydenta Billa Clintona, który polecił przesunięcie znacznych sił i środków z dotychczasowych, tj. tradycyjnych operacji wywiadowczych, czyli poprzednio ukierunkowanych m.in. na rozpoznawanie rosyjskiego potencjału nuklearnego – na realizację zadań w ramach szpiegostwa gospodarczego skierowanego przeciwko rywalom gospodarczym USA. Wkrótce zaowocowało to istotnymi sukcpesami. Przykładowo, CIA poinformowała Kongres, że w przeciągu kilku ostatnich lat wykryto usiłowania wręczenia wielkich łapówek w trakcie negocjowania kontraktów gospodarczych. Próby korupcji oceniono na sumę około 30 miliardów dolarów.

Zarówno CIA, jak i inne profesjonalne wywiady państwowe, zatrudniają wielu specjalistów, analityków komputerowych, a także ekspertów w dziedzinie informatyki, oprogramowania i elektroniki oraz wielu innych dziedzin mających niezwykle ważne znaczenie dla gospodarki. Pozwala to na szybkie przyswojenie zebranych informacji, ocenę ich znaczenia oraz ukierunkowanie ich wykorzystania.

289 Z. Bagiński, *Wywiad***,** Warszawa 1975, s. 68-69.

290 K. Dubiński. I. Jurczenko**.** *Być szpiegiem,* Warszawa 1994, s. 24-25.

291 S. Walczak, *Szpiegostwo przemysłowe*, „Rzeczpospolita" z dnia 15 stycznia 1998 r.

W strategii zarządzania wielkimi korporacjami, których dochody nierzadko plasują się na poziomie niektórych państw, działalność wywiadu gospodarczego i naukowo-technicznego wydaje się czymś naturalnym. Z tego względu wielkie organizacje gospodarcze, a niejednokrotnie nawet małe firmy organizują wyspecjalizowane wydziały, które zajmują się profesjonalnym zbieraniem i analizowaniem informacji. Niektórzy specjaliści doszli do perfekcji, której mogą pozazdrościć nawet pracownicy CIA, MI6, Mosadu, KGB i innych wywiadów. Na marginesie warto zaznaczyć, że to właśnie profesjonaliści z tych wywiadów zasilili komórki wszystkich rodzajów wywiadu gospodarczego.

Osiągnięcia współczesnej informatyki w naturalny sposób ukierunkowują zainteresowania wszelkiego typu wywiadów w stronę baz danych gromadzących, przechowujących, przetwarzających i przekazujących informacje. Systemy informatyczne to obecnie najbardziej wrażliwe i najbardziej zagrożone obiekty. Wymagają one szczególnej ochrony, która powszechnie określana jest jako polityka bezpieczeństwa, czyli strategia ochrony tych systemów.

Powiązania wywiadu gospodarczego i naukowego z wywiadem wojskowym są oczywiste, chodzi bowiem o zdobywanie nowych technologii przeciwnika i zaoszczędzenie olbrzymich wydatków na prowadzenie własnych badań naukowych.

Tak np. było ze zdobywaniem sprzętu komputerowego najnowszej generacji. Produkowany w latach 70. w krajach b. Rady Wzajemnej Pomocy Gospodarczej komputer RIAD II to kopia IBM 370, a mikrokomputer AGAT to kopia APPLE II. Legalny zakup technologii informatycznych nie był wówczas możliwy z uwagi na embargo nałożone na kraje socjalistyczne. W tej sytuacji niektóre firmy zachodnie nielegalnie dostarczały sprzęt komputerowy do b. ZSRR. Ilustracją tego stwierdzenia może być wykryta w 1983 roku afera dotycząca sprzedaży 11 kontenerów ze sprzętem zawierającym części komputera VAX.

## 7. Kompleksowe gromadzenie informacji w interesie bezpieczeństwa narodowego

Niektóre media w USA, jak np.: „Wired”[292], „The Week Magazine”[293], „Huffington Post”[294], „The Philly Post”[295] – żywo interesują się i komentują zasady przechwytywania i rejestrowania przez służby specjalne takich informacji jak: wszystkich rozmów telefonicznych, e-maili, SMS-ów oraz wszystkich szczegółów elektronicznych transakcji finansowych (rachunki bankowe, numery i rachunki kart kredytowych), a nawet takich danych z zakresu służb państw obcych jak tajne depesze dyplomatyczne, przekazywane informacje wojskowe, raporty o przebiegu rokowań dyplomatycznych i handlowych**,** dane giełdowe, rozmów telefonicznych, słowa klucze wpisywane do Google’a, dane o zakupach książek, rezerwowanych podróżach, a nawet dane o opłatach parkingowych, itp. Nie gardzi się nawet najmniej wartą informacją[296].

292 http://www.wired.com/magazine/(12.02.2011)

293 http://theweek.com//(12.02.2011)

294 http://content.usatoday.com/topics/topic/Organizations/Companies/Publishers,+Media,+Music/Huffington+Post/ (12.02.2011)

295 http://blogs.phillymag.com/the_philly_post//(12.02.2011)

296 C. Stolarczyk, *Wielkie ucho Wielkiego Brata*, „Angora” nr 27 z 8 lipca 2012 r.

Zdaniem mediów dane te są potajemnie przejmowane, magazynowane i odszyfrowywane. W takiej sytuacji informacja najbardziej chroniona i termin tajemnica tracą rację bytu.

Wszystko to ma związek z nowym terminem i nazwą *Utah Data Center*, której koncepcja narodziła się po wydarzeniach z 11 września 2001 roku. Zasadniczym celem tego projektu jest uchronić się przed ewentualnymi konsekwencjami, czyli skutecznie przeciwdziałać, wykryć i unieszkodliwić zagrożenie, nim dojdzie do jego realizacji[297]. Ta super tajna, największa na świecie inwestycja powstaje na odludziu w stanie Utah. Prace trwają od początku 2011 roku, a dotychczas na kosztowały ponad 2 miliardy USD.

Anonimowi funkcjonariusze wywiadu stwierdzają (zapewne za cichą wiedzą swoich szefów), że - *Teraz każdy jest celem, każdy, kto się komunikuje, czyli każdy kto wymienia informacje – znajdzie się w odpowiednim zbiorze działającym pod egidą największej agencji wywiadu elektronicznego, czyli National Security Agency - NSA*. Zadaniem tej agencji jest: potajemnie przechwytywać, analizować, magazynować i dekodować wszystkie impulsy i sygnały emitowane przez wszelkie stacje nadawcze i przekaźniki za pośrednictwem satelitów, podziemnych i podwodnych kabli telekomunikacyjnych. Ogromne hale serwerów i urządzeń do przechowywania pamięci elektronicznej pomieszczą przesyłane informacje finansowe,

Do takich działań niezbędna jest niezwykle obszerna objętość pamięci, która z łatwością pomieści miliony jawnych stron internetowych funkcjonujących na świecie. Operatorzy będą mieli na uwadze dane chronione, kodowane i opatrzone hasłami, najczęściej stosowane w komunikacji rządowej i militarnej.

Projektanci z Pentagonu lansują prognozy, które przewidują kilkakrotne nasilanie się ruchu w Internecie do roku 2015, w którym liczba ludzi z połączeniem internetowym osiągnie do 2,7-3,0 mld. Zatem tak rozbudowują sieć stacji przechwytujących na świecie, żeby mogły one wchłaniać dane o rozmiarach $10^{15}$ bajtów na sekundę. Nikt inny nie dysponuje czymś porównywalnym.

Wprawdzie nowy komputer jest znacznie szybszy niż „Jaguar" – skonstruowany w 2009 roku jako najszybszy wówczas komputer świata. Jednakże to nie koniec zamierzeń rządowych, gdyż specjaliści pracują nad superkomputerem o większej szybkości operacji, tj. do $10^{21}$ na sekundę, uzasadniając to następująco: „Czego nie możemy rozszyfrować dziś, rozszyfrujemy jutro. Ekstrapolując dane z przeszłości, będziemy w stanie z większą dozą prawdopodobieństwa przewidywać aktualne i przyszłe decyzje rządów innych państw"[298]. Przykładowo, szacuje się, że w okresie dziesięciolecia po 11 września 2001 r. – przechwycono między 15 a 20 bilionów różnorodnych informacji i przekazów.

W okresie rządów George'a Busha wykryto, że NSA nielegalnie, czyli bez zgody sądu, gromadziła informacje, inwigilowała i podsłuchiwała prywatnych obywateli. Sprawy kwalifikowały się do sądu, ale w roku 2008 Kongres USA zalegalizował prawnie taką działalność ze względu na bezpieczeństwa narodowe.

297 Szacuje się, że w okresie dziesięciolecia po 11 września 2001 r. – przechwycono między 15 a 20 bilionów różnorodnych informacji i przekazów, bez względu na to czy były jawne czy chronione?

298 C. Stolarczyk, *Wielkie ucho Wielkiego Brata*, „Angora" nr 27 z 8 lipca 2012 r.

Niektórzy eksperci potrafią udowodnić, że mało istotne są oficjalne zgody i zezwolenia. Wiele afer w USA, chociażby Snowdena czy Wikileaks, a także w innych krajach, a nawet w Polsce udowodniło, że prywatne wywiady mogą wiele uczynić wbrew interesom państwa. Na tym tle doszło do wielu kompromitujących sytuacji. Przykładowo, niemieckie media zebrały materiały na temat nielegalnego podsłuchiwania nie tylko Angeli Merkel, na co są twarde dowody, o których alarmował Edward Snowden, ukrywający się w Moskwie, ale również od lat 90. XX wieku podsłuchiwano niemieckie resorty finansów, gospodarki i rolnictwa, gdy problemem było ratowanie greckiej gospodarki.

Kolejny specjalista w publikowaniu tajnych materiałów Julian Assange – założyciel platformy internetowej, bardzo przysłużył się w publikowaniu wykradzionych tajnych dokumentów. Tylko w 2010 roku zdobył dziesiątki tysięcy amerykańskich depesz dyplomatycznych, także o podsłuchiwaniu przez NSA francuskich prezydentów, pomimo że od 2012 roku sam ukrywa się w Ambasadzie Ekwadoru w Londynie, ścigany za popełnienie przestępstw seksualnych.

Po lekturze tego fragmentu książki Czytelnik ma podstawy do zastanowienia się nad kilkoma problemami, z których czołowy dotyczy zasad rzetelnej informacji na temat potrzeby i zasad ochrony różnego rodzaju danych.

# Rozdział 6

# Analiza działalności wywiadowczej i ocena gromadzonych informacji

## 1. Podstawowe zasady działania wywiadu i kontrwywiadu gospodarczego

Wywiad i kontrwywiad gospodarczy spełniają niezwykle istotną rolę w zapewnieniu bezpieczeństwa przedsiębiorstwa i uzyskaniu najlepszych warunków jego rozwoju. Kluczowymi przesłankami działania są istnienie społeczeństwa informacyjnego i nieustanny postęp w dziedzinie techniki informatycznej. Wiąże się to z narastającym systematycznie zapotrzebowaniem na specjalistyczne usługi informacyjne, a w tym o charakterze wywiadowczym i kontrwywiadowczym.

Swoisty rozwój inteligencji cyberprzestrzeni, obszarów wirtualnych i cyfrowych dotyczy nie tylko uprawnionych przedsiębiorstw i służb. Dotyczy to wszystkich sektorów gospodarki. Tym złożonym procesom towarzyszy stała, o charakterze lawinowym, rewolucja elektroniczna. Rozwój komputeryzacji wiąże się ze zmianą środków i metod pozyskiwania informacji, co pociąga za sobą potrzebę zmiany metod pracy.

Działalność wywiadowcza i kontrwywiadowcza wywiadu państwowego, to wiele wzajemnie powiązanych, współzależnych i uzupełniających się przedsięwzięć, które można określić cyklem wywiadowczym lub cyklem kontrwywiadowczym[299]. Wspomniane cykle można porównywać z wywiadem i kontrwywiadem gospodarczym.

Cykl wywiadowczy służby państwowej obejmuje wszystkie fazy działalności służby wywiadu, o d planowania poczynając, na dystrybucji gotowego materiału wywiadowczego kończąc. Cykl ten dzielony jest zazwyczaj na pięć etapów, na które składają się następujące działania wywiadu i kontrwywiadu gospodarczego:

1. planowanie i ukierunkowanie pracy operacyjnej wywiadu, sposobów zdobycia informacji oraz kontrola efektywności działania jednostek zajmujących się jej gromadzeniem,
2. gromadzenie, proces zdobywania informacji i przekazywania ich do dalszej obróbki,
3. przetwarzanie, proces porządkowania i ujednolicenia uzyskanych informacji czy ujednolicenie formatu danych teleinformatycznych,
4. wytwarzanie, proces przekształcania informacji przetworzonej w gotowe dane wywiadu, obejmujący analizę, ocenę i interpretację,

299 Por.: A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 248.

5. przekazywanie, dystrybucja danych wywiadowczych dla uprawnionych użytkowników[300].

Natomiast cykl kontrwywiadu państwowego, to zespół czynności właściwych dla zespołu kontrwywiadu, który może składać się z następujących przydatnych etapów, a mianowicie:

1. planowanie i ukierunkowanie działań na podstawie istniejących zagrożeń dla przedsiębiorstwa w powiązaniu ze sposobami zdobywania informacji oraz kontrolą efektywności,
2. rozpoznawanie, gromadzenie oraz poszukiwanie sygnałów dotyczących zagrożeń dla bezpieczeństwa przedsiębiorstwa i przekazywanie ich do dalszych kompetentnych analiz,
3. przetwarzanie, weryfikacja zdobytych informacji i materiałów, które potwierdzają istniejące zagrożenia, analiza, ocena i interpretacja,
4. wszczęcie postępowania analitycznego, dalszy sposób postępowania przy zastosowaniu odpowiednich, w zależności od potrzeb metod i środków, ze szczególnym uwzględnieniem gromadzenia informacji o zdarzeniu, osobie lub grupie osób,
5. przekazywanie, dystrybucja danych kontrwywiadowczych dla uprawnionych użytkowników (na przykład członka zarządu przedsiębiorstwa ds. bezpieczeństwa)[301].

Analiza treści uzyskanych informacji, bez względu na rodzaj wywiadu, powinna pozwolić na ich weryfikację oraz wnioskowanie, a mianowicie:

1. czy uzyskana informacja, na podstawie dotychczasowych ustaleń jest prawdopodobna?
2. czy informacja została skonfrontowana i porównana z informacjami uzyskanymi z innych źródeł?
3. czy treść informacji zgadza się z posiadanymi danymi, a szczególnie z tymi, które uznano za autentyczne. Jeżeli informacja przedstawia dane odmienne od danych uzyskanych z innych źródeł, pozostaje właściwym sposobem wyjaśnić, która z tych informacji jest prawdziwa[302].

## 2. Wywiad biały i czarny – formalny i nieformalny

W literaturze przedmiotu powszechnie przyjmuje się, że wywiad, bez względu na jego rodzaj, wykorzystuje następujące trzy rodzaje informacji:

1. biały wywiad, czyli źródła otwarte – stanowi 80% współczesnych informacji pozyskiwanych w drodze eksploracji źródeł jawnych: państwowych, czyli prawnych, prasowych, a także prywatnych;
2. szary wywiad, tj. źródła zamknięte – to blisko 15% informacji, które są pozyskiwane w drodze działań o charakterze detektywistycznym i śledczym w trakcie: inwigilacji (obserwacji i monitoringu), infiltracji, analiz kryminalistycznych oraz działań o charakterze socjotechnicznym.
3. czarny wywiad, czyli szpiegostwo – to około 5% informacji, które pochodzą ze źródeł niejawnych i chronionych właściwymi klauzulami, często kluczowych, gromadzonych jest w oparciu o czynności często nielegalne, takie jak szpiegostwo

300 Por. N. Polmar, T. B. Allen, *Księga szpiegów. Encyklopedia,* Warszawa 2000, s. 137.
301 Por. tamże.
302 Por.: *A. Żebrowski, Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 253.

przemysłowe i polityczne. Polega to na: instalacji podsłuchu i podglądu pomieszczeń i aparatury, monitoringu osób, pozorowaniu włamań, kradzieży cudzej tożsamości i parametrów biometrycznych, łamanie zabezpieczeń kryptograficznych, a także poprzez zwerbowaną w drodze szantażu lub korupcji agenturę[303].

Natomiast M. Kwieciński, po analizie literatury francuskiej podaje, że ze źródeł otwartych wywiad gospodarczy uzyskuje 70 % informacji, ze źródeł zamkniętych 20%, a ze szpiegostwa aż 10 % informacji.

Wszystkie pozycje literatury największą wagę pokładają w otwartych źródłach informacji, z których najsilniejszym są media. Należy mieć świadomość, że różnice w ocenie zagadnienia danych na temat źródeł informacji są trudne do zweryfikowania ze względu na brak możliwości przeprowadzenia wiarygodnych badań.

W literaturze przedmiotu powszechna jest stosowana terminologia dotycząca dwóch podstawowych źródeł informacji. Ogólnie wymienia się źródła formalne i źródła nieformalne. Do tych pierwszych zaliczyć należy przede wszystkim raporty wywiadowni gospodarczych i inne oficjalne dokumenty. Drugi rodzaj źródeł ma charakter ważniejszy i są one bardziej liczne, zarówno jawne jak i niejawne, czyli chronione. Te są przedmiotem zainteresowania bez względu na rodzaj odbiorcy czy instytucji, która zajmuje się gromadzeniem informacji. W nawiązaniu do jednostki wywiadu, tj. zarówno gospodarczego, jak i państwowego, mogą to być bardzo zróżnicowane materiały, a szczególnie:

1. różnorodne opracowania, ekspertyzy czy analizy,
2. media, a szczególnie: Internet, radio, telewizja, prasa,
3. raporty dyplomatyczne,
4. prospekty giełdowe,
5. zwiad lotniczy i satelitarny,
6. elektroniczne systemy podsłuchowe i inwigilacyjne,
7. technika komputerowa oraz
8. inne[304].

Powszechnie uważa się, że źródła nieformalne są najistotniejsze, gdyż stanowią 75% tego typu użytecznych informacji, a w przypadku wywiadu handlowego i konkurencyjnego aż 90%, (gdy w rozpoznaniu technologicznym tylko 60%). Pozostałe źródła przypadają na źródła formalne[305]. Dane te trzeba traktować z dużą swobodą, pamiętając jednak, że opinie doświadczonych wywiadowców czy analityków informacji gospodarczych, zgodne są co to tego, iż 90-95% wszystkich potrzebnych informacji można w uzyskać ze źródeł jawnych. Taki system lokowania i ochrony informacji daje wiele do myślenia[306]. Wciąż bowiem otwarty jest problem: co warto reklamować, a co ukrywać przed konkurencją?

W życiu społecznym funkcjonuje wiele różnorodnych formalnych źródeł informacji z zastrzeżeniem, że jak trafnie podaje J. Konieczny, trudno wymienić wszystkie; przykładowo są nimi:

303 K. Turaliński https://www.e-bookowo.pl/publicystyka/wywiad-gospodarczy-i-polityczny.html(18.08.2015)
304 Por. *Nowa Encyklopedia Powszechna PWN*, Warszawa 1997, s. 937.
305 B. Martinet, Y.M. Marti, *Wywiad gospodarczy…wyd. cyt.,* s. 41.
306 Por. J. Konieczny, *Wprowadzenie*…wyd. cyt., s. 150.

1. prasa ogólna, która przynosi wiele inspirujących informacji;
2. prasa specjalistyczna, cenna i dla każdej branży stanowi lekturę obowiązkową, najczęściej dotyczącą wydarzeń z przeszłości;
3. książki jako ważna pozycja podnosząca wiedzę osobistą, ale jest jeszcze bardziej przestarzała niż prasa specjalistyczna,
4. banki danych, tanie i dostępne, zawierają także płytką wiedzę, ale ułatwiają formułowanie konkretnych pytań;
5. opisy patentowe, zawierają bardzo wiele użytecznych informacji, są jednak niełatwe do zdobycia, zawierają minimum niezbędnych wiadomości, nawet na pograniczu niekompletności. Bywają czasem elementem operacji mistyfikujących, gdy firma patentuje wiele rozwiązań podobnych, w różnych częściach świata, aby ukryć właściwy, chroniony pomysł;
6. raporty agencji ratingowych, świadczyć mogą o wiarygodności przedsiębiorstwa, banku a nawet państwa. Wśród kryteriów oceny ujmuje się: sektor działania, rodzaj działalności, specyfikę konkurencji, sytuację finansowa, jakość zarządzania i inne;
7. Internet, wprawdzie zawiera wiele bezpłatnych informacji, lecz należy odnosić się do nich z dużą rezerwą. Znanych jest wiele przykładów błędnych i fałszywych informacji;
8. firmowe sprawozdania finansowe bardzo ważne źródła, jednakże wiele firm prywatnych, wbrew obowiązującym przepisom, nie składa ich w sądach rejestrowych;
9. informacje ze źródeł rządowych również są niezwykle istotnym zbiorem informacji. Ich uzyskanie ułatwia dostęp do informacji publicznej. Szeroki jest indeks źródeł gdyż można zwracać się do poszczególnych ministerstw, Centrum Informacji Gospodarczej, Głównego Urzędu Statycznego, a także do innych instytucji administracji rządowej i samorządowej;
10. raporty placówek eksperckich. Są to zazwyczaj instytuty prywatne, grupy konsultingowe i firmy doradcze, które dysponują niejednokrotnie szerokim zakresem wiedzy i doświadczenia. Przed skorzystaniem z tego rodzaju, zazwyczaj drogich usług, warto upewnić się co do reputacji takiej firmy;
11. jawne dokumenty źródłowe firm, czyli takie, które nie są objęte tajemnica przedsiębiorstwa lub tajemnicą handlową, tj.: wyciągi z rejestrów, bilans za ostatni rok, zaświadczenie o nie zaleganiu ze zobowiązaniami podatkowymi itp.;
12. źródła prawnicze, z których podstawowym jest Krajowy Rejestr Sądowy, a także inne wynikające ze spraw sądowe, hipoteki, dane dotyczące promocji i reklamy, katalogi, foldery, cenniki i inne dokumenty, mogące dostarczyć wielu różnorodnych i przydatnych informacji nt. konkurencji;
13. polskie placówki zagraniczne mają informacje na temat sytuacji gospodarczej na swoim terenie działania, często także o konkretnych przedsiębiorstwach. Znakomicie ułatwiają nawiązanie kontaktów i uzyskanie informacji[307].

Nieformalne źródła informacji wymagają osobistego zaangażowania w ich pozyskaniu i wykorzystaniu. Właściwe umiejętności, które J. Konieczny określa jako kluczowe, w zależności od typu osobowości wywiadowcy i jego wiedzy, to przede wszystkim: zdolność do nawiązywania kontaktów i umiejętność słu-

307 J. Konieczny, *Wprowadzenie*…wyd. cyt., s. 153,154.

chania, a także umiejętność przebywania w interesujących miejscach, związana z tym spostrzegawczość, umiejętność zapamiętywania, pomysłowość i elastyczność myślenia[308].

Najważniejsze źródła nieformalnych informacji to:

- konkurenci, dostawcy i podwykonawcy. Szczegółowymi źródłami są: wzajemna korespondencja, analiza ich wydawnictw wewnętrznych, stawanie się ich dostawcami lub podwykonawcami, uczestnictwo w imprezach towarzyskich z ich udziałem i wchodzenie w zażyłe stosunki towarzyskie;
- podróże służbowe, które są niezwykle ważne, chociaż kosztowne. Ich efektywność jako źródło informacji zależy w wielkim stopniu od przygotowania wyjazdu i profesjonalizmu podróżującego. Pozyskane korzyści powinny odpowiadać na pytania: co?, z kim?, o czym?;
- wystawy, targi, sympozja z natury rzeczy nastawione są na wymianę informacji. Od sesji oficjalnych ważniejsze bywają kuluary (nawiązywanie kontaktów, rozmowy nieformalne);
- stażyści, studenci, początkujący naukowcy mają często bardzo interesujące i różnorodne informacje;
- kandydaci do pracy. Wiele firm urządza sesje rekrutacyjne, ograniczając się tylko do rozmów z kandydatami i tylko po to by ich „odsłuchać", jeśli pracują dla konkurencji. To cenne źródło informacji, jednakże należy uważać, aby nie być posądzonym o nieuczciwą konkurencję;
- współpracownicy mają dużą wiedzę o otoczeniu firmy. Istotą umiejętności wydobycia tej wiedzy jest orientacja w zakresie: kto co wie lub kto i co może bez trudu ustalić,
- profesjonalny wywiadowca umiejętnie gromadzi informacje w formie: zwięzłych notatek, nagrań, nawet takich materiałów jak zbiory anegdot, historie konfliktów i studia przypadków związanych ze środowiskiem, a także notatki z zajęć szkoleniowych, opisy trafnych rozwiązań praktycznych w różnych dziedzinach, opisy sukcesów i porażek;
- sieć relacji osobistych jest najważniejszym źródłem dla każdego zainteresowanego gromadzeniem informacji[309].

Jedną z podstawowych form pracy, mającą wpływ na efektywność wywiadowcy, bez względu na kierunek jego działania i rodzaj służby, jest budowa szerokiej i skutecznej, a także użytecznej sieci powiązań osobistych. Wymaga to wielu dobrze zorganizowanych przedsięwzięć i obszernej wiedzy. Wspomniana sieć powinna opierać się na znajomości licznych środowisk. Wywiadowca powinien zatem bywać w różnych miejscach i spotykać się z wieloma interesującymi osobami. Mogą to być stowarzyszenia profesjonalne, społeczne, kulturowe, kluby, nocne lokale rozrywkowe itp. Trzeba być w nich zauważonym, czyli dobrze się prezentować. Jednym słowem trzeba umieć znaleźć się tam, gdzie dzieje się coś ważnego, a także samemu organizować imprezy towarzyskie, na które należy zapraszać szerokie grono osób. Sieć osobistych kontaktów powinna cecho-

308 Por. Tamże, s. 154, 155.

309 Szerzej: B. Martinet, Y.M. Marti, *Wywiad gospodarczy…wyd. cyt., s.46-49.*

wać się urozmaiceniem, różnorodnością, dużą liczbą znajomych i rozmaitością środowisk, w których działają. To tylko wybrane aspekty działań umożliwiających zdobywanie poszukiwanych informacji[310].

## 3. Kierunki działania wywiadu i kontrwywiadu państwowego a gospodarczego

Współczesna cywilizacja charakteryzuje się natłokiem różnorodnych informacji jawnych. Nie ma większego problemu z ich pozyskiwaniem, opracowywaniem i dystrybucją. Interesują się nimi służby specjalne, a w tym wywiad i kontrwywiad państwowego, a także wywiad i kontrwywiad gospodarczy.

Informacje dotyczące bezpieczeństwa państwa są przedmiotem zainteresowania wywiadów i kontrwywiadów państwowych. Mają one odpowiednią organizację i struktury odpowiedzialne za nadzorowanie, przetwarzanie informacji, a szczególnie związane z zarządzaniem informacjami. Do ważnych atrybutów informacji z punktu widzenia bezpieczeństwa państwa, a udostępnianych przez systemy informacyjne uprawnionym odbiorcom, zalicza się przede wszystkim: aktualność, prawdziwość, retrospektywność, predykcję, wiarygodność, użyteczność zupełność, przyswajalność, a także dostępność, kompletność, porównywalność i poufność zebranych i przetwarzanych informacji[311].

Biorąc pod uwagę rodzaje i kategorie wykorzystywanych źródeł, a także sposoby zdobywania informacji, określono następujące kategorie rozpoznania:

- rozpoznanie osobowe,
- rozpoznanie z ogólnodostępnych źródeł,
- rozpoznanie sygnałów elektromagnetycznych, które obejmuje rozpoznanie: łączności radiowej, elektroniczne, które z kolei dzieli się na rozpoznanie urządzeń innych niż łączności radiowej, telemetryczne i radiolokacyjne pasywne,
- rozpoznanie akustyczne,
- rozpoznanie obrazowe, które pozwala na wytworzenie danych na podstawie zobrazowania pochodzących ze zdjęć fotograficznych, radiolokatorów, przyrządów elektrooptycznych pracujących w podczerwieni i termowizyjnych oraz innych urządzeń,
- rozpoznanie pomiarowe i sygnaturowe, które polega na analizie parametrów technicznych i cech charakterystycznych pochodzących z urządzeń technicznych, co pozwala na identyfikowanie źródeł, nadajników i urządzeń promieniujących. Zalicza się do niego rozpoznanie: akustyczne, radiolokacyjne, podczerwieni, chemiczne i biologiczne, broni wiązkowej,
- rozpoznanie studyjne.
- Informacja jest podstawowym składnikiem każdego systemu rozpoznania, co umożliwia działalność wywiadowczą i kontrwywiadowczą. Jednakże praca z nagromadzonymi informacjami jest trudnym i złożonym procesem, który rzutuje na skuteczność wykonywanych czynności operacyjno-rozpoznawczych zainteresowanych służb.

310 Tamże, s. 55-58.

311 A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 222.

Warto zauważyć, że metody i formy stosowane przez służby wywiadu i kontrwywiadu w procesie pozyskiwania informacji są dostosowywane i doskonalone w zależności od poziomu rozwoju nauki, techniki i technologii[312]. Właściwe przedsięwzięcia i stosowanie odpowiednich urządzeń technicznych określają przepisy służbowe.

## 4. Źródła gromadzonych informacji

Każdy, kto poszukuje interesującej go informacji może sięgnąć do jawnych źródeł. Dla właściwych instytucji i organizacji, a także dla wywiadu gospodarczego, wprawdzie nie zawsze wyczerpującymi, a także nie zawsze dostępnymi źródłami informacji, mogą być przykładowo:

- PESEL (dostępny tylko dla niektórych instytucji państwowych);
- ZUS (tylko w uzasadnionych sprawach wyjątkowo można uzyskać informacje o stanie zatrudnienia firmy i opłacanych składkach);
- firmy ubezpieczeniowe (o ile nie dotyczą tajemnicy ubezpieczeniowej);
- banki (o ile nie dotyczą tajemnicy bankowej);
- urzędy skarbowe i urzędy kontroli skarbowej (o ile nie dotyczą tajemnicy skarbowej),
- urzędy stanu cywilnego;
- komornicy,
- notariusze,
- urzędy celne (o ile nie dotyczą tajemnicy celnej);
- Najwyższa Izba Kontroli, która niejednokrotnie udostępnia raporty nawet dla prasy;
- Prokuratura (o ile nie dotyczą tajemnicy śledztwa);
- sądy (jawność procesów; akta ujawniane są stronom i ich obrońcom lub pełnomocnikom; niekiedy także dziennikarzom);
- książki telefoniczne oraz różnego rodzaju informacje telefoniczne;
- katalogi firm (panoramy);
- sądy rejestrowe: rejestr spółek, stowarzyszeń, partii politycznych, fundacji, spółdzielni, tytułów gazetowych;
- rejestr skazanych;
- GUS (często jednak dane statystyczne z GUS otoczone są tajemnicą);
- hipoteki;
- spisy wokand sądowych;
- biura radców handlowych;
- izby handlowo-przemysłowe, (o ile nie dotyczą informacji chronionych);
- Internet;
- także telefony komórkowe i inne urządzenia medialne, z powodzeniem służą nie tylko do uzyskiwania wielu informacji, mogą również być wykorzystywane jako urządzenia naprowadzające;
- inne źródła.

312 Tamże.

Źródła informacji można podzielić według różnych kryteriów. Ze względów praktycznych należy przyjąć podział na **źró**dła ogólnodostępne, źródła o ograniczonej dostępności i źródła relatywnie niedostępne[313]. Wydaje się, że energiczny analityk nie będzie miał trudności w zdobywaniu informacji z dwóch pierwszych źródeł. Natomiast źródła relatywnie niedostępne, a inaczej oparte na źródłach operacyjnych, najczęściej wymagają wykorzystania metod niejawnych, m.in. rozmowy z osobą zaufaną, podsłuchu czy obserwacji. W praktyce metody te są wykorzystywane przez firmy detektywistyczne realizujące zamówienie złożone przez klienta, który chce zdobyć określone informacje. Można do nich zaliczyć:

- ustalenie faktycznej działalności firmy;
- określenie źródła pochodzenia pieniędzy partnera (kraj, w tym tzw. raje podatkowe, osoby, rodzaj i legalność wcześniejszej działalności);
- ustalenie numeru i stanu konta bankowego;
- wywiad biograficzny dotyczący właścicieli i osób sprawujących w firmie kluczowe stanowiska decyzyjne, również pod kątem ich powiązań ze środowiskami przestępczymi i służbami specjalnymi;
- ustalenie faktycznie planowanych kierunków rozwoju firmy,
- rozpoznanie polityki cenowej firmy, np. określenie możliwych upustów, faktycznych kosztów;
- ustalenie lojalności w interesach;
- opinie partnerów o danym podmiocie gospodarczym;
- ustalenie składników majątkowych, np. formy własności, obciążenia hipoteki;
- ustalenie nastrojów wśród załogi (szczególnie dotyczy to prywatyzowanych firm); informacje dotyczą m.in. aktywności związków zawodowych, ewentualnych planów strajków i protestów;
- zdobycie dowodów nielegalnej działalności:
- kradzież technologii, ustalenie źródeł zaopatrzenia czy składników produktów;
- *insider trading* (tzw. transakcja przeciekowa) – polega przede wszystkim na zdobywaniu poufnych informacji na temat przyszłych ruchów cen akcji.

Media zwróciły uwagę dopiero w roku 1998 na możliwość ujawniania informacji relatywnie niedostępnych przez agencje detektywistyczne. Ich pracownicy to jeszcze nie wywiadowcy gospodarczy, uzyskiwali takie informacje metodami niejawnymi, np. poprzez podsłuch i obserwację. Ponadto, wykorzystywali kontakty przyjacielskie i zawodowe swoich pracowników, często byłych funkcjonariuszy milicji i policji oraz byłych funkcjonariuszy służb specjalnych, od których wręcz kupowali interesujące materiały. Zdarzenia takie są wielce prawdopodobne, gdyż byłych funkcjonariuszy służb i prokuratury można znaleźć w niemal wszystkich agencjach detektywistycznych, w tym zakładanych np. przez banki i firmy ubezpieczeniowe[314].

Wyniki analizy dostępnej literatury wskazują, że w przeważającej mierze źródłami informacji są media i oficjalne dokumenty, jak na przykład:

313 T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 92-96.
314 A. Marszałek: *Wiadomość jako towar*, „Rzeczpospolita" z 9 czerwca 1998.

- sprawozdania, oceny, opinie, a także
- niezwykle interesujące charakterystyki przedsiębiorstw w prospektach emisyjnych;
- informacje i komentarze marketingowe czy giełdowe;
- oferty pracy;
- oferty dotyczące nowych zakupów i inwestycji, w tym również sprzętu komputerowego, a przede wszystkim oprogramowania.
- zamówione i uzyskane informacje z wywiadowni gospodarczych.

Metody zbierania informacji bez względu na sposób (jawny czy tajny), zawsze uwzględniają prognozowaną możliwość dostępu do: tajemnic organizacji, placówek naukowo – badawczych, przedsiębiorstw, umów handlowych, bankowych, ubezpieczeniowych itp. Nie można jednak określić dokładnej granicy pomiędzy metodami jawnymi a tajnymi. Te ostatnie są najczęściej rozszerzeniem metod jawnych. Zakres zbierania informacji tajnych może być ściśle ukierunkowany. Przykładowo, badanie może dotyczyć zadania mającego na celu zdobycie nowej technologii opracowanej przez określoną firmę.

Ukierunkowanie może również dotyczyć całości tajemnic, a szczególnie tajemnic penetrowanego przedsiębiorstwa. Przedmiot zainteresowań i analiz danych o konkurencji to przede wszystkim strategia konkurencyjnej, czyli badanej organizacji w zakresie:

- jej stanu ekonomicznego i finansowego;
- stanu rachunków bankowych;
- listy klientów,
- wykazu dostawców i odbiorców;
- efektów ekonomicznych: koszty produkcji, sprawy kadrowe, płace, inne,
- planów rozwojowych, polityki marketingowej, planów zakupów;
- nowych osiągnięć: prototypów, nowych produktów, planów zdobycia nowych rynków, nowych klientów itp.

W celu zdobycia tych ostatnich dokumentów wywiadowcy starają się pozyskać kogoś z firmy, która jest przedmiotem penetracji, co może prowadzić do szpiegostwa gospodarczego a wtedy łatwiej będzie uzyskać dokumenty dostępne wyłącznie dla zarządu, dyrekcji, a może nawet przechowywane w kancelarii tajnej (np.: dane statystyczne, opracowania i analizy, korespondencję, opinie konsultantów, wyniki kontroli i inne).

Specjalistyczne źródła informacji to przykładowo:

1. oficjalnie publikowane dane agend rządowych, np. Biuletyny Informacji Publicznej, dane GUS, Rządowego Centrum Studiów Strategicznych, innych centralnych urzędów,
2. wydawnictwa branżowe i specjalistyczne,
3. publikacje akademickie;
4. sądy rejestrowe: rejestr spółek, stowarzyszeń, partii politycznych, fundacji, spółdzielni,

5. media i archiwa prasowe,
6. hipoteki,
7. spisy wokand sądowych;
8. rejestry izb przemysłowo - handlowych.
9. bazy PESEL i ZUS;
10. umowy zawierane przez firmy ubezpieczeniowe oraz umowy rachunków bankowych,
11. urzędy skarbowe i organy kontroli skarbowej;
12. urzędy stanu cywilnego;
13. urzędy celne;
14. komornicy;
15. raporty Najwyższej Izby Kontroli;
16. prokuratura i sądy oraz policyjne bazy danych.

Inne źródła z ograniczonym dostępem uzyskiwane na podstawie zamówień w profesjonalnych firmach, a przykładowo:

- ustalenie faktycznej działalności firmy;
- określenie źródła pochodzenia dochodów;
- ustalenie numeru i stanu konta bankowego;
- wywiad biograficzny dotyczący właścicieli i osób sprawujących w firmie kluczowe stanowiska decyzyjne,
- ustalenie faktycznie planowanych kierunków rozwoju firmy,
- rozpoznanie polityki cenowej firmy, np. określenie możliwych upustów, faktycznych kosztów;
- ustalenie lojalności w interesach;
- opinie partnerów o danym podmiocie gospodarczym;
- ustalenie składników majątkowych, np. formy własności obciążenia hipoteki;
- ustalenie nastrojów wśród załogi;
- zdobycie dowodów nielegalnej działalności:
- ustalenie źródeł zaopatrzenia czy składników produktów;
- zdobywanie innych poufnych informacji na temat przyszłych dochodów, majątku i przewidywanych cen akcji[315].

## 5. Źródła informacji z cyberprzestrzeni

Z różnych powodów wiele osób i firm umieszcza różnorodne informacje w Internecie, a niektórzy specjaliści z branży informatycznej – lokują dane w chmurze. Analitycy-wywiadowcy, bez względu na rodzaj zainteresowań analizują te informacje i wykorzystują je dla potrzeb wywiadu. Najbardziej znane

315 Szerzej T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 92-96.

internetowe źródła danych możliwe do uzyskania w ramach białego wywiadu to przede wszystkim[316]:

1. serwisy informacyjne, portale, wortale,
2. blogi (dzienniki internetowe):
   a) internetowe pamiętniki, w których autor dzieli się osobistymi przemyśleniami,
   b) fotoblogi, videoblogi, błogi muzyczne, zdjęcia, filmy, czy utwory muzyczne,
   c) blogi korporacyjne, organizacyjne – na potrzeby public relations, marketingu, bądź do wewnętrznej komunikacji w obrębie firmy,
   d) blogi tematyczne: polityczne, edukacyjne, filmowe, o podróżach, modzie etc.
3. fora internetowe, listy dyskusyjne – wśród potencjalnych korzyści z analizowania dostępnych na forach i listach dyskusyjnych informacji wymienić można:
   a) podobnie jak w przypadku blogów - uzyskanie dodatkowego źródła informacji,
   b) ocena popularności bądź też ładunku emocjonalnego,
   c) analiza trendów.
4. otwarte serwisy Chat oraz IRC.
5. serwisy społecznościowe jak np.: Facebook, nasza-klasa.pl czy ukierunkowany biznesowo linkedin.com.
6. Inne rodzaje źródeł internetowych jak np.:
   a) strony domowe,
   b) bazy danych,
   c) serwisy aukcyjne i z drobnymi ogłoszeniami,
   d) sieci wymiany plików i inne.

Opracowywanie dokumentów i wnioskowanie odbywa się w korelacji z informacjami uzyskanymi ze wszystkich źródeł, czyli również ze źródeł tajnych. Ze wszystkich tych publikatorów można wydobyć wiele interesujących informacji. Należy jednak pamiętać, że z uwagi na wrażliwość niektórych danych i objęcie ich ustawami ograniczającymi dostęp do informacji, ich uzyskanie jest ograniczone.

## 6. Analiza ekonomiczna i zarządzanie uzyskanymi informacjami

Jednym z kolejnych zadań analityka informacji czy wywiadowcy, po uzyskaniu i zgromadzeniu informacji, jest dokonanie analizy, czyli dokładne opracowanie i wnioskowanie co do przydatności. Według T.R. Aleksandrowicza jako podstawowe reguły pracy analitycznej należy uznać następujące:

- dokonanie opracowania dla potrzeb konkretnego odbiorcy – zleceniodawcy, z maksymalnym zasobem wiedzy, niezbędnej do podjęcia optymalnej decyzji w zależności od poziomu kompetencji decydenta. Im jego wyższy poziom tym mniej szczegółów zawierać powinna gotowa analiza;

316 P. Maciołek, *Internet a OSINT – szanse i praktyczne zastosowania* w: W. Filipkowski, W. Mądrzejowski (red) *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012 s. 222-242.

- analizę zawsze sporządza się dla konkretnego odbiorcy, na jego konkretne zamówienie, zatem analityk musi uwzględnić możliwości percepcyjne i zasób wiedzy fachowej decydenta, inaczej zatem przygotowuje się analizę dla prawnika, inaczej zaś dla inżyniera;
- forma analizy jest podporządkowana jej celowi, czyli redakcja dokumentu musi zapewnić możliwość szybkiego i łatwego zrozumienia treści. (Autor sugeruje, że jeśli decydent nie zainteresuje się treścią dokumentu w ciągu 10 do 15 sekund, prawdopodobnie uzna go za analitycznie bezwartościowy). Zatem informacje najważniejsze powinny rozpoczynać dokument, rozwinięcia i uzasadnienia umieszcza się w dalszej kolejności;
- treść analizy ma również swoją specyfikę. Z tego względu umieszcza się wyłącznie to, co ma znaczenie dla odbiorcy. Jeśli coś zostało pominięte, adresat analizy może poprosić o uzupełnienie. Należy być również przygotowanym na to, że tę samą informację różni szefowie w zależności od zajmowanego stanowiska, będą analizować z innych punktów widzenia, jak np.: szef produkcji i szef marketingu;
- istotnym czynnikiem jest czas, a więc ważne są sprawy bieżące i elementy prognozy[317].

Aby spełnić swój cel, analiza musi być merytorycznie poprawna, przygotowana i przekazana odbiorcy we właściwym czasie, uwzględniać zapotrzebowania odbiorcy, zainteresować go, zostać przezeń zrozumiana i przekonać o słuszności zawartych w niej tez. Jeśli materiał analityczny nie spełnia tych wymogów jest bezużyteczny[318].

Dokument analityczny może być prezentowany w formie pisemnej, zwięzły tytuł, sprawy najważniejsze umieszcza się na początku, następna jest czołówka, czyli 3 do 5 zdań, zawierających wnioski płynące z analizy. Kolejne dwa akapity relacjonujące zdarzenie czy zagadnienie oraz komentarze, opinie, prognozy i wnioski oraz także 3-5 zdań analitycznych ze wskazaniem uzasadnień, w malejącym porządku ważności.

Może być również ustna forma przekazu informacji wraz z jej analizą dla odbiorcy zwana briefingiem. Taka sesja trwa zazwyczaj 30 minut, z których 15 min. przeznacza się na pytania i odpowiedzi, jest organizowana zwykle wtedy, gdy zamówienie określało krótki termin wykonania analizy i brakło czasu na przygotowanie właściwych dokumentów. Metodyka pracy analitycznej jest zasadniczo taka sama, jak w przypadku przygotowania materiałów pisemnych. Analityk musi jednak wziąć pod uwagę kwestie związane ze słuchaczami, a przykładowo: ich stanowiska służbowe, dostęp do tajemnic przedsiębiorstwa, a także poziom wiedzy w badanych zagadnieniach.

Konkretna praca analityka rozpoczyna się od dostarczenia mu informacji. Na wagę analizy wpływa taka sytuacja, w której analityk dysponuje informacją wielośródłową, potwierdzoną i wiarogodną. Znawcy przedmiotu określają, że nie zdarza się to zbyt często. Zatem praca analityka polega również na „ważeniu" źródeł, tj. dokonaniu wyboru źródła, czy źródeł najbardziej wiarogodnych.

Kolejnym, niezwykle ważnym etapem pracy analityka jest myślenie kreatywne: kojarzenie faktów, rozumienie związków pomiędzy nimi, odróżnianie rzeczy ważnych od nieistotnych, wskazanie dróg wiodących do celu. Należy mieć rów-

317 T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 25-36.
318 Tamże, s. 36.

nież na uwadze, że zarządzanie w biznesie, a szczególnie jego bezpieczeństwo nie odbywa się jedynie na podstawie uzyskiwanych pojedynczych odpowiedzi na konkretne na zadane pytania – problemy. Zawsze zatem należy analizować nawet kontrowersyjne punkty widzenia, które rozwijają i zmieniają się w czasie. J. Konieczny trafnie przestrzega, że *od ryzyka związanego z nieoznaczonością i wieloznacznością proponowanych rozwiązań nie ma ucieczki*[319].

Wśród wybranych, różnorodnych elementów mających wpływ na skuteczność pracy wywiadowcy ważny jest profesjonalizm w zakresie analizy informacji.

Rzetelna analiza informacji powinna wykazać jej rzeczywistą wartość, która uzależniona jest od wielu czynników, a przykładowo:

1. powinna ujmować rzeczywistą analizę potrzeb zamawiającego informację;
2. opierać się na właściwych, tj. na odpowiednich merytorycznie i jakościowo źródłach;
3. zawierać wysoką jakość analizy, tj. przydatną dla zamawiającego.

Analiza powinna być niezwłocznie udostępniona zamawiającemu, a zamawiający powinien zwrotnie powiadomić analityków o jej wartości. W uzasadnionych przypadkach powinien zgłosić pytania dodatkowe, które mogą sugerować głębsze wyjaśnienie uzyskanych informacji, nigdy bowiem treść dokumentu nie zawiera tego wszystkiego, co się zdarzyło, o czym rozmawiano, co ustalono itp. – nawet wówczas, gdy zdarzenie było rejestrowane na nośniku. W takim przypadku niezbędna jest charakterystyka atmosfery rozmawiających, wygląd osób i inne cechy.

Oczywiście, różnorodne informacje chronione, a także mające znaczenie strategiczne powinny być właściwie zabezpieczone i udostępnione jedynie osobom do tego upoważnionym[320].

Odbiorca zamówionej analizy powinien również mieć świadomość, że przykładowo w analizie znajduje się tzw. informacja przeciekowa jak np. *insider trading,* który może mieć miejsce przy poufnych informacjach na temat przyszłych ruchów cen akcji.

Budowanie strefy ochronnej na zasoby informacyjne zależy od rodzaju informacji. Przykładowo, ochrona informacji ściśle tajnych leży w kompetencjach służb specjalnych. Natomiast ochrona informacji w zakresie tajemnicy zawodowej mieści się w zakresie określonej branży, firmy czy przedsiębiorstwa.

Zarzadzanie informacjami związane jest ściśle z ich wartością. Zatem procesy zarządzania informacjami w przedsiębiorstwie przenikają przez wszystkie jednostki organizacyjne, procedury operacyjne, a także funkcje zarządzania na wszystkich szczeblach organizacji.

Według *Encyklopedii Zarządzania* na zarządzanie informacjami składają się następujące przedsięwzięcia:

- zespół działań tworzących funkcję informacyjną przedsiębiorstwa, tj. pozyskiwanie informacji, przetwarzanie informacji, dyfuzja informacji,
- zespół działań w ramach płaszczyzn (technologicznej, organizacyjnej, zasobów ludzkich) wpływających na realizację tej funkcji[321].

319 J. Konieczny, *Wprowadzenie*… wyd. cyt., s. 159.
320 Por. B. Martinet, Y.M. Marti, *Wywiad gospodarczy…* wyd. cyt., s. 18, 19.
321 http://mfiles.pl/plindex.php/Kategoria:Zarz%C4%85dzanie_informacjami(12.08.2014).

Na tym tle określa się główne zadania kierownictwa odpowiedzialnego za zarządzanie zasobami informacyjnymi. Związane jest to ze stałym dostosowywaniem ewoluujących technologii informatycznych (w dziedzinie sprzętu, oprogramowania, komunikacji) do dynamicznie zmieniających się potrzeb organizacji. Podstawą jest zatem realizacja procesu dostosowywania się do wyzwań stawianych przez konkurentów i zmieniające się otoczenie.

Jako główne obszary problemowe zarządzania informacjami określono:

- zadania i odpowiedzialność kierownictwa,
- organizację systemu zarządzania,
- aspekty socjologiczne i zachowania użytkowników,
- planowanie i kontrola operacyjna,
- projektowanie systemów informacyjnych,
- bezpieczeństwo przetwarzanych danych,
- zasoby ludzkie,
- kulturę organizacyjną[322].

Wszystkie te elementy powinny uwzględniać zarówno bezpieczeństwo przedsiębiorstwa związane również z zadaniami w formie kontrwywiadu gospodarczego, jak i właściwy stosunek do konkurencji.

Przed analitykiem informacji może roztaczać się obszerna sieć błędów i pułapek, jak to określa T.R. Aleksandrowicz swoistych „wilczych dołów", w które analityk może niespodziewanie wpaść. Ich lista jest długa i praktycznie nieograniczona. Zalicza się do nich przede wszystkim:

1. przekonanie, że dysponuje się już wystarczającą wiedzą do napisania analizy i przy jednoczesnej niechęcci do uwzględniania nowych informacji;
2. zbyt duże zaufanie do określonego źródła informacji i nieweryfikowanie pochodzących z niego danych lub też brak zaufania do określonego źródła informacji i bezpodstawne negowanie pochodzących z niego danych;
3. niechęć do weryfikowania przyjętych na wstępie założeń i przywiązanie się do pierwszej koncepcji, to najpoważniejszy z grzechów;
4. tendencja do „wiecznego" samoredagowania tekstu, która wiąże się m. in. ze zwlekaniem z ostateczną redakcją tekstu w oczekiwaniu na kolejne informacje
5. niechęć do stosowania technik twórczego myślenia
6. emocjonalne zaangażowanie w analizowany problem
7. pisanie „pod przełożonego" lub „pod odbiorcę" (syndrom „posłańca przynoszącego złe wieści").
8. niechęć do podejmowania ryzyka popełnienia błędu
9. dążenie za wszelką cenę do znalezienia „drugiego dna" w każdej sytuacji.

Cytowany autor proponuje szereg sposobów na unikanie wspomnianych wyżej niebezpieczeństw, gdyż opisane wcześniej błędy i pułapki mogą spowodować wiele problemów, co jednak nie oznacza, że są niemożliwe do uniknięcia. Pierwszym krokiem jest bez wątpienia uświadomienie samemu sobie, że takie

322 Tamże.

zagrożenia występują i dotyczą każdego, kto para się pracą analityczną. Warto zatem wziąć pod uwagę następujące propozycje[323]:

1. Uwierz we własną zdolność do formułowania profesjonalnych ocen;
2. Wykaż gotowość do dyskusji i wysłuchania opinii i argumentów;
3. Bądź agresywny intelektualnie, nie bój się pomylić;
4. Lepiej przyznać się do pomyłki, niż przedstawić jako produkt finalny błędną analizę;
5. Za wszelką cenę unikaj efektu lustrzanego odbicia. Jest to jedno z największych zagrożeń obiektywizmu. Polega przede wszystkim na ocenie motywacji i prognozie zachowań innych ludzi na podstawie własnych systemów wartości i wyznawanych przez siebie zasad;
6. Analiza nie ma żadnej wartości, jeżeli nie została dostarczona odbiorcom;
7. Koordynacja i uzgadnianie wniosków w sytuacji, gdy analizę przygotowuje wspólnie kilka podmiotów, jest niezbędna, ale nie może oznaczać narzucania opinii;
8. Gdy wszyscy się zgadzają, to prawdopodobnie wszyscy popełniają błąd;
9. Odbiorca nie jest zainteresowany tym, jak wiele wiesz na określony temat; on chce się od ciebie dowiedzieć tylko tego, co jest naprawdę istotne;
10. Forma nigdy nie jest ważniejsza niż treść;
11. Nie traktuj zbyt poważnie uwag edytorskich;
12. Nigdy nie stawiaj swojej kariery ponad swoje obowiązki;
13. Bycie analitykiem nie przynosi popularności;
14. Nie traktuj swojej pracy ze śmiertelną powagą.

Wiele sposobów zdobywania informacji jest zarówno pracochłonnych i kosztownych, jak i wielce ryzykownych. Może się okazać, że zdobyte informacje nie są warte wydatków, które poniesiono. Warto zatem dokonać wstępnego rozpoznania mającego na celu orientację czy na przykład:

- istnieje możliwość zdobycia poszukiwanej informacji?
- jakie korzyści przyniesie zdobyta informacja?
- jakimi metodami i jakimi kosztami należy się posłużyć?
- jakie jest ryzyko ujawnienia zainteresowanego (wywiadowcy, informatora, przedsiębiorczego zleceniodawcy), który poszukuje informacji?
- kiedy poszukiwana informacja straci swoją aktualność?

Najbardziej rzeczowe pytanie to: jak zdobyć poszukiwane informacje? Odpowiedź wymaga nie tylko wiedzy, wymaga również praktyki. Niezbędne jest zatem zarówno teoretyczne, jak i praktyczne przygotowanie[324].

Zdaniem praktyków – analityków informacji gospodarczych skuteczność zdobywania poszukiwanych informacji zależy od systemu organizacyjnego w przedsiębiorstwie, a przede wszystkim od:

323 Tamże, s. 129-138.
324 H. Cornwall, *Datatheft. Computer Fraud*, wyd. cyt., s. 121, 122.

a) zidentyfikowania potrzeb informacyjnych,

b) opracowania spójnej strategii metodologii informacyjnej,

c) poszukiwania informacji ze źródeł najlepszych, czyli nieformalnych lub nawet nieoficjalnych,

d) opracowania odpowiedniej metodologii przetwarzanych informacji, które powinny być maksymalnie przydatne dla użytkowników,

e) udostępniania informacji użytkownikom i zapewnienia ich wykorzystania[325].

We wspomnianym systemie mamy do czynienia z trzema grupami uczestników wywiadu gospodarczego, są to:

- decydenci, którzy formułują zadania (pytania), kierunkują pracę i oceniają wyniki,
- osoby pozyskujące informacje, czyli wszyscy pracownicy przedsiębiorstwa, tj. nie tylko profesjonalni wywiadowcy, gdyż każdy z racji swojego stanowiska zdobywa informacje, przykładowo: księgowy telefonujący do banku, handlowiec kontaktujący się ze swoimi dostawcami i odbiorcami,
- profesjonaliści, czyli osoby wyszkolone i zatrudnione w charakterze wywiadowców lub na innych (zakonspirowanych) etatach, lecz zajmujące się zawodowym zbieraniem, przetwarzaniem i przekazywaniem decydentom zdobytych informacji. Dla pozyskania właściwej kadry w wielu krajach wyższe uczelnie, nie tylko policyjne, prowadzą kierunki studiów związane z wywiadem i kontrwywiadem, nie tylko gospodarczym.

## 7. Rozpoznanie i ocena partnera transakcyjnego

We współczesnym biznesie nie jest zaskoczeniem wcześniejsze rozpoznanie partnera transakcyjnego. Nawet w czasie negocjacji okazuje się, że konkurencja jest dobrze przygotowana do trudnych rozmów. Przykładowo, dysponuje doskonałym rozpoznaniem o kluczowych członkach zarządu spółki, z którą planuje współpracę. Niejednokrotnie znane są nie tylko nazwiska lecz również życiorysy i zainteresowania. Jednakże najbardziej typowa jest znajomość rodzajów i form produkcji, rodzaj wyposażenia i ostatnio zawarte kontrakty.

Działania zespołów wywiadu, jak i kontrwywiadu gospodarczego spełniają niezwykle istotną rolę w bezpieczeństwie przedsiębiorstwa i jego rozwoju. Temu rozwojowi nadaje wiodący ton rozwój społeczeństwa informacyjnego i towarzyszący mu proces związany z rozwojem techniki informatycznej. Towarzyszy mu również narastające systematycznie zapotrzebowanie na specjalistyczne usługi informacyjne, a w tym o specjalistycznym (branżowym) charakterze wywiadowczym i kontrwywiadowczym.

Natomiast swoisty rozwój inteligencji cyberprzestrzeni, obszarów wirtualnych i cyfrowych dotyczy nie tylko uprawnionych przedsiębiorstw i służb. Dotyczy to przede wszystkim wszystkich sektorów gospodarki. Tym złożonym procesom towarzyszy stała o charakterze lawinowym rewolucja elektroniczna. Rozwój komputeryzacji wiąże się ze zmianą środków i metod pozyskiwania informacji, które pociągają za sobą potrzebę zmiany metod pracy.

325 Por.: B. Martinet, Y.M. Marti, *Wywiad...* s. 262.

Niezwykle trafna jest opinia, że działalność wywiadowcza i kontrwywiadowcza to wiele wzajemnie powiązanych, współzależnych i uzupełniających się przedsięwzięć, które można określić cyklem wywiadowczym lub cyklem kontrwywiadowczym[326]. Teoretycznie można wspomniane cykle porównywać z wywiadem i kontrwywiadem gospodarczym.

Cykl wywiadowczy służby państwowej obejmuje wszystkie fazy działalności służby wywiadu, od planowania poczynając, na dystrybucji gotowego materiału wywiadowczego kończąc. Dzielony jest zazwyczaj na pięć etapów, na które składać się powinny adekwatne działania wywiadu i kontrwywiadu gospodarczego:

1. planowanie i ukierunkowanie pracy operacyjnej wywiadu, sposobów zdobycia informacji oraz kontrola efektywności działania jednostek zajmujących się jej gromadzeniem,
2. gromadzenie, proces zdobywania informacji i przekazywania ich do dalszej obróbki,
3. przetwarzanie, proces porządkowania i ujednolicenia uzyskanych informacji czy ujednolicenie formatu danych teleinformatycznych,
4. wytwarzanie, proces przekształcania informacji przetworzonej w gotowe dane wywiadu, obejmujący analizę, ocenę i interpretację,
5. przekazywanie, dystrybucja danych wywiadowczych dla uprawnionych użytkowników[327].

Analizując metody działania kontrwywiadu, należy mieć na uwadze cykl kontrwywiadu państwowego, na który składa się zespół czynności właściwych dla zespołu kontrwywiadu przemysłowego, który może obejmować następujące etapy przydatne dla działań związanych z bezpieczeństwem przedsiębiorstwa, a mianowicie:

1. planowanie i ukierunkowanie działań na podstawie istniejących zagrożeń dla przedsiębiorstwa w powiązaniu ze sposobami zdobywania informacji oraz kontrolą efektywności,
2. rozpoznawanie, gromadzenie oraz poszukiwanie sygnałów dotyczących zagrożeń dla bezpieczeństwa przedsiębiorstwa i przekazywanie ich do dalszych kompetentnych analiz,
3. przetwarzanie, weryfikacja zdobytych informacji i materiałów, które potwierdzają istniejące zagrożenia, analiza, ocena i interpretacja,
4. wszczęcie postępowania analitycznego jako dalszy sposób postępowania przy zastosowaniu odpowiednich, w zależności od potrzeb metod i środków, ze szczególnym uwzględnieniem gromadzenia informacji o zdarzeniu, osobie lub grupie osób,
5. przekazywanie, dystrybucja danych kontrwywiadowczych dla uprawnionych użytkowników (na przykład obowiązanego członka zarządu przedsiębiorstwa ds. bezpieczeństwa)[328].

Analiza treści uzyskanych informacji powinna pozwolić na ich weryfikację oraz wnioskowanie, a mianowicie:

326 Por.: A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 248.

327 Por. N. Polmar, T. B. Allen, *Księga szpiegów. Encyklopedia,* Warszawa 2000, s. 137.

328 Por. tamże.

1. czy uzyskana informacja, na podstawie dotychczasowych ustaleń jest prawdopodobna?
2. czy informacja została skonfrontowana i porównana z informacjami uzyskanymi z innych źródeł?
3. czy treść informacji zgadza się z posiadanymi danymi, a szczególnie z tymi, które uznano za autentyczne. Jeżeli informacja przedstawia dane odmienne od danych uzyskanych z innych źródeł, pozostaje właściwym sposobem wyjaśnić, która z tych informacji jest prawdziwa[329].

Działania dotyczące wywiadu i kontrwywiadu państwowego znajdują się w gestii służb specjalnych, które prowadząc właściwe przedsięwzięcia wykonują również właściwe przedsięwzięcia w zakresie wywiadu i kontrwywiadu gospodarczego.

329 Por.: *A. Żebrowski, Wywiad i kontrwywiad..,* wyd. cyt., s. 253.

# Rozdział 7

# Wybrane metody działania w praktyce wywiadu i kontrwywiadu elektronicznego

## 1. Sabotaż komputerowy

Różnorodne formy sabotażu w cyberprzestrzeni mogą być wykorzystywane przez nieuczciwą konkurencję, wywiad gospodarczy czy szpiegostwo gospodarcze. Polegają one na działaniach zmierzających do zakłócania lub uniemożliwiania automatycznego gromadzenia albo przekazywania informacji oraz na niszczeniu, wymianie, uszkodzeniu nośników lub urządzeń służących do automatycznego przetwarzania, gromadzenia czy przesyłania informacji.

Celem działania sprawcy jest sparaliżowanie funkcjonowania określonego systemu komputerowego lub sieci teleinformacyjnej, a zatem doprowadzenie do dezorganizacji, a nawet sytuacji kryzysowej całego przedsiębiorstwa czy jednostki administracyjnej. Zagadnienia te szerzej omówiono w rozdziale 3. Warto jednak podkreślić, że istotą działania jest zablokowanie możliwości przyjmowania i wysyłania informacji niezbędnych dla bezpieczeństwa państwa czy określonej jednostki administracyjnej lub przedsiębiorstwa. Atakowane mogą być różnorodne obiekty, a przykładowo:

1. budynki mieszczące ośrodki obliczeniowe,
2. sprzęt i wyposażenie ośrodków obliczeniowych,
3. programy i bazy danych,
4. a także instytucje państwowe i społeczne, na które atak może spowodować dezorganizację społeczną,
5. wszelkiego rodzaju firmy czy przedsiębiorstwa.

Najczęściej użytkownicy nie znają stosowanych metod sabotażu, a w związku z tym zgłaszają jedynie awarie systemu. Natomiast brak dociekań specjalistów od ochrony systemów teleinformatycznych na temat przyczyn awarii – jest dostatecznym czynnikiem umożliwiającym przestępcom kontynuowania destrukcyjnej działalności.

Nasilający się obecnie sabotaż komputerowy związany jest z występującymi już na skalę masową uszkodzeniami komputerów osobistych specjalnie opracowanymi programami zawierającymi wirusy komputerowe. Programy te są rozpowszechniane przede wszystkim przez pirackie kopie i stanowią już znaczną część przestępstw komputerowych; wchodzą one do innych programów danego systemu z opóźnieniem powodując znaczne szkody.

Liczba wirusów znajdujących się w obiegu stale rośnie. Niejednokrotnie są one umieszczane w programie przez producenta, aby przeciwdziałać nielegalnemu kopiowaniu.

## 2. Wirusy komputerowe jako metoda zdobywania informacji chronionych

Wprowadzenie wirusów komputerowych do systemów teleinformatycznych może być celowym działaniem we wszystkich dotychczas rozpoznanych kategoriach przestępstw komputerowych, które omówiono w rozdziale 9 tej książki. Zatem wirusom warto poświęcić więcej uwagi, co uczyniono w rozdziale 5 tej książki.

Wirus komputerowy przenosi się poprzez pliki, co wymaga obecności systemu plików, lub przez bezpośredni zapis w wybranym sektorze bądź jednostce alokacji zewnętrznego nośnika danych np. dysku twardego, poczty, pendrive'a.

Na tle tych rozważań słuszna staje się teza, że wirus bywa groźny jak szpieg. Celowa produkcja wirusów komputerowych służyć może do przechwytywania planów informacji o charakterze technicznym, poufnych dokumentów, a także do podsłuchiwania rozmów. Wirus Flame został napisany specjalnie do wykradania tajemnic dotyczących instalacji w Iranie, co potwierdzili eksperci firmy zajmującej się bezpieczeństwem danych Kaspersky Lab.

Zdaniem tej firmy Flame to najbardziej skomplikowane i najdoskonalsze narzędzie, jakie opracowano do wykradania danych. Włamywacze interesują się głównie plikami AutoCAD (z planami inżynierskimi), dokumentami tekstowymi i PDF oraz treścią listów e-mail. Warto również przypomnieć, że słynny poprzednio Stux-net, służył do badania irańskich instalacji jądrowych.

Flame, dzieło izraelskich inżynierów, od 2008 roku podobno służył do prowadzenia tajnej operacji w cyberprzestrzeni. Nie tylko rozprzestrzeniał się w sieciach komputerowych i wykradał zapisane dane, lecz również ma możliwość rejestrowania obrazu na ekranie, wciśniętych klawiszy oraz nagrywania rozmów, a streszczenia wysyłał do swoich autorów[330].

## 3. Programy sprawdzająco-monitorujące

Podstawowym zadaniem tego typu programów jest czuwanie nad systemem i zapisywanie wszystkich czynności wykonanych za pomocą klawiatury, tj. naciskanych przez użytkownika klawiszy. W każdej chwili można sprawdzić kto i co pisał na klawiaturze badanego komputera, podczas obecności lub nieobecności użytkownika czy właściciela. Oprogramowanie monitoruje klawiaturę i zapisuje każdy wciśnięty klawisz, ponadto potrafi zapisać zawartość ekranu do pliku graficznego oraz wysłać dane na e-mail. Utrwala datę, godzinę oraz tytuł aplikacji, w której wpisywany był tekst. Używane są różne typy programów przykładowo umożliwiające:

1. blokowanie dostępu do stron według kryteriów osoby nadzorującej komputer. Aplikacja posiada opcje blokujące dostęp do wybranych funkcjonalności np. komunikator, listy dyskusyjne, pobieranie plików itp. Z powodzeniem śledzi, jakie strony odwiedza użytkownik;
2. jednostanowiskowe monitorowanie aktywności użytkownika na komputerze domowym lub firmowym. Działa w sposób dyskretny, nie dodaje wpisów w panelu sterowania, ani nie tworzy ikonek;

330 P. Kościelniak, *Wirus gorszy niż szpieg*, „Rzeczpospolita" z 5 czerwca 2012 r.

3. badanie aktywności pracy użytkownika w postaci monitoringu polegającego na automatycznym zapisywaniu zrzutów ekranów z czynności odbywających się na komputerze[331].

W praktyce departamentów bezpieczeństwa instytucji finansowych od kilku lat stosuje się programy monitorujące pracę konsultantów telefonicznych i komputerowych. Na ekranie kontrolnym widoczna jest treść korespondencji konsultanta. Pozwala to wykryć szereg nieprawidłowości, a nawet ujawnienie tajemnicy przedsiębiorstwa w kontaktach z konkurencją.

## 4. Eksponowanie szpiegowskich możliwości praktycznych

Wyszukiwarka internetowa Google na hasło *szpieg komputerowy* w dniu 1.02.2012 roku wyświetliła 51.700 pozycji. Natomiast 2 sierpnia 2015 r. aż 188.000 ze wskazaniem na wiele nowoczesnych i tańszych produktów oferujących najwyższą technikę dostępną w handlu urządzeniami elektronicznymi. Przykładowo, *zdalny szpieg komputerowy*[332], reklamowany jest jako urządzenie nadające się do monitorowania komputerów dziecka, żony, pracownika i męża. Niektóre reklamy proponują nawet wersję darmową szpiega.

Prawdą jest, podkreślane w reklamach, że istnieje duże zapotrzebowanie na ochronę dzieci korzystających z Internetu, że powinny być skutecznie rozpoznawane i wykrywane wszelkie próby oszustwa w firmie. Dla wielu osób ważne jest ujawnienie i udowodnienie zdrady współmałżonka, a czasem ujawnienie innych okoliczności. W związku z powyższym pojawiły się rozwiązania umożliwiające monitorowanie aktywności użytkownika komputera. Właśnie w realizacji wspomnianych celów, zdaniem reklamodawców, mają być przydatne najnowocześniejsze urządzenia szpiegowskie.

To wysokiej klasy profesjonalne urządzenia, które umożliwiają pełne monitorowanie sposobu użytkowania komputera. Celem instalacji urządzenia jest prowadzenie dyskretnej obserwacji użytkownika pracującego na komputerze[333].

Sama instalacja i konfiguracja jest prosta. Wystarczy dostęp do komputera, na którym zalogowany jest użytkownik jedynie na czas do 30 sekund. Instalacja jest szybka i wygodna, łatwa w obsłudze i nie ogranicza funkcjonalności komputera. Szpieg nie musi być podłączony na stałe do komputera, a także zapewnia pełne bezpieczeństwo i dyskrecję. Należy zatem przypuszczać, że użytkownik komputera nie ma orientacji o zainstalowaniu szpiega. Podłączenie polega na włączeniu urządzenia szpiegowskiego, o wyglądzie PenDriva, do portu USB komputera i uruchomieniu programu służącego do kontrolowania jego funkcjami.

Możliwości kilku reklamowanych transmiterów szpiegowskich to:

1. nagrywanie dźwięków wokół komputera, czyli podsłuch pomieszczenia;
2. podsłuch rozmów prowadzonych przez komunikatory internetowe takie jak Skype czy Gadu-Gadu;
3. rejestrowanie wszystkiego, co zostało napisane na klawiaturze;

331 http://www.programosy.pl/kategoria,monitoring_komputera,1,1.html(04.02.2012)

332 Znany również jako profesjonalna pluskwa komputerowa.

333 http://www.youtube.com/watch?v=PPgsZYutIlw&feature=player_embedded(01.02.2012)

4. zapamiętuje informacje o uruchamianych programach, odwiedzanych stronach internetowych, wpisywanych danych w formularzach na stronach www, wiadomościach pisanych w komunikatorach (np. gadu-gadu) i na portalach społecznościowych (np. nasza-klasa, facebook, randkowych);
5. zapisanie zrzutów ekranu co określony czas, pozwala to na odtworzenie sposobu używania komputera przez użytkownika;
6. rejestracja dokładnego czasu wykonywania tych czynności;
7. w wersji mail – prowadzenie zdalnego monitoringu komputera i przesyłanie wszystkich informacji na skrzynkę e-mail;
8. umożliwianie monitorowania konta użytkownika z ograniczeniami bez uprawnień administratora;
9. oprogramowanie niewykrywalne przez programy antywirusowe i zapory firewall;
10. bardzo proste zainstalowanie i konfiguracja, urządzenie jest od razu gotowe do użycia;
11. działanie programu niemożliwe do wykrycia przez użytkownika komputera, dzięki czemu użytkownik nie będzie wiedział, że jest szpiegowany;
12. zapewniona pełna dyskretna kontrola komputera;
13. urządzenie dostarczan w formie przenośnej pamięci PenDrive o pojemności 4GB, działa także jako zwykła pamięć;
14. urządzenie produkowane w różnych wersjach językowych polskiej, angielskiej i niemieckiej.

Reklamowane urządzenia typu szpieg komputerowy mogą być wykorzystywane jako: monitoring pracowników czy opiekun dziecka, a także pomagają przechytrzyć innych szpiegów i nieuczciwych partnerów. *Dzięki naszemu szpiegowi będziesz wiedział czy i z kim flirtuje Twoja żona, podczas gdy Ty ciężko pracujesz po godzinach. Sprawdzisz czy mąż rzeczywiście ogląda mecz z kumplami, czy może surfuje po serwisach randkowych*[334].

Systemy monitorowania komputerów i sieci umożliwiają szereg różnorodnych działaniach polegających również na:

1. śledzeniu i analizowaniu ruchu pakietów w sieci komputerowej,
2. znajdowaniu błędów w istniejącej konfiguracji sieci i jej składowych,
3. rozwijaniu i pielęgnacji sieciowego oprogramowania.

334 Kolejne reklamy to np.: Zastanawiasz się co dzieje się za zamkniętymi drzwiami pokoju Twojego malucha? Czy na pewno odrabia lekcje czy może przegląda strony przeznaczone dla dorosłych? Dzięki naszemu programowi będziesz mógł kontrolować czas jaki Twoje dziecko spędza w sieci oraz kontakty jakie tam nawiązuje. Twoja czujność może pomóc uniknąć tragedii. Nasz system z powodzeniem wykorzystasz w biurze lub firmie. Dowiesz się czy Twoi pracownicy rzetelnie wykonują swoje obowiązki czy może spędzają czas na portalach społecznościowych lub komunikatorach internetowych. A może szukają pracy u konkurencji lub wynoszą z firmy poufne dane? Efektywny – program monitorujący. Dyskretny w działaniu oraz prosty w obsłudze i instalacji. To szpieg komputerowy, który pozwoli Ci w skuteczny sposób prowadzić monitoring klawiatury komputera swoich pracowników, męża, żonę, partnerkę czy partnera. Opiekun dziecka – masz pełną kontrolę nad tym co w sieci robi twoje dziecko. Poznaj prawdę o tym czy w twoim związku pojawiła się zdrada. Pojawia się również trafna reklama wspominająca o możliwości ujawnienia oszusta. Szerzej: http://www.keylogger-szpieg.pl/(01.02.2012)

Monitorowanie sieci można podzielić na pasywne i aktywne. Pasywne polega na obserwowaniu sieci i obiektów sieciowych bez bezpośredniego oddziaływania na ich stan. Natomiast monitorowanie aktywne, zwane zarządzaniem, pozwala również zmieniać stan obiektów monitorowanych, a także oddziaływać na nie bezpośrednio.

Monitorowanie pasywne dzieli się na obrazujące w czasie rzeczywistym komunikację sieciową i na retrospektywne, korzystające z wcześniej zgromadzonych danych.

Zdefiniowano pięć kluczowych obszarów zarządzania siecią: zarządzanie błędami, bezpieczeństwem, wydajnością, konfiguracją i kontami. Zarządzanie siecią można zdefiniować jako proces kompleksowego kontrolowania danych sieci w celu zwiększenia jej wydajności i produkcyjności.

Wyprodukowane nowoczesne urządzenia służą do wysyłania i odbierania pakietów sieciowych. Przy czym odbieranie polega na „podglądaniu" pakietów płynących siecią i przekazywaniu każdego, który spełnia określone kryteria, do procesu docelowego[335].

## 5. Podsłuchy na tle praktyki szpiegostwa elektronicznego

Na popularnym internetowym portalu aukcyjnym można kupić urządzenia podsłuchowe, (tzw. pluskwę) za niewielką sumę, a przykładowo:

1. za 200 zł – urządzenie rejestrujące wszystkie rozmowy w promieniu kilku metrów co najmniej przez 24 godziny;
2. za 700 zł – urządzenie do podsłuchu telefonicznego, które umieszcza się wewnątrz telefonu, a działa nawet rok;
3. za ok. 1.200-1.500 zł – profesjonalne urządzenie z mikronadajnikiem, który przekazuje na bieżąco wszystkie rozmowy prowadzone z danego telefonu.

Jednakże najdroższa i najtrudniejsza do wykrycia jest aplikacja szpiegowska typu „Spy-phone" – instalowana zdalnie, w formie zamaskowanego SMS-u. Użytkownik zaatakowanego telefonu nie ma szans na jej wykrycie.

Największym powodzeniem cieszy się urządzenie z mikroskopijnym zasilaczem za ok. 2.500 złotych. Wersja wysokiej klasy kosztuje 5.000-8.000 złotych i wyposażona jest w miniaturowy nadajnik, który jest bieżącym przekaźnikiem danych do odbiorcy. Ponadto, za 1.500 zł można kupić rejestrator, który w siedzibie właściciela zapisuje i archiwizuje podsłuchiwane treści. Dzięki temu w każdej chwili można je odsłuchać.

Współczesne metody podsłuchiwania nie kojarzą się wyłącznie z fabułą powieści czy filmów szpiegowskich. Stosowanie podsłuchów nie tylko przez służby specjalne wszystkich krajów stało się powszechne. Podsłuchują biznesmeni i konkurenci, politycy i przestępcy. Podstawowym powodem inwigilacji obywateli była rzekoma walka z terroryzmem i pozorowane przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Wiele spraw karnych zaczęło się właśnie od informacji zaczerpniętych z podsłuchiwanych rozmów.

Doceniając te sukcesy kolejni specjaliści spowodowali postęp w technice szpiegowskiej, a na rynku pojawiły się nowoczesne, profesjonalne urządzenia.

Podsłuchy, zarówno w biznesie, jak i w polityce wymagają pomysłowości. Jej przykładem mogą być: prezent z podsłuchem, którego współczesnym wynalazcą był ambasador ZSRR w Waszyngtonie. W latach 70. XX w. podczas okolicznościowe-

335 http://students.mimuw.edu.pl/SR/prace-mgr/korol/index.html(04.02.2012)

go spotkania wręczył ówczesnemu wiceprezydentowi USA pióro wieczne, życząc, aby służyło do podpisywania traktatów pokojowych. Zainstalowany podsłuch, przysporzył sowieckiemu wywiadowi wielu cennych informacji. Podobny sposób wykorzystał dyrektor pewnej znanej firmy farmaceutycznej. Spotkał się on w 2008 roku, w Warszawie z szefem konkurencyjnej spółki, aby porozmawiać o podziale rynku. Na wstępie wręczył swojemu rozmówcy elegancki, pozłacany zegar stojący zawierający logo firmy. We wnętrzu zegara znajdował podsłuch z miniaturowym nadajnikiem. Ofiarodawca słyszał i rejestrował wszystko to, co działo się w gabinecie rywala. A efektem było wytypowanie i poznanie wielu danych dotyczących kandydatów na nowych klientów i rozpoznanie metod ich pozyskiwania.

Ustalono, że pod Warszawą budowany jest dom jednego z prezesów konkurencyjnej firmy. W surowych jeszcze ścianach umieszczono urządzenia podsłuchowe nowej generacji. Potem dom został otynkowany, a tynki przykryły urządzenia. W ten sposób zarząd rywalizującej firmy dowiadywał się wszystkiego o życiu, zwyczajach i pracy szefa konkurencji.

Innym sposobem jest zlecenie specjalistom umieszczenie podsłuchu w samochodzie służbowym, w toalecie, gdzie również prowadzone są ważne rozmowy, (także telefoniczne)[336].

Najnowsze osiągnięcia naukowe mogą mieć zastosowanie przy podsłuchach i podglądach. Przykładowo, żywe zwierzęta kontrolowane przez wszczepione czipy będą zwiadowcami nowej generacji. Nad takimi cyborgami pracuje amerykańska Agencja Zaawansowanych Projektów Obronnych (DARPA) przygotowująca nowe technologie do użycia przez wojsko. Najnowszy pomysł naukowców to owad z wszczepionym w odwłok układem, który umożliwia zdalne sterowanie jego lotem. Badania są prowadzone z motylami i karaluchami[337].

Uzasadnione jest przekonanie, że stosowanie podsłuchów na masową skalę stało się elementem walki biznesowej. Dotyczy to nieuczciwej konkurencji, bo przecież najczęściej chodzi o ujawnienie tajemnic przedsiębiorstwa. Proceder ten doprowadził do powstania i prężnego rozwoju nowej gałęzi rynku: usług kontrwywiadowczych w różnych formach, a przede wszystkim antypodsłuchowych, czyli przeciwdziałania szpiegostwu gospodarczemu[338], którą to dziedziną zainteresowane są szczególnie: *banki i firmy ubezpieczeniowe, różnego rodzaju korporacje, duże firmy farmaceutyczne i inne przedsiębiorstwa, które ostro i brutalnie rywalizują z konkurencją. Takie zadania kontrwywiadowcze realizują zarówno firmy detektywistyczne, jak i specjaliści z zakresu wywiadu gospodarczego. Jednakże dopiero praktyka śledcza wykaże czy są to w rzeczywistości nielegalni „łowcy szpiegów". Tymczasem niezwykle ważną dzia-*

336 L. Szymowski,*Szpieg w biznesie*, „Angora" nr 5(1129) z 5 lutego 2012 r.

337 P. Kościelniak, *Owad zdalnie sterowany* http://www.rp.pl/artykul/320825,810456-Owad-zdalnie-sterowany.html(11.02.2012)

338 Por.: L. Szymowski, Szpieg w biznesie, wyd. cyt.

*łalność prowadzą firmy zajmujące się wykrywaniem podsłuchów. Najczęściej polega to na mozolnym przeszukiwaniu biura klienta, przy pomocy specjalnego detektora, w celu zlokalizowania podłożonego urządzenia* np. w telefonie, telewizorze czy lampie. Najczęściej skanowanie całego gabinetu trwa około 8 godzin i kosztuje blisko 5 tys. zł. Przeszukać należy nie tylko gabinet prezesa, a wszystkie pomieszczenia, gdzie odbywają się narady. Duża firma powinna być przygotowana na wydatek nawet do 100 tys. zł.

W przypadku ujawnienia urządzeń podsłuchowych, aparatów fotograficznych czy kamer, mikrofonów – co jest dzisiaj zupełnie realne dzięki powszechnej dostępności nowoczesnych technologii – łatwo ustalić ich wykonawcę, a niejednokrotnie zleceniodawcę, niezbędne jest stosowanie odpowiednich środków zabezpieczających i powiadomienie organów ścigania zgodnie z art. 504 k.p.k.

## 6. Wybrane metody i techniki stosowane przez profesjonalistów

### 6.1. Techniki tradycyjne

W ogólnodostępnej literaturze przedmiotu można wyłonić pewien zakres informacji dotyczących przechwytywania i przekazywania różnorodnych wiadomości, zapisywanie ich do dziennika informacji o wiadomościach i połączeniach, zdalne podsłuchiwanie i potajemne zestawianie połączeń, a także usługi lokalizacyjne, oto niektóre tylko elementy mogące stanowić niezwykle istotną bazę danych zarówno dla zorganizowanych przestępców, jak i cyberprzestępców, a cyberterrorystów w szczególności. Metody działania są zróżnicowane, od prostych aż do zainstalowanej w pełni funkcjonalnej aplikacji szpiegowskiej, co całkowicie pozbawia prywatności podczas rozmów, gdyż osoba kontrolująca oprogramowanie ma dostęp do wszystkich informacji.

Narzędzia tego typu mogą posłużyć do zdrady tajemnicy przedsiębiorstwa, szpiegostwa przemysłowego, kradzieży tożsamości i informacji z baz danych, podszywania się pod inne osoby, aż do oszustw finansowych (a szczególnie bankowych czy giełdowych) na szkodę instytucji finansowych i ich klientów.

Różnego rodzaju wywiadowcy i szpiedzy gospodarczy stosują zróżnicowane metody i techniki – od najprostszych, jak np. biały wywiad, do najbardziej skomplikowanych, jak gra operacyjna, a nawet wyrafinowane przestępstwa komputerowe. Generalnie rzecz biorąąc stosowane metody działania szpiegów gospodarczych to przede wszystkim:

1) techniki personalne**,** tj. docieranie do odpowiednich pracowników przy pomocy korupcji lub szantażu polegającego na kupowaniu lub wymuszaniu informacji; infiltracja środowiska poprzez wyszukiwanie osób uważających się za pokrzywdzone przez firmę, zwalnianych lub poszukujących zatrudnienia w innej firmie;
2) wykorzystywanie tradycyjnych, czyli technicznych źródeł informacji**,** a szczególnie:

- kradzież lub przywłaszczenie zbiorów danych,
- wykorzystywanie materiałów zużytych, na przykład: wydruków i nośników informacji,

- podłączanie się do systemu teleinformatycznego i stosowanie podsłuchu;
- instalowanie transmiterów wewnątrz komputerów;
- stosowanie podsłuchu czy podglądu odpowiednich osób i pomieszczeń;
- inne – nie ujawnione do publicznej wiadomości;

3) stosowanie najnowszych środków technicznych**,** zarówno powszechnie dostępnych, jak i będących wyłącznie w dyspozycji służb specjalnych czy grup wysoko wykwalifikowanych inżynierów umożliwiających przede wszystkim:
   a) przechwytywanie i analizowanie promieniowania elektromagnetycznego emitowanego przez sprzęt komputerowy,
   b) przechwytywanie i analizowanie wiązek mikrofal łączności satelitarnej;
   c) inne – nie ujawnione do publicznej wiadomości;

Wszystkie nowe technologie nastawione są na pozyskiwanie informacji za pomocą programów komputerowych, a w szczególności:

- technologie analityków – agentów, którzy wyszukują informacje na zamówienie,
- pojawią się inteligentne interfejsy wyszukujące odpowiednie informacje z najróżnorodniejszych typów serwerów,
- raporty wywiadowców-analityków oparte na programach umożliwiających realizację określonego polecenia,
- przeciwdziałanie szpiegostwu komputerowemu również oparte na programach komputerowych m.in. poprzez: skanowanie i analizowanie poczty elektronicznej, bazy danych, poczty wewnętrznej i innych.

W rezultacie stosowanie sabotażu komputerowego w działaniach wywiadów może być wykorzystywane przede wszystkim przez profesjonalne służby wywiadowcze. Zatem warto orientować się, że działania te polegają one na działaniach zmierzających do zakłócania lub uniemożliwiania automatycznego gromadzenia lub przekazywania informacji oraz na niszczeniu, wymianie, uszkodzeniu nośników lub urządzeń służących do automatycznego przetwarzania, gromadzenia czy przesyłania informacji.

## 6.2. Gra operacyjna i dezinformacja

Profesjonalne zbieranie informacji, obok rutynowych działań zapobiegawczych, nie jest wolne od różnego rodzaju gier wywiadowczych. Przykładem mogą być powszechnie znane wpadki wywiadu radzieckiego i japońskiego. Były to skutki swoistej gry operacyjnej, czy inaczej wywiadowczej prowadzonej najprawdopodobniej przez profesjonalne służby państwowe. Do metod tych zaliczyć należy stosowany z dużym powodzeniem przez Anglików, wybitnych specjalistów w tego rodzaju operacjach, a odnotowanych z dużym powodzeniem w czasie II wojny światowej tzw. brytyjski system podwójnych agentów[339]. Brak jest podstaw, aby negować podobne przedsięwzięcia w ramach intensywnie rozwijającego się na całym świecie wywiadu gospo-

339 Szerzej: J.C. Masterman, *The Double Cross System in the War of 1939 – 1945,* Yale University Press 1972. Tłumaczenie tej pracy: *Brytyjski system podwójnych agentów 1939-1945* ukazało się nakładem Wydawnictwa Ministerstwa Obrony Narodowej w 1973 r. Ten dokument historyczny pozwala uświadomić, że system podwójnych agentów, w czasie drugiej wojny światowej, był rewelacyjnym wynalazkiem angielskich specjalistów. Natomiast współczesna praktyka wywiadu państwowego w niektórych krajach zna już system potrójnych agentów.

darczego i konieczności intensywnego przeciwdziałania w postaci profesjonalnych działań zapobiegawczych.

Wśród różnorodnych form kontrwywiadu gospodarczego czy przemysłowego istotne miejsce zajmuje taktyka zdyskredytowania konkurenta, naruszenia jego pozytywnego wizerunku lub sprowokowania jego pożądanej reakcji. Zatem skuteczna wydaje się dezinformacja.

Dezinformacja według T.R. Aleksandrowicza oznacza taki sposób przekazywania informacji prawdziwej lub fałszywej, aby wprowadzić w błąd konkurenta czy przeciwnika i skłonić go do zachowania zgodnego oczekiwaniami i dla nas korzystnego. Polega raczej na stworzeniu odpowiednio szerokiego pola możliwości intelektualnych, by w umyśle przeciwnika doszły do głosu jego własne preferencje. Istotą dezinformacji jest danie przeciwnikowi argumentu, by wierzył w to, w co chce wierzyć. Nic na świecie nie przekona człowieka do tego, w co nie chce wierzyć, natomiast byle pretekst wystarczy, by zignorował on nawet wiele dowodów przeszkadzających w wyciągnięciu wniosków, jakie chciałby wyciągnąć"[340]. Zatem dezinformacja nie jest prostym kłamstwem, czyli przekazaniem fałszywej informacji, a jest podstępem.

Przedsięwzięcia polegające na dezinformacji niejednokrotnie są przeprowadzane na podstawie informacji prawdziwych, lecz podanych w taki sposób, iż konkurent uznaje je za fałszywe. Nawet sprawdzając wiarygodność badanych źródeł napotyka przynajmniej na kilka niezależnych od siebie źródeł i kanałów informacyjnych. Dezinformacja w zasadzie nie usiłuje zakryć prawdy.

Dezinformacja może spowodować daleko idące skutki, jak to miało miejsce w przypadku afery z perfumami *Champagne* we Francji. Producenci szampana uzyskali wyrok sądowy zabraniający stosowania tej nazwy do kosmetyków. Tuż po ogłoszeniu wyroku właściciele perfumerii otrzymali telefoniczne polecenie zniszczenia całego zapasu. Ekipie, która przybyła w tym celu wydano dobrowolnie cały posiadany zapas perfum. Trudno opisać zdziwienie, kiedy wkrótce do właściciela perfum zwrócił się producent, aby nie wyrzucać flakonów z perfumami, a jedynie zmienić ich etykietę. Śledztwo nie doprowadziło do ustalenia, kim byli autorzy dezinformacji: złodziejami, czy agentami konkurencji[341].

Jedna z firm francuskich produkujących środki do prania miała zwyczaj dokonywania testów w tym samym regionie. Zwyczaj ten odkryła firma konkurencyjna, która podjęła fałszowanie testów poprzez podejmowanie akcji promocyjnych mających na celu zablokowanie wprowadzenia na rynek nowych, konkurencyjnych, czyli groźnych produktów. Jakość tych produktów oceniano jako mierną. Podstawowym celem konkurencyjnej firmy było skłonienie rywala do nadmiernej rozbudowy mocy produkcyjnych i spowodować w ten sposób zamrożenie znacznych kwot pieniężnych[342]. Powyższy przykład ma na celu zilustrować jedną z podstawowych zasad taktyki kontrwywiadu gospodarczego, która brzmi: najlepszą taktyką jest nadwyrężanie budżetu przeciwników**.**

W efektach działań wywiadowczych daje się zauważyć bardzo istotna prawidłowość, a mianowicie: im większa firma, tym większy dopływ informacji, tym większe zadowolenie i profity wywiadowców. Zatem, jeżeli duża organizacja przeznacza wy-

340 T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 98, 99.
341 B. Martinet, Y.M. Marti, *Wywiad ....,* s. 198.
342 Tamże, s. 214.

starczające środki na wywiad gospodarczy, z pewnością zaowocuje to odpowiednimi efektami ekonomicznymi. Istotnym problemem jest jednak pytanie: czy takie efekty z pewnością będą miały wiele wspólnego z etyką biznesu?

### 6.3. *Benchmarking* i inne metody

Profesjonalne metody działań wywiadu i kontrwywiadu gospodarczego, opierają się na metodach naukowych, a zawierają wiele przedsięwzięć o charakterze perfekcyjnym. Wymienia się przede wszystkim:

- opracowywanie scenariuszy działań agresywnych,
- stosowanie różnorodnych form dezinformacji,
- *Due diligence* oznaczający należytą staranność w analizowaniu określonej sytuacji prawnej, gospodarczej i finansowej,
- wojny patentowe, np.: niezgłaszanie wynalazków do opatentowania, zachowanie dyskrecji mimo uzyskania patentu, kamuflowanie swoich patentów oraz mnożenie wniosków patentowych;
- ochrona informacji na tle współdziałania, a nawet integracji na linii: klient – dostawca;
- ochrona informacji zawodowych w trakcie negocjacji z klientami;
- wykorzystywanie niezadowolenia lub gadatliwości pracowników firm konkurencyjnych[343];
- penetrowanie wytypowanych wcześniej lub *ad hoc* namierzonych uczestników kongresów naukowych;
- monitorowanie informacji medialnych.

Aktualny system napływu informacji, czyli stale zwiększająca się liczba kanałów informacyjnych, doprowadzić może do swoistych przekłamań, szumu informacyjnego, zaplanowanej dezinformacji, a niejednokrotnie nawet do nieświadomej czy nieplanowanej dezinformacji. Przykładem w tej mierze może być przedsiębiorca japoński, który udzielił wywiadu lokalnej gazecie na temat produkcji nowoczesnego i skutecznego testera do ujawniania fałszywych banknotów. Wspomniany przedsiębiorca listownie poinformował o tym fakcie swojego kolegę bankowca w Londynie. Informacja została wprowadzona do międzynarodowej bazy danych, a w europejskim piśmie z dziedziny techniki ukazał się artykuł o testerze. Fragmenty tej publikacji cytowano w literaturze przedmiotu.

W związku z nasilającymi się wciąż fałszerstwami znaków pieniężnych i związanym z tym dużym zainteresowaniem polskich bankowców wspomnianym testerem, autor niniejszej książki w 1994 roku, po zapoznaniu się z treścią jednego z artykułów, po długich poszukiwaniach zwrócił się pisemnie do japońskiego przemysłowca, od którego pochodziła źródłowa informacja. Po wykonaniu wielu czynności sprawdzających okazało się, że wynalazca-przemysłowiec planuje dopiero badania nad opracowaniem wspomnianego testera, lecz z uwagi na brak funduszy odłożył prace na bliżej nieokreśloną przyszłość.

343 Wyciekanie informacji za sprawą współpracowników jest powszechnie znane. Dobrym ostrzeżeniem może być angielskie powiedzenie z czasów drugiej wojny światowej: *Loose lips sink chips,* co w wolnym tłumaczeniu oznacza –- nieostrożne gadanie zatapia statki.

*Benchmarking* polega na porównaniu cech organizacji z konkurentami lub firmami wiodącymi w danej branży oraz kopiowanie sprawdzonych wzorów. Porównywanie takie stosowane jest od dawna, stąd niektórzy autorzy wskazują, iż nie jest metoda zasługująca na szczególną uwagę. Termin *benchmarking* pochodzi z języka angielskiego, gdzie *benchmark* to ustawiony na widocznym z daleka miejscu, np. na wzgórzu, punkt orientacyjny wykorzystywany w pomiarach niwelacyjnych.

Stosując *benchmarking* próbuje się wyeliminować podstawowy problem porównań – niemożność bycia lepszym niż ten, od kogo zapożyczamy rozwiązania. Oznacza działania polegające na analizowaniu produktów konkurencji i wyciągnięciu wniosków przy projektowaniu produktów własnych, czyli uczeniu się od konkurencji. Powszechnie uznawany jest jako działanie etyczne w ramach wywiadu gospodarczego. Niezbędna potrzeba prowadzenia systematycznej analizy działań podejmowanych przez konkurentów doprowadza do poszukiwania nowych metod zarządzania i urealnia konieczność zmian dla poprawienia sytuacji ekonomicznej. Przedsiębiorcy są zmuszeni do ciągłego śledzenia poczynań konkurentów. Jednym ze skutecznych narzędzi stosowanych w ramach wywiadu gospodarczego jest właśnie *benchmarking*, którego znaczenie w dobie niezwykle nasilonej konkurencji i rozwoju technologii na rynkach globalnych wzrasta.

*Benchmarking* to proces systematycznego porównywania własnego przedsiębiorstwa z innymi, albo porównywania ze sobą różnych działów przedsiębiorstwa, aby ustalić stan obecny i czy potrzebna jest jakaś zmiana. Zwykle poszukiwane są przykłady wykazujące najwyższą efektywność działania w danym obszarze, co pozwala na naśladowanie najlepszych. Jednakże poprawianie obszarów firmy nie powinno mieć charakteru jednorazowego. Konieczne jest stałe gromadzenie informacji i poszukiwanie lepszych rozwiązań[344].

W aspektach historycznych podstaw *benchmarkingu* jako metody działania można się dopatrywać u filozofa chińskiego Sun Tsu, żyjącego około 500 r. p.n.e., a także w zasadach japońskich sztuk walki, które głosiły, że należy poznać swoje silne i słabe strony, poznać i uczyć się od najlepszych by osiągnąć zwycięstwo[345].

Genezy europejskiego *benchmarkingu można* dostrzec w 1983 roku w ramach specjalnego programu koncernu Xerox. Opracowano wówczas program mający na celu uratowanie firmy przed upadkiem. Wprawdzie program nosił nazwę „Bycie liderem poprzez jakość" ale druga część nosiła tytuł *Benchmarking* i stosowana była od 1979 roku, gdy w ofercie japońskiego Canona pojawił się produkt tańszy, ale porównywalny pod względem technicznym. Xerox rozpoczął nowatorskie badania mające na celu porównywanie własnych rozwiązań z rozwiązaniami stosowanymi przez najlepsze przedsiębiorstwa, dążąc do odbudowania swojej pozycji na rynku[346].

Według American Productivity and Quality Centre, *benchmarking* to proces identyfikacji i zrozumienia najlepszych praktyk i procesów zarządzania oraz ich przejmowania od innych światowych organizacji, wspomagania swojego przedsiębiorstwa w celu poprawienia efektywności działania. Istotą jest zatem ciągły proces, w którym

344 http://mfiles.pl/pl/index.php/Benchmarking(22.03.2015)

345 J. Dahlgaard, K. Kristensen, G.K. Kanji, *Podstawy zarządzania jakością,* Warszawa 2004. Cyt. za: M. Solak, *Benchmarking jako skuteczne narzędzie wywiadu gospodarczego,* w: J. Kaczmarek, M. Kwieciński (red.) *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 288.

346 J.P. Lendzin, A. Stankiewicz-Mróz, *Wprowadzenie do organizacji i zarządzania,* Kraków 2005, s. 184.

porównywane są produkty, usługi oraz procesy i metody funkcjonowania wielu firm. Proces ten ma na celu ujawnić różnice między przedsiębiorstwami oraz ustalić powody tych różnic, a także wnioskować w zakresie sposobów i metod ich doskonalenia. Badania porównawcze należy przeprowadzać z przedsiębiorstwami wiodącymi w badanych metodach i procesach, Tego rodzaju firmy określane są mianem „*best in class",* czyli najlepszych we własnej klasie, branży, a stosowane działania mają prowadzić do naśladowania najlepszych przedsiębiorstw i wypracowanych metod.. Jednakże na uwagę zasługuje dążenie do naśladownictwa o twórczym charakterze.

*Benchmarking* konkurencyjny dotyczy bezpośrednich konkurentów firmy, którzy są liderami z tego samego sektora, wytwarzającymi zbliżony asortyment lub posiadającymi podobną technologię wytwarzania. Jednym z przykładów jest zakup wyrobów konkurencji oraz analiza ich cech i atrybutów, w celu porównania z własnym produktem oraz zaadaptowania najlepszych rozwiązań. Natomiast b*enchmarking* ogólny, zwany też funkcjonalnym, polega na porównaniu się pod względem podobnych funkcji z organizacjami nie będącymi konkurentami z tego samego sektora działalności, w celu odkrycia stosowanych przez nie nowatorskich rozwiązań stosowanych przy realizacji określonych funkcji, np. logistyki lub obsługi klienta[347].

W Europie wprowadzono *European Benchmarking Code of Con- duct* – kodeks etyczny na bazie promowanego przez *International Benchmarking Clearinghouse,* dostosowany do prawa Unii Europejskiej[12]. Obejmuje on osiem następujących zasad:

- dobrego przygotowania – aby oszczędzić czas partnera benchmarkingowego, należy się wcześniej odpowiednio przygotować,
- kontaktów – należy ustalić procedury i osoby odpowiedzialne za kontakty między współpracującymi firmami,
- wymiany – analizować informacje o podobnym poziomie istotności, jakie udostępnia firma wzorcowa,
- poufności – wszystkie uzyskane dane należy traktować jako poufne i nie rozpowszechniać bez zgody partnera,
- wykorzystania informacji – tylko do wcześniej ustalonych i zaakceptowanych celów,
- legalizmu – najbardziej podkreślana zasada, odnosząca się do zdobywania informacji w sposób legalny i z legalnych źródeł,
- sfinalizowania – należy dążyć do wypełnienia wcześniejszych uzgodnień,
- zrozumienia partnerów i sposobu, w jaki chcę wykorzystać przekazywane informacje.

Można wyróżnić dwa podstawowe cele: pierwszym jest fakt, że przestrzeganie powyższych zasad uchroni przedsiębiorstwo przed posądzeniem o stosowanie szpiegostwa gospodarczego. Natomiast drugim mającym znaczenie praktyczne jest uzasadnione przekonanie, że omawiana metoda działania zapewnia jedno z najlepszych narzędzi wywiadu gospodarczego, stosowane w celu rozwiązywania problemów, usprawniania procesów, wprowadzania innowacji, a także dążenia do realizacji założonego celu, czyli poprawy jakości i wyników ekonomicznych przedsiębiorstwa.

Warto rozpowszechniać omawianą metodę działania nie tylko w przedsiębiorstwach, lecz również w administracji z nadzieją, że poprawi ona praktykę funkcjonowania wielu instytucji i organizacji.

347 M. Solak, *Benchmarking jako*.. wyd. cyt.,

## 6.4. *Due diligence* – jako istotny materiał dla analiz wywiadu gospodarczego

*Due diligence*, czyli należyta staranność, to analiza sytuacji prawnej, gospodarczej i finansowej spółki przygotowywana w związku z zamiarem dokonania transakcji przejęcia spółki. Celem takiej analizy jest ustalenie, na jakim poziomie ekonomicznym znajduje się badana firma.

Efekty badania *due diligence* są doskonałym materiałem dla różnorodnych analiz i wniosków przydatnych dla potrzeb wywiadu gospodarczego. Ten zespół kompleksowych analiz dotyczących wartości ekonomicznych przedsiębiorstwa, zasad jego zarządzani, kapitału ludzkiego, a także potencjału twórczego czy produkcyjnego, może być wzięty nie tylko do przejęcia, ale także jako istotny zasób przydatny do współpracy czy walki konkurencyjnej z badaną firmą, na przykład w zakresie produkcji czy usług.

Badanie *due diligence* powinno być prowadzone w sferze biznesowej, prawnej i finansowo-podatkowej oraz obejmować wszystkie sfery działalności spółki, a zwłaszcza audyt: korporacyjny, finansowy, podatkowy, pracowniczy. Powinno obejmować również zagadnienie sporów sądowych i postępowań administracyjnych, nieruchomości, zawartych umów i innych zagadnień według właściwości badanej spółki. W trakcie audytu pracowniczego należy zbadać m.in.: stan zatrudnienia, podstawy zatrudnienia, zawarte umowy o pracę i kontrakty menedżerskie, regulaminy pracy, regulaminy wynagradzania, regulaminy zakładowego funduszu świadczeń socjalnych. Z kolei audyt korporacyjny powinien opisywać m.in. strukturę kapitałową badanej spółki lub grupy spółek, powiązania z innymi podmiotami, uprawnienia osobiste wspólników, dopuszczalność ewentualnych działań restrukturyzacyjnych, badanie składu i sposobu działalności organów[348].

Audyt, a następnie raport z wyników badania powinien obejmować szczególne obszary właściwe dla danej branży, w tym badanie spełnienia wymogów wykonywania działalności reglamentowanej, prowadzonej na podstawie koncesji, licencji lub zezwoleń. Powinien również wskazywać potencjalne szanse i zagrożenia oraz przedstawiać ich ewentualne konsekwencje w każdej sferze. Jako najpoważniejsze zagrożenia to m.in. zła kondycja finansowa firmy, zagrożenie upadłością, realizacja zawartych niekorzystnych kontraktów, istnienie sporów sądowych o zapłatę wysokich kwot.

Strona techniczna prowadzonego badania *due diligence* odbywa się poprzez analizę wszystkich dokumentów spółki, udostępnionych w tzw. pokoju danych, który może być pomieszczeniem w spółce lub też platformą informatyczną, gdzie dostępne są w wersji elektronicznej kopie wszystkich dokumentów. Ze względu na to, że dostęp do dokumentów badanej spółki mają osoby ze spółki konkurencyjnej, częstą praktyką jest składanie oświadczeń o zachowaniu poufności oraz o niewykorzystywaniu uzyskanych informacji w celach gospodarczych[349].

Wykorzystanie raportu *due diligence* dla potrzeb wywiadu gospodarczego powinno odbyć się w aspektach założeń, analiz i wniosków dotyczących planowanego czy prognozowanego kierunku działania.

348 D. Reck, T. Kowolik, *Due diligence chroni przed nieodpowiednią fuzją*, „Rzeczpospolita" z 4.03.2015
349 Tamże.

### 6.5. Program *Know Your Customer* (KYC) – Poznaj Swojego Klienta

KYC jest niezwykle wnikliwym źródłem poszerzającym wiedzę o badanej firmie w zakresie informacji o potencjalnych i obecnych klientach, pozwala bowiem na dokonanie szczegółowej analizy. To doskonałe połączenie informacji z globalnej bazy danych oraz instytucji skupiających dane o praniu pieniędzy czy list sankcyjnych. Program ten ma znaczenie praktyczne, gdyż jest wnikliwym źródłem poszerzającym wiedzę o badanej firmie w zakresie informacji o:

1) powiązaniach firmy z innymi podmiotami w kraju i za granicą,
2) obecności osób zarządzających firmą na listach sankcyjnych,
3) nformacji o obecności firm na giełdach światowych,
4) sytuacji gospodarczej w danym kraju (w postaci ratingu kraju).

Korzyści z posiadania programu to przede wszystkim:

1. możliwość dokonania głębszej analizy potencjalnych i obecnych klientów,
2. monitorowanie działalności firmy w celu zapewnienia zgodności z obowiązującymi przepisami prawa, regulacjami i polityką przedsiębiorstwa. (To zagadnienie określane jest również jako *compliance*),
3. ochrona instytucji finansowych przed negatywnymi skutkami prawnymi, związanymi ze współpracą z podmiotami wspierającymi terroryzm,
4. zminimalizowanie i analiza ryzyka współpracy z firmą.

Program dostarcza informacji szczególnie na temat:

1. ostatecznego właściciela badanej firmy (ostateczny beneficjent),
2. danych rejestrowych,
3. osób i firm na listach sankcyjnych,
4. składu zarządu firmy badanej,
5. giełd, na których notowana jest firma,
6. danych finansowych podmiotu,
7. kondycji kraju, w którym zarejestrowana jest firma.

Program korzysta głównie z następujących źródeł wiedzy:

1. Światowa baza (powiązania oraz dane rejestrowe),
2. HM Treasury list (Ministerstwo Skarbu UK),
3. OFAC list (Rządowa Agencja USA)
4. PEP list (Lista osób publicznych wyeksponowanych na korupcję i pranie pieniędzy[350]),
5. UN Security Council Sanctions Comittee,
6. Foreign Affairs and International Trade Canada,
7. UK Foreign & Commonwealth Office,

350 To zagadnienie w Polsce ujęte jest w art. 1 pkt 1f ustawy z 16 listopada 2000 roku o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (tj. Dz. U. z 2010 r.Nr 46, poz. 276). Wspomniana ustawa na podstawie Trzeciej Dyrektywy Komisji Europejskiej (2005/60/EC) w sprawie prania pieniędzy zakłada obowiązek raportowania podejrzanych transakcji oraz identyfikacji klientów.

8. Australian Department of Foreign Affairs and Trade,
9. ponad 100 list sankcyjnych z całego świata.

Korzystanie z Programu KYC, pozwala na dokonanie analizy potencjalnych i obecnych klientów. To doskonałe połączenie informacji z globalnej bazy danych oraz instytucji skupiających dane o praniu pieniędzy czy list sankcyjnych.

Jako korzyści ze stosowania KYC należy wymienić przede wszystkim:

1. dokonanie głębszej analizy działalności potencjalnych i obecnych klientów,
2. monitorowanie działalności firmy w celu zapewnienia zgodności z obowiązującymi przepisami prawa, regulacjami i polityką przedsiębiorstwa,
3. ochrona instytucji finansowych przed negatywnymi skutkami prawnymi, związanymi ze współpracą z podmiotami wspierającymi terroryzm,
4. zminimalizowanie i analiza ryzyka współpracy z firmą.

KYC dostarcza informacji na temat:

1. ostatecznego właściciela badanej firmy (ostateczny beneficjent),
2. danych rejestrowych,
3. osób i firm na listach sankcyjnych monitorowanych przez D&B,
4. składu zarządu firmy badanej,
5. giełd na których notowana jest firma,
6. danych finansowych podmiotu,
7. kondycji kraju, w którym zarejestrowana jest firma.

Powyższy program posiada charakter światowy, zawiera wiele zalet i możliwości. Jego wnikliwość została wielokrotnie zweryfikowane przez zagraniczne i krajowe banki a także inne konsorcja, co gwarantowało bezpieczeństwo ich portfela transakcyjnego[351].

Współcześnie trudno jest stwierdzić, kto jest autorem programu. W Polsce po raz pierwszy zaistniał on w dniu 3 marca 1993 roku na sympozjum w Warszawie. Referat na ten temat wygłosił R. A. Small[352], prezentując program jako ważne narzędzie w przeciwdziałaniu praniu pieniędzy. Oto polska definicja aktywnie od tego czasu wykorzystywana w polskiej bankowości: *Program Poznaj Swojego Klienta określić można jako zbiór danych (elementów) składających się na aktualny stan wiedzy o kliencie w celu ustalenia jego wiarygodności i profilu transakcyjnego*[353]. Podstawowe czynności sprawdzające wówczas miały miejsce w 3 etapach: w trakcie otwierania rachunku, w ramach czynności zmierzających do identyfikacji tożsamości klienta oraz w trakcie współpracy z klientem, o ile zaistniały jakiekolwiek powody lub kwalifikacje do „grupy podwyższonego ryzyka". Takie grupy zostały wyłonione według określonych kryteriów już w 1991 roku przez ekspertów Financial Action Task Force.

Wyżej podana wersja KYC, zapewne została zmodyfikowana do współczesnych zagrożeń i potrzeb przez Bisnode D&B Polska Sp. Z o.o.[354].

351 http://www.dnb.com.pl/download/brochures/KYC.pdf(10.08.2015)

352 R.A. Small, *Know Your Customer Policy* (w:) Financial Action Task Force: Money Laundering Symposium. March 2-5. 1993, Warsaw, Poland.

353 J.W. Wójcik, *Kryminalistyczne problemy zapobiegania oszustwom zaliczkowym (nigeryjskim). Program Poznaj Swojego Klienta*, Toruń 1996, s. 90.

354 http://www.dnb.com.pl/AudytPowiazan.aspx?id=KnowYourCustomer(10.08.2015)

## 6.6. Era szpiegostwa w cyberprzestrzeni

Rozwój cywilizacji w cyberprzestrzeni szybko doprowadził najwybitniejszych specjalistów do przekonania, że jakiekolwiek środki ostrożności podejmowane w celu wyeliminowania nadużyć – okażą się zawodne. Natomiast prognostycznie rzecz biorąc należy spodziewać się, że różnego rodzaju manipulacje będą się mnożyć. Już w latach 70. XX wieku znana była uzasadniona teza, że komputeryzacja to nie koniec wywiadu gospodarczego, to tylko przejście na nowy, wyższy etap, umożliwiający większą efektywność działań[355].

Rodzaje i rozmiary wszystkich możliwych zagrożeń, związanych z ewentualnym bezprawnym dostępem do przechowywanych informacji nawet trudno sobie wyobrazić. Przykładowo, jedna z finansowych firm angielskich pod koniec lat 70. XX wieku posiadała komputer wartości 8 milionów USD. Jego zabezpieczenia i ochrona fizyczna były również niezwykle kosztowne. Natomiast dobra chronione były wprost nieobliczalnej wartości, gdyż w bazie danych znajdowały się informacje dotyczące 250 maklerów giełdowych i ich klientów. Dostęp do tego typu danych mógłby umożliwić swobodne manipulowanie giełdą londyńską.

Szpiegostwo w cyberprzestrzeni jest jedną z najistotniejszych form działania wszelkiego rodzaju współczesnych wywiadów. Polega ono na zdobywaniu takich danych, które – zawarte na nośnikach informacji, są przedmiotem zainteresowania innych organizacji (również zagranicznych), a szczególnie konkurencji, w tym także placówek naukowo-badawczych, rozwojowych, banków, innych instytucji finansowych itp.[356]

W ustawodawstwie wielu krajów pojęcie szpiegostwa w cyberprzestrzeni nie jest związane jedynie z działaniem na rzecz obcego wywiadu. Przykładowo, w Niemczech zachodzi wówczas, gdy określona grupa osób dokona przywłaszczenia lub spieniężenia danych uzyskanych z cudzej bazy informatycznej i wyrządzi szkody finansowe nawet osobom trzecim. Tego rodzaju przestępstw w Niemczech ujawnia się stosunkowo dużo. Z początkiem lat 90. XX wieku ujawniano blisko 200 takich spraw rocznie. Jednakże ich wykrywalność wciąż nie jest imponująca.

Formy szpiegostwa w cyberprzestrzeni są zróżnicowane. Już w 1988 roku do tego typu działań w Japonii zastosowano wirusa komputerowego. Ponadto, systematycznie stosowany jest podsłuch telefoniczny, podsłuch komputerowy i różne formy hakingu, a stale prognozowana jest możliwość wykorzystywania sabotażu.

Przestępstwo to polega na nielegalnym przechwytywaniu lub uzupełnianiu (zmianie) informacji przesyłanych poprzez systemy teleinformatyczne. Współczesne osiągnięcia techniczne pozwalają także na ingerencję związaną z wprowadzeniem informacji do podsłuchiwanego systemu. Są to zagrożenia zupełnie realne chociaż stosowanie ich jest kosztowne.

Świadomość możliwości nieuprawnionego stosowania różnego rodzaju technik podsłuchu, nie tylko przez wywiad gospodarczy lecz również przez służby specjalne, staje się niezwykle drażliwym problemem społecznym w wielu krajach świata. Okazuje się, że część stosowanych podsłuchów wobec niektórych osób, m.in. w stosunku do dziennikarzy, może pozostawać poza kontrolą niezawisłej instancji sądowej. Z uwagą przyglądają się temu problemowi polskie media[59].

We wrześniu 2016 roku portal Yahoo! ujawnił, że dwa lata wcześniej cyberprzestępcy ukradli dane ok. 500 mln osób korzystających z usług tego portalu głównie za

355 L. Bajer, *Wywiad gospodarczy,* Warszawa 1979, s. 96.

356 J.W. Wójcik, *Przestępstwa komputerowe*. Cz. I – *Fenomen cywilizacji*, wyd. cyt., s. 132 – 147.

pośrednictwem poczty elektronicznej. To była największa ujawniona do tego czasu cybernetyczna kradzież. O przygotowanie i przeprowadzenie tej akcji Departament Sprawiedliwości USA oskarżył dwóch oficerów Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej Igora Suszczina i Dmitrija Dokuczajewa, a także działających pod ich komendą hakerów Rosjanina Aleksieja Biełana i Karima Baratowa – Kazacha, który dostał obywatelstwo Kanady[357].

Wiadomo, że Federalna Służba Bezpieczeństwa (FSB) wywodzi się z sowieckiej tajnej policji KGB. FSB zajmuje się gównie kontrwywiadem, ale odpowiada również za wywiad elektroniczny. Na świecie coraz częściej FSB kojarzy się ze szpiegostwem cybernetycznym. Wspomniani agenci pod koniec roku 2014 wykradli z serwerów Yahoo! bazę zawierającą dane użytkowników, adresy e-mail, numery telefonów oraz informacje potrzebne do stworzenia ciasteczek autoryzujących dostęp do skrzynek. Następnie uzyskali dostęp do wewnątrzfirmowego narzędzia do zarządzania użytkownikami (Account Management Tool), które wykorzystywali, by tworzyć dla nich ciasteczka umożliwiające dostęp do ich zawartości.

Według komunikatu Departamentu Sprawiedliwości podczas tego cybernetycznego włamania skradziono kluczowe informacje na temat co najmniej 500 milionów kont na portalu Yahoo! Dzięki temu włamaniu można było także przeszukiwać zasoby innych dostawców Internetu. Jednak oficerów FSB interesowało przede wszystkim: 6,5 tys. kont należących do dziennikarzy z Rosji, urzędników państwowych z USA i Rosji, firmy transportowej z Francji i linii lotniczej z USA, amerykańskich firm z branży usług finansowych, a także banków ze Szwajcarii.

Natomiast w 2013 r. cyberprzestępcy wykradli dane co najmniej 1 mld użytkowników Yahoo! W zamian za swoje usługi dwaj hakerzy kierowani przez FSB mogli okradać klientów Yahoo! Poznawali dane pozwalające im korzystać z cudzych kart kredytowych i elektronicznych kart podarunkowych. Popełniali też bardziej wyrafinowane oszustwa. Oskarżeni o włamanie do Yahoo! hakerzy są doskonale znani specom od zwalczania cyberprzestrzępczości.

Aleksiej Biełan (29 lat) został oskarżony o cyberprzestępstwa w USA już w 2012 i 2013 r. Od listopada 2013 r. znajduje się na liście najbardziej poszukiwanych przez FBI cyberprzestępców. Od połowy 2013 r. jest również poszukiwany przez Interpol. Na tej podstawie został zatrzymany w 2013 r. w jednym z państw Europy, ale uciekł do Rosji. Formalnie rzecz biorąc, powinien tam być zatrzymany, bo Rosja należy do Interpolu. Ale tak się nie stało. W grudniu 2016 r. ówczesny prezydent USA Barack Obama nałożył sankcje na Biełana. Drugim poszukiwanym jest Karim Baratow (22 lat), który słynął wśród znajomych jako wielbiciel luksusowych samochodów (astonów martinów, lamborghini, porsche i mercedesów). Na portalach społecznościowych chwalił się, że już na studiach stać go było na nową limuzynę BMW 7 i zakup domu. Obu tym hakerom postawiono zarzuty, zagrożone w USA karą po 219,5 roku pozbawienia wolności.

Podsłuch telefoniczny umożliwiają wzajemne związki między przetwarzaniem danych a telekomunikacją oraz przechodzenie na cyfrowy system połączeń telefonicznych. Przestępcy penetrują centrale telefoniczne operatorów, a docierają tam przez zwykle łącza przekazywania danych. Wiadomo, że wszystkie rodzaje telefonów, nadajniki fal radiowych, a także łącza satelitarne niekodowane, są obiektami łatwo do-

357 A. Kublik, *Rosyjscy szpiedzy szperają w Yahoo!*, „Gazeta Wyborcza" z 17 marca 2017 r.

stępnymi, a osoby nieuprawnione posługując się odpowiednim sprzętem zdobywają chronione informacje.

Różnorodne techniki podsłuchu były i są stosowane jako rutynowe działania zarówno przez profesjonalne instytucje państwowe zgodnie z obowiązującymi przepisami, jak i przez osoby czy firmy nieuprawnione. Przykładowo, tajne służby b. NRD stosowały różne techniki podsłuchu w stosunku do polityków, pracowników służb specjalnych i innych urzędników mających dostęp do informacji niejawnych w ramach tajemnicy państwowej w RFN. Podsłuchiwane rozmowy były automatycznie nagrywane i analizowane. Aktualnie służby specjalne wszystkich krajów posługują się podobnymi metodami.

Według opublikowanych danych amerykańskiej Służby Bezpieczeństwa Narodowego (NSA), na przełomie XX i XXI wieku obsługiwała ona m. in. ponad 2000 urządzeń podsłuchu telefonicznego, które umożliwiały jednoczesną rejestrację ponad 54.000 rozmów w różnych regionach świata. Dane na temat liczby urządzeń prowadzących podgląd i podsłuch satelitarny nie są publikowane, jednakże nie ulega wątpliwości, że jeśli wszystkie są monitorowane, to rejestruje się miliony takich rozmów.

## 6.7. Informacje niejawne z podsłuchu jako gra wywiadów

Media w interesujący sposób informują o podsłuchiwaniu obcych placówek dyplomatycznych w wielu krajach świata. Przykładowo, drugi sekretarz ambasady rosyjskiej w Waszyngtonie, Stanisław Gusiew, rozpoznany jako oficera wywiadu wyspecjalizowany w obsłudze urządzeń podsłuchowych, długo nie był podejrzewany przez Federalne Biuro Śledcze, choć od ponad roku regularnie spacerował wokół Departamentu Stanu i parkował swój samochód w pobliżu budynku. FBI dopiero po roku odkryło, iż Rosjanin podsłuchuje toczące się w Departamencie Stanu rozmowy za pomocą zdalnie sterowanej „pluskwy". Zaskoczenie było jeszcze większe, gdy okazało się, że owa „pluskwa" zainstalowana została w pokoju konferencyjnym na najpilniej strzeżonym siódmym piętrze, gdzie mieści się gabinet sekretarz stanu i jej zastępców[358].

Wprawdzie S. Gusiewa wydalono z USA, ale najważniejsze pytania nadal pozostają bez odpowiedzi: kto i kiedy zainstalował podsłuch w jednym z obiektów o kluczowym znaczeniu dla bezpieczeństwa Stanów Zjednoczonych oraz dlaczego instalację podsłuchu rozpoznano dopiero po roku?

Podczas szczytu G20 w Sankt Petersburgu 5-6 września 2013 r. Rosjanie wręczyli swoim gościom ukryte w upominkach urządzenia szpiegowskie. Takie rewelacje przynosi największy wioski dziennik „Coriere della Sera". Uwiarygodnia je fakt, że zostały zdementowane wyłącznie przez Rosję, a rzekome ofiary pułapki rosyjskiego wywiadu – głowy najważniejszych państw świata i ich rządy, także przewodniczący Rady Europejskiej Herman Van Rompuy – odmawiają jakichkolwiek komentarzy. Dziennik poświęcił sprawie obszerny tekst na dwie strony pt. „Tak Putin chciał szpiegować Europę". Wynika z niego, że podczas pełnego napięcia szczytu G20 poświęconego przede wszystkim kwestii ewentualnej interwencji w Syrii, uczestnicy, około 300 osób, zgodnie z tradycją otrzymali szereg upominków. Były to: pluszowe misie, filiżanki, notesy, nieprzemakalne kurtki z logo zimowych igrzysk w Soczi, ale też pendrive'y USB (8 giga, Made in China) i kabelki do ładowania telefonów ko-

358 K. Darewicz, *Agenci kosztują*, „Rzeczpospolita" z 21 grudnia.1999 r.

mórkowych. Van Rompuy i jego unijna delegacja, jak zwykle po powrocie z ważnych spotkań za granicą, poddani zostali procedurze „debriefingu" przez brukselskich speców, od kontrwywiadu. Pendrive'y i kabelki wzbudziły podejrzenia, więc przekazano je do analizy niemieckim służbom. Te wykryły, że oba gadżety wyposażone zostały dodatkowo w urządzenia i oprogramowanie, które przekazują informacje zawarte w komputerach i telefonach[359].

Były pracownik Agencji Bezpieczeństwa Narodowego Edward Snowden[360] ujawnił, że NSA inwigiluje Internet niemal wszędzie na świecie. Prawdziwa burza wybuchła jednak bynajmniej nie wtedy, gdy się okazało, że amerykańska agencja dokonała 70 mln zapisów rozmów telefonicznych Francuzów, a okazało się, że podsłuchiwano również Hiszpanów. Europejskich polityków rozsierdziła wiadomość, że oni także są ofiarami szpiegowskiego skandalu. Agencja miała monitorować rozmowy 35 przywódców, m.in. kanclerz Niemiec i premiera Hiszpanii.

Podczas gdy media na świecie spekulują, czy Barack Obama o tym wiedział, a z kolejnych europejskich stolic słychać głosy, że podsłuchiwanie sojuszników jest „niedopuszczalne", szef amerykańskich służb wywiadowczych James Clapper powtarza w wywiadach: „Robimy to samo co wszystkie państwa". I nie chodzi wyłącznie o państwa sobie wrogie[361]. Odpowiedzią na ujawniony w 2013 r. podsłuch Angeli Merkel i Hollande'a ma być zaostrzenie ochrony danych osobowych w Unii. To jednak z pewnością nie ograniczy działań wywiadu USA.

Brytyjskie media ujawniły dokument kontrwywiadu, w którym oceniano, że na terenie Wielkiej Brytanii działają agenci 20 służb, w tym m.in. francuskich i niemieckich. W 2013 roku w oprogramowaniu komputerowym Pałacu Elizejskiego znaleziono „tylne drzwi" świadczące o tym, że ktoś nieupoważniony regularnie penetrował system używany przez francuskiego prezydenta. Podejrzenia padły na NSA, ale Waszyngton stanowczo zaprzeczył, a wyniki dochodzenia utajniono.

W wielu dużych firmach trwa nieustannie – na całym świecie – rekrutacja na stanowiska *collection managers*. C*ollection manager* to osoba z najwyższych warstw wywiadu, która nie tylko pracuje i pozyskuje informacje wywiadowcze, ale też decyduje, co jest ważne i jakich środków użyć oraz w jaki sposób je należy wykorzystać. Ponadto, decyduje o kierunkach działań wywiadu i zarządza operacjami szpiegowskim. Praktycznie ma również status pracownika rządowego. Nie może jedynie wydawać publicznych pieniędzy i zatwierdzać wydatków ani zatrudniać lub zwalniać pracowników rządowych[362].

Jeśli wierzyć dokumentom ujawnionym przez Snowdena, skala szpiegowania jest bezprecedensowa, tym bardziej, że mało wiadomo o podobnych programach innych

359 P. Kowalczuk, *Rosjanie podsłuchują przywódców,* „Rzeczpospolita" z 31.10- 1.11.2013 r.

360 Ciekawostką jest fakt, że Edward Snowden nie został przyjęty do służby w ABN na stanowisko szpiega. Jest komputerowym samoukiem, który nie skończył nawet szkoły średniej. Jego pierwsza praca w wywiadzie była czynnością ochroniarza w jednej z placówek NSA. W wywiadzie dla „Guardiana" Snowden powiedział, że potem został zatrudniony przez CIA z powodu swych umiejętności komputerowych i miał czuwać nad bezpieczeństwem sieci. W 2009 roku przeszedł do sektora prywatnego. Praca, którą wykonywał jako wynajęty pracownik dla NSA, polegała na pomocy technicznej i rozwiązywaniu bieżących problemów IT.

361 A.Kaźmierska, *Etyka szpiegowania, „*Rzeczpospolita" z 29.10. 2013

362 D. Bennet, M. Riley, *Szpieg, który zarabiał. Jak amerykańska firma consultingowa zmieniła się w najbardziej zyskowną organizację wywiadowczą świata,* „Bloomberg Businessweek" z 24-30 czerwca 2013.

państw. Działający od 1995 r. rosyjski SORM służy do monitorowania komunikacji internetowej i telefonicznej teoretycznie tylko w Rosji, ale zakres działania systemu nie jest znany. Wątpliwości potwierdza fakt ujawnienia istnienia chińskiej wojskowej jednostki 61398, która wedle ekspertów jest prawdopodobnie „jednym z największych na świecie oddziałów zajmujących się szpiegostwem w sieci". Przypisuje się jej kradzież tysięcy terabajtów danych z koncernów i systemów państwowych na całym świecie. Natomiast o indyjskim Centralnym Systemie Monitoringu mówi się, że działa podobnie jak PRISM.

Aktualnie politycy europejscy głoszą, że sojusznicy nie powinni wzajemnie podsłuchiwać swych przywódców. Na wniosek Francji i Niemiec należy wynegocjować z Waszyngtonem pakt podobny do tego, jaki USA podpisały z Wielką Brytanią, Australią, Kanadą i Nową Zelandią. Chodzi o tzw. *Five Eyes,* czyli umowę ścisłej współpracy, która w zasadzie polega na tym, że zamiast szpiegować się nawzajem, kraje te wspólnie szpiegują innych. A my oczywiście nie dowiemy się, jakie nowoczesne technologie pozyskały zjednoczone siły w ramach szpiegostwa gospodarczego. Takie informacje utrzymywane są w najgłębszej tajemnicy.

# Rozdział 8

# Organizacja zespołu wywiadu gospodarczego i ochrony kontrwywiadowczej w przedsiębiorstwie

## 1. Opracowanie koncepcji pracy zespołu

Podstawowym zadaniem wywiadu i kontrwywiadu gospodarczego jest możliwość dysponowania takimi instrumentami wynikającymi z posiadanej wiedzy, które przydatne będą lub istotnie mogą wpływać na system usprawniania i zarządzania przedsiębiorstwem, a stosowanie których jest zgodne z przepisami obowiązującego prawa.

Współczesne wydarzenia związane z nielegalnymi podsłuchami stosowanymi wobec członków rządu i biznesmenów to ewidentne przykłady, że aktualnie stosowane są wszelkie dostępne narzędzia i metody bez względu na rodzaj planowanego działania czy przeciwdziałania, ich legalność czy nawet zagrożenie karą pozbawienia wolności.

Wiele przedsiębiorstw, nie tylko w czasie kryzysu, ale również w okresie szybkiego rozwoju ekonomicznego staje przed szeregiem pytań i problemów, które mogą wpłynąć na ich dalszy rozwój i rzeczową grę konkurencyjną. Przykładowo, na tak istotne problemy zwraca uwagę prof. Jerzy Konieczny:[363]:

1. co twoje przedsiębiorstwo (organizacja) robi dla zbudowania systemu tworzenia, zdobywania wiedzy o klientach, uzyskiwania nad nimi wpływu celem poprawy sytuacji biznesowych?
2. jakie systemy zostały wdrożone celem zabezpieczenia wiedzy i doświadczenia pracowników opuszczających firmę?
3. czy organizacja nagradza motywowanie pracowników do wzajemnego dzielenia się wiedzą?
4. jakie straty ponosi twoja organizacja z powodu braku dostępności do istniejącej już wiedzy i informacji?
5. czy strategia uczenia się w twojej organizacji jest dostosowana do rodzaju prowadzonej działalności?
6. czy masz okazję do wskazywania kierunków rozwoju wiedzy w twojej organizacji, a także strategicznych kierunków uczenia się w niej?
7. w jaki sposób mierzysz kulturę uczenia się twojej organizacji?

Niejednokrotnie wyniki takiej analizy stają się istotnym przyczynkiem do utworzenia zespołu czy innego rodzaju komórki analitycznej wywiadu gospodarczego. Na-

363 J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu,* wyd. cyt., s. 160.

zwa zespołu jest obojętna. Zdarzają się nazwy, jak: wydział informacji, zespół analiz, sekcja dokumentalna, biuro przygotowań itp.

Współcześnie opracowane procedury ułatwiają utworzenie jednostki wywiadu gospodarczego w organizacji. Wskazują jej potrzeby, zadania i metodykę działania. Podstawą sukcesu w organizowaniu i działaniu jest określenie:

1. potrzeb informacyjnych, które może mieć również postać listy celów informacyjnych przedsiębiorstwa. Zazwyczaj są one uzupełniane przez zarząd, bieżącymi zadaniami informacyjnymi. W tej kwestii J. Konieczny przestrzega przed popadnięciem we „wszystkoizm", który powoduje rozmycie skuteczności. Tylko w określonych warunkach można uprawiać wywiad wszechstronny;
2. typów badanych źródeł, a szczególnie źródeł formalnych, czyli np. wydawnictw i dokumentów, które będą gromadzone. Sprecyzowanie tego zadania należy do specyfiki dokumentalistów;
3. podziału zadań. Niezbędna jest decyzja dotycząca sprecyzowania zadań wykonywanych samodzielnie i zadań zlecanych innym. Korzystanie z wywiadowni gospodarczych znacznie ułatwia pracę. Problemem może być potrzeba wykorzystania specjalisty z określonej dziedziny. W zależności od potrzeb, zarówno naukowiec jak i ekspert w danej dziedzinie nauki bywa zatrudniony na stałe lub doraźnie. Można również zlecić czynności wyspecjalizowanej agencji;
4. metodyki przetwarzania informacji, która obejmuje przede wszystkim analizę gromadzonych materiałów. Ponieważ wciąż brak specjalistów w tej dziedzinie można podjąć przygotowanie (szkolenie) własnych analityków wywiadu gospodarczego i informacji z tym związanych;
5. procedury wykorzystywania informacji, która ściśle wiąże się z określeniem: kompetencji do wyznaczania zadań, wydaniem wewnętrznych przepisów dotyczących tajemnic przedsiębiorstwa związanych z funkcjonowaniem zespołu wywiadu, instrukcji obiegu dokumentów w zakresie obiegu dokumentów kierownictwo – wywiad, organizację briefingów, a także dostępu do kierownictwa w przypadku sytuacji nadzwyczajnej, jaka może mieć miejsce w przypadku pojawienia się informacji szczególnej itp.;
6. roli wywiadowców „spontanicznych". Każdy pracownik powinien mieć przynajmniej podstawową orientację w zakresie zasad działania w przypadku ewentualnego uzyskania ważnej informacji. Zachowania ważne dla przedsiębiorstwa powinny być nagradzane, a wiedzę a ten temat pracownicy powinni uzyskiwać na specjalnych szkoleniach wewnętrznych.

Pomysł zmian w przedsiębiorstwie może napotkać na mniej lub bardziej sprzyjający klimat. Największe niebezpieczeństwo dla powodzenia nowego przedsięwzięcia kryje się w posiadaniu i wykorzystaniu zasobów informacyjnych, jako poważnych środków, które mogą być w dyspozycji nowej komórki. Zatem każde przedsiębiorstwo decydujące się na założenie komórki wywiadu gospodarczego musi rozstrzygnąć, jaki dział będzie najlepiej przystosowany do podjęcia takich zadań. Wyboru dokonuje się najczęściej między działami marketingu a badań i rozwoju.

Przedsiębiorstwo posiadając określoną specyfikę, ma również wynikające z niej potrzeby dotyczące własnej organizacji. Zatem przedsiębiorstwo o działalności ściśle

technologicznej, będzie skłaniać się ku koncepcji oparcia komórki wywiadu gospodarczego na swoich inżynierach, zajmujących się profesjonalnie tą działalnością, natomiast w każdym innym przypadku, zarządzanie komórką wywiadu należeć będzie do pracowników działu marketingu.

Oparcie się na dziale marketingu ma w tej sytuacji szereg istotnych atutów, do których należą:

a) otwarcie na otoczenie przedsiębiorstwa, zwłaszcza jeśli idzie o klientów i konkurentów,

b) doskonała znajomość produktów, wynikająca ze ścisłego powiązania z ich powstaniem i rozwojem,

c) znajomość i opanowanie narzędzi, zwłaszcza związanych z badaniem rynku, co może mieć szczególne zastosowanie w wykorzystaniu i przetwarzaniu danych,

d) szerokie kontakty wewnątrz organizacji przedsiębiorstwa z najważniejszymi działami, które zostaną wciągnięte w proces wdrażania wywiadu gospodarczego, poczynając od działu badań i rozwoju, poprzez dział sprzedaży, aż po dział promocji i reklamy[364].

Dokonując szerszej analizy można dojść do wniosku, że korzystniej będzie utworzyć niezależną komórkę bezpośrednio powiązaną z zarządem przedsiębiorstwa, w której decydującą rolę odgrywać będzie specjalista do spraw wywiadu gospodarczego w formie mediatora.

Należy mieć na uwadze również realny stopień bezpieczeństwa przedsiębiorstwa, aktualne możliwości i oferty rynku, z których warto skorzystać w określonych sytuacjach biznesowych, czy np. w razie potrzeby uniknięcia zagrożeń. Przykładowo, w związku ze wzrastającą aktualnie przestępczością gospodarczą, a szczególnie z oszustwami finansowymi i nieuczciwą konkurencją czy szpiegostwem gospodarczym, uwidacznia się narastający zakres zapytań o aktualnych, a także potencjalnych konkurentach biznesowych, które kierowane są do profesjonalnych firm wywiadu gospodarczego. Nieliczne działające na polskim rynku tego typu przedsiębiorstwa oferują szeroki zakres usług. Są to działania w zakresie badań wykonywanych przez profesjonalny wywiad i kontrwywiad gospodarczy, a szczególnie:

- długoterminowe czynności ukierunkowane na badanie konkretnego obszaru rynku,
- śledzenie działalności przedsiębiorstw konkurencyjnych,
- ocena ryzyka inwestycyjnego.

W ramach czynności wywiadowczych kierowane zapytania dotyczą wykonywania takich przedsięwzięć jak: monitorowanie udziału w przetargach, ustalanie listy kontrahentów, zbieranie danych o kluczowych pracownikach, czy identyfikacja partnerów strategicznych.

Wspomniane firmy prowadzą profesjonalne wywiady środowiskowe, badają powiązania kapitałowe, dokonują oceny stanu majątkowego. Ponadto, badają i weryfikują naruszenia prawa i powiązania ze światem przestępczym, sprawdzają stan majątkowy dłużników, a także dokonują oceny wiarygodności kontrahentów. W uzasadnionych przypadkach prowadzą śledztwa gospodarcze.

364 M. Kwieciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa-Kraków 1999., s. 83-85.

Niektóre z tych firm posiadają możliwość prowadzenia swojej działalności na całym świecie. Przykładowo, wywiad gospodarczy prowadzony przez firmę Profesjonalny Wywiad Gospodarczy Skarbiec, to m.in.:

- ocena strategii walki konkurencyjnej,
- dyskretna weryfikacja kontrahentów,
- identyfikacja i ocena zagrożeń dla planowanych inwestycji,
- śledztwa gospodarcze,
- procedury *due diligence*[365].

Wspomniana firma dokonuje analizy przepływów finansowych, bada dokumentację księgową transakcji i zapisy księgowe, analizuje listę kontrahentów, a także łańcuchy dostaw. Ponadto, dokonuje wieloaspektowej weryfikacji osób zatrudnionych. Specjalizacją kontrwywiadowczą tej firmy jest przede wszystkim:

- identyfikacja działań konkurencji,
- przeciwdziałanie i zwalczanie szpiegostwa gospodarczego,
- informatyka i księgowość śledcza,
- ochrona własności intelektualnej i marki
- raport o firmie czy osobie weryfikowanej[366].

## 2. Opracowanie tematyki szkolenia pt. Podstawowe zasady działania wywiadu i kontrwywiadu gospodarczego w interesie bezpieczeństwa przedsiębiorstwa

Działania wywiadu i kontrwywiadu gospodarczego spełniają niezwykle ważną rolę w bezpieczeństwie przedsiębiorstwa i jego rozwoju. Towarzyszy mu rozwój społeczeństwa informacyjnego i proces związany z postępem techniki teleinformatycznej. Wiąże się to również z narastającym systematycznie zapotrzebowanie na specjalistyczne usługi informacyjne, a w tym o charakterze wywiadowczym i kontrwywiadowczym.

Swoisty rozwój inteligencji cyberprzestrzeni, obszarów wirtualnych i cyfrowych dotyczy nie tylko uprawnionych przedsiębiorstw i służb. Dotyczy to wszystkich sektorów gospodarki. Tym złożonym procesom towarzyszy stała o charakterze lawinowym rewolucja elektroniczna. Rozwój komputeryzacji wiąże się ze zmianą środków i metod pozyskiwania informacji, co pociąga za sobą potrzebę zmiany metod pracy.

Działalność wywiadowcza i kontrwywiadowcza to wiele wzajemnie powiązanych, współzależnych i uzupełniających się przedsięwzięć, które można określić jako cykle wywiadowcze lub cykle kontrwywiadowcze[367]. Teoretycznie można wspomniane cykle porównywać z wywiadem i kontrwywiadem gospodarczym.

Cykl wywiadowczy służby państwowej obejmuje wszystkie fazy działalności służby wywiadu, od planowania poczynając, na dystrybucji gotowego materiału wy-

365 Szerzej patrz rozdział 7 p. 6.4.

366 Profesjonalny Wywiad Gospodarczy Skarbiec https://www.wywiad-gospodarczy.pl/kontrwywiad-gospodarczy.html(30.XI.2017).

367 Por.: A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 248.

wiadowczego kończąc. Dzielony jest zazwyczaj na pięć etapów, na które składać się powinny adekwatne działania wywiadu i kontrwywiadu gospodarczego:

1. planowanie i ukierunkowanie pracy operacyjnej wywiadu, sposobów zdobycia informacji oraz kontrola efektywności działania jednostek zajmujących się jej gromadzeniem,
2. gromadzenie, proces zdobywania informacji i przekazywania ich do dalszej obróbki,
3. przetwarzanie, proces porządkowania i ujednolicenia uzyskanych informacji czy ujednolicenie formatu danych teleinformatycznych,
4. wytwarzanie, proces przekształcania informacji przetworzonej w gotowe dane wywiadu, obejmujący analizę, ocenę i interpretację,
5. przekazywanie, dystrybucja danych wywiadowczych dla uprawnionych użytkowników[368].

Natomiast cykl kontrwywiadu państwowego, to zespół czynności właściwych dla zespołu kontrwywiadu, który może składać się z następujących etapów przydatnych dla kontrwywiadu gospodarczego, a mianowicie:

1. planowanie i ukierunkowanie działań na podstawie istniejących zagrożeń dla przedsiębiorstwa w powiązaniu ze sposobami zdobywania informacji oraz kontrolą efektywności,
2. rozpoznawanie, gromadzenie oraz poszukiwanie sygnałów dotyczących zagrożeń dla bezpieczeństwa przedsiębiorstwa i przekazywanie ich do dalszych kompetentnych analiz,
3. przetwarzanie, weryfikacja zdobytych informacji i materiałów, które potwierdzają istniejące zagrożenia, analiza, ocena i interpretacja,
4. wszczęcie postępowania analitycznego, dalszy sposób postępowania przy zastosowaniu odpowiednich, w zależności od potrzeb metod i środków, ze szczególnym uwzględnieniem gromadzenia informacji o zdarzeniu, osobie lub grupie osób,
5. przekazywanie, dystrybucja danych kontr wywiadowczych dla uprawnionych użytkowników (na przykład członka zarządu przedsiębiorstwa ds. bezpieczeństwa)[369].

Analiza treści uzyskanych informacji powinna pozwolić na ich weryfikację oraz wnioskowanie, a mianowicie:

1. czy uzyskana informacja, na podstawie dotychczasowych ustaleń jest prawdopodobna?
2. czy informacja została skonfrontowana i porównana z informacjami uzyskanymi z innych źródeł?
3. czy treść informacji zgadza się z posiadanymi danymi, a szczególnie z tymi, które uznano za autentyczne. Jeżeli informacja przedstawia dane odmienne od danych uzyskanych z innych źródeł, pozostaje właściwym sposobem wyjaśnić, która z tych informacji jest prawdziwa[370].

368 Por. N. Polmar, T. B. Allen, *Księga szpiegów. Encyklopedia*, Warszawa 2000, s. 137.
369 Por. tamże.
370 Por.: A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 253.

## 3. Koncepcja wykorzystania wywiadu gospodarczego w przedsiębiorstwie – przygotowanie projektu analizy praktycznej

Omawiając koncepcje wykorzystania wywiadu gospodarczego dla potrzeb praktyki i efektywnego rozwoju przedsiębiorstwa należy uwzględnić wyniki profesjonalnych analiz M. Kwiecińskiego. Autor sprawnie określa bogactwo produktów wewnętrznych, wynikających z realizowanych różnorodnych konstruktywnych funkcji wywiadu gospodarczego. Zalicza się do nich zagadnienia, które:

a) umożliwiają podejmowanie decyzji w oparciu o przeanalizowaną informację,

b) stanowią narzędzie wczesnego ostrzegania przed zagrożeniami,

c) są środkiem dostarczania wiarygodnych i rzetelnych ocen,

d) są sposobem poprawy pozycji konkurencyjnej,

e) są swoistą procedurą,

f) stanowią integralną część struktury najlepszych przedsiębiorstw,

g) są wyjątkowym narzędziem umożliwiającym perspektywiczne myślenie,

h) stanowią narzędzie wspomagające taktyczne i strategiczne działania[371].

Ten sam autor rozpoznał i określił dwa zasadnicze nurty wywiadu gospodarczego**,** a mianowicie:

1. jako narzędzie wsparcia w strategicznym wymiarze działalności przedsiębiorstwa, poczynając od tworzenia bazdanych o konkurentach, poprzez analizę sektora i konkurentów, aż po budowę podstaw do wypracowania decyzji strategicznych;
2. jako narzędzie wczesnego ostrzegania.

Rozpatrując istotę wywiadu gospodarczego z perspektywy nurtu pierwszego należy przyjąć, że głównym celem przedsiębiorstwa jest zdobycie i utrzymanie przewagi konkurencyjnej. Takie ujęcie sytuuje sam wywiad, jako najistotniejszy fragment w całokształcie działalności przedsiębiorstwa, który obejmuje trzy główne nurty, a mianowicie:

- wywiad marketingowy,
- wywiad konkurencyjny,
- wywiad technologiczny.

Ujęcie powyższe czyni wywiad gospodarczy koncepcją o walorach strategicznych, co powinno w konsekwencji uzasadniać umieszczeniem menedżera wywiadu gospodarczego w strukturze zarządu.

Gromadząc i analizując bogactwo różnorodnych informacji z otoczenia, czyni także wywiad gospodarczy wiodącym środkiem prowadzącym do identyfikacji i opisu zagrożeń według nurtu drugiego. Ryzyko gospodarcze wpisane jest w naturę działań przedsiębiorstwa, a wywołane jest zmianami strukturalnymi. Powodują one powstawanie różnorodnych zagrożeń, których identyfikacja może zostać wpisana w obszar aktywnych działań wywiadu gospodarczego.

371 M. Kwieciński, *Wywiad gospodarczy jako meta koncepcja zarządzania przedsiębiorstwem* w: J. Kaczmarek, M. Kwieciński (red.) *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 255.

Zawsze istotne jest spojrzenie na zagadnienie pożytków, jakie może przynieść wywiad gospodarczy. Zależy to od jego umiejscowienia w koncepcji strategii przedsiębiorstwa, jako narzędzia monitorowania zagrożeń.

Rozpoznawcza rola wywiadu gospodarczego daje istotną możliwość reagowania na symptomy zbliżającego się kryzysu. Niejednokrotnie może to mieć miejsce z dużym wyprzedzeniem w ramach rozpoznanych zagrożeń na podstawie systemu wczesnego ostrzegania.

Określając obszary informacyjnej filtracji Competitive Intelligence M. Kwieciński zwraca uwagę na potrzebę doskonalenia narzędzi penetracji otoczenia wśród konkurencji, elementów kształtowania struktur, a także na potrzebę szczegółowych charakterystyk osobowych oraz analizyzachowań osób sprawujących kierownicze funkcje w firmach konkurencyjnych.

Niezwykle interesująca jest propozycja dotycząca obszaru możliwych rozstrzygnięć analitycznych, które przedstawiono w poniższej tabeli. Autor zastrzega, że propozycje te nie wyczerpują wszystkich uwarunkowań i okoliczności „personalnego" tworzenia faktów i wiedzy o motywach i efektach działań firmy konkurenta, jednakże trafnie podkreśla wagę tak istotnych czynników psychologicznych, jak: emocje, animozje, zażyłości, uprzedzenia osobiste i sympatie oraz system ideałów i wartości. Warto dodać, że wszystkie te czynniki, a niejednokrotnie również inne, bardziej radykalne mogą zaistnieć, gdy dochodzi do ostrej rywalizacji o klienta. Niezbędna jest wówczas obszerna wiedza o kliencie aby stworzyć szerokie możliwości strategii działania jako podstawy ekspansji i filozofii przedsięwzięć wobec klienta.

**Tabela. Osobowy kontekst analizy konkurencji prowadzonej w ramach wywiadu gospodarczego**

| Lp. | Obszar analiz | Oczekiwany wynik badań | Kontekst osobowy (who?) |
|---|---|---|---|
| 1. | Benchmarking | uczenie się od konkurencji, zmiany w podejściu do oceny biznesu prowadzonego przez konkurencję | liderzy konstruowania przepływu i wiedzy, główni analitycy i stratedzy |
| 2. | Badanie sieci łańcucha wartości | poznanie dostawców czynników produkcji, kanałów dystrybucji, efektywnych kosztów produkcji, wpływu na zysk brutto, efektywność strategii dystrybucji | personalne i osobiste, oparte na emocjach, motywy decyzji wyboru dostawców, kanałów dystrybucji – kapitał relacyjny |
| 3. | Internet | zmiany na stronach WWW konkurenta, efektywność marketingu prowadzonego przez Internet, wykorzystanie przez konkurenta Internetu dla monitorowania danej branży, wpływ stron WWW na aktywizację sprzedaży konkurenta | liderzy aktywności na stronach WWW oraz potencjał ich możliwości |
| 4. | Finanse | przemiany w stanie finansów, wpływ na siłę finansową konkurencji, zmiana ceny akcji/wartości rynkowej firmy konkurenta, stopa zwrotu z zaangażowanego kapitału konkurenta | ocena zmian personalnych w składzie top managementu przez analityków rynków finansowych |

| | | | |
|---|---|---|---|
| 5. | Wyznaczanie cen | zmiany cen hurtowych, zmiany cen detalicznych, polityka marż, wpływ na sprzedaż cen konkurenta, stosowane metody dyskontowania, zmiany w zyskach brutto, efektywność przyjętych strategii cenowych | liderzy zmian w polityce cen i marż, ich osobiste motywy, kompetencje, doświadczenia |
| 6. | Promocja | wizerunek marki, program prezentacji, program PR, program marketingu detalicznego, zmiany w strategii promocji, upowszechnianie wizerunku poprzez wycinanie i wysyłanie do klienta artykułów z gazet, w których mowa o firmie *(Media Clipping)*, efektywność reklamy dla grupy celowej, wpływ reklamy konkurenta na sprzedaż | „mózgi" polityki promocji w wydaniu konceptualnym i narzędziowym |
| 7 | Produkty/usługi | wprowadzenie nowych produktów/usług, informacje przesyłane w prospektach (broszurach), oczekiwania od produktów/usług konkurenta, stosowane technologie produkcji, a także możliwości wprowadzania nowości przez pion B&R, numer linii produktu/usługi, asortyment (różnorodność), koszty produkcji/dostawy konkurenta, poziom wartości dodanej, zmiany w jakości | skład osobowy pionu B&R, kompetencje, doświadczenia technologów, zdolność do tworzenia trudnych do naśladowania koncepcji produktów, wszelkie negatywne emocje, konflikty np. na tle prestiżu wśród zespołu twórców |
| 8. | Sprzedaż | wielkość miesięcznej sprzedaży, całokształt potencjału rynkowego dla różnorodnych produktów/usług, wielkość portfela zamówień, nowe rynki zbytu, zmiany w produktach/usługach konkurencji, zmiany w obsłudze posprzedażnej, budżet promocji rynkowej konkurenta, częstotliwość kontaktów z klientami, porównanie wielkości sprzedaży, ranking przedstawicieli (agentów) handlowych, wpływ obsługi klienta na wielkość sprzedaży, prognoza sprzedaży konkurentów | ranking przedstawicieli (agentów) handlowych, ich krąg znajomości, przebieg kariery, odnotowane i potencjalne animozje i niechęci w rywalizacji w zespole sprzedawców |
| 9. | Badania | efektywność poznania preferencji klienta względem produktu/usługi, kontakty konkurenta z firmami i osobami trzecimi, poziom ufności konkurenta we własne badania rynku | motywy i efekty zażyłości z klientami odnotowane wśród menedżerów firmy konkurenta |

| | | | |
|---|---|---|---|
| 10 | Strategia marketingowa | zamiary fuzji (połączeń) konkurenta, plany wdrożenia patentów, efektywność strategii marketingowych, zmiany w strategiach marketingowych, wpływ wdrożenia nowej strategii marketingowej na sprzedaż | osobiste motywy zamiarów fuzji i aliansów |
| 11. | Personel | aktywność rekrutowania pracowników przez konkurenta, liczba zwolnień (odejść) pracowników, schemat organizacyjny firmy konkurenta, informacje o doświadczeniach zawodowych personelu zarządzającego firmą konkurenta | osobiste motywy odejść (zwolnień) personelu, wybitni menedżerowie i twórcy mózgi firmy konkurencyjnej |
| 12. | Klienci | Częstotliwość zmiany upodobań wśród klientów dokonujących zakupu produktów/usług konkurenta, opinie klientów o produkcie/usłudze, poziom lojalności klientów wobec firmy konkurenta | czołówka opiniotwórcza klientów firmy, podstawy emocjonalne kształtowania opinii o produktach i firmie |

Źródło: M. Kwieciński, *Wywiad gospodarczy jako meta koncepcja zarządzania przedsiębiorstwem*w: J. Kaczmarek, M. Kwieciński (red.) *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 259-261.

W powyższej tabeli dostrzegamy niezwykle szeroki zakres działalności konkurencyjnego przedsiębiorstwa, o której zgromadzono olbrzymi kapitał wiedzy. Autor trafnie określa, że może to pozwolić na uruchomienie znacznych możliwości subtelnych działań, podejmowanych z korzyścią dla beneficjenta przetworzonych informacji, a zatem firmy organizującej skomplikowany aparat narzędziowy, program i strukturę wywiadu gospodarczego[372].

Można przyjąć, że jest to wzorcowy model praktycznego działania, jednakże powinien on być dostosowany do potrzeb określonego przedsiębiorstwa.

Jednym z kolejnych zagadnień jest budowa systemu wczesnego ostrzegania zagrożeń, która powinna obejmować:

3. sporządzanie mapy obszarów wysokiego ryzyka,
4. budowę systemu wskaźników ostrzegawczych,
5. monitorowanie wskaźników,
6. uruchamianie alarmów[373].

Należy wyrazić przekonanie, że system wczesnego ostrzegania zarówno w zarządzaniu firmą, jak i w jej bezpieczeństwie np.: transakcyjnym, finansowym, ekonomicznym czy elektronicznym, a także w ochronie mienia – odgrywa podstawowe znaczenie.

372 Tamże, s. 261.

373 M. Ciecierski, *Wywiad gospodarczy w walce konkurencyjnej przedsiębiorstw*, Warszawa 2007, s. 58.

## 4. Opracowanie koncepcji współpracy zespołu wywiadu gospodarczego z innymi działami na rzecz wsparcia klientów oraz polityki wobec konkurentów

Praktycy, w personelu merytorycznym zespołu wywiadu gospodarczego wyróżniają trzy grupy pracowników, są to mianowicie:

1. dokumentaliści – osoby kompetentne w zakresie obsługi zbiorów dokumentacji naukowej, prasowej i innej, umiejący tworzyć i obsługiwać bazy danych, a także bibliotekoznawcy, archiwiści i inni w miarę potrzeb,
2. pracownicy „liniowi"– najczęściej byli funkcjonariusze służb państwowych, mający zwykle liczne kontakty, potrafiący też nawiązać nowe kontakty, budować sieć powiązań i wywierać wpływ na otoczenie, ich podstawowym zadaniem jest wykorzystanie źródeł nieformalnych,
3. analitycy specjaliści w zakresie opracowywania uzyskanych informacji, wyciągania wniosków, budowania prognoz i sugerowanie kierunków działania zespołu[374].

Cenne są wskazówki J. Koniecznego dla menedżerów i wywiadowców-analityków informacji, na temat taktyki obchodzenia się z informacją uzyskaną dla potrzeb przedsiębiorstwa, a mianowicie:

1. *znaj przedmiot twojego działania. Im więcej wiesz o dziedzinie, w której się poruszasz, tym mniejsze prawdopodobieństwo wprowadzenia cię w błąd,*
2. *ustal najlepsze źródła informacji, którymi się zajmujesz, Zidentyfikuj najlepsze bazy danych, specjalistyczne czasopisma i autorów, piszących o twojej branży. Jednym z największych problemów epoki Internetu jest: komu wierzyć?*
3. *rozmawiaj z ekspertami. Gdy dowiesz się o czymś nowym, traktuj to jako wskazówkę, a nie odkrycie. Przedyskutuj rzecz ze znawcami tematu,*
4. *jeśli to możliwe, korzystaj z więcej niż jednego źródła, porównuj dane,*
5. *jeśli masz pytania na temat dostarczonego materiału, wezwij dostawcę informacji. Spytaj o źródła i metody zebrania informacji. Czy jesteś usatysfakcjonowany odpowiedzią?*
6. *rozmowa z autorem materiału jest zawsze pożyteczna. Na ogół pisze się znacznie mniej niż się wie lub domyśla, w rozmowie bezpośredniej można wyjaśnić lub przybliżyć wiele spraw,*
7. *pamiętaj, że budowanie prognoz polega na zgadywaniu,*
8. *zawsze sprawdzaj przypisy, jednostki pomiaru lub zliczenia, odnośniki itp. Czasem im mniejsza czcionka tym ważniejsza wydrukowana nią treść,*
9. *czytając studia lub analizy zbadaj ich cel lub sponsora. Cel publikacji może być polityczny, ideologiczny lub podporządkowany innym dalekim od obiektywizmu celom,*
10. *dawaj pierwszeństwo źródłom pierwotnym przed źródłami z drugiej (lub dalszej) ręki,*
11. *spróbuj opanować metodykę i metodologię badań w interesującej nas dziedzinie,*

374 J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu,* wyd. cyt. s.161, 162

*12. myśl krytycznie! Uzyskuj potwierdzenia, zadawaj pytania, wykorzystuj intuicję itd. Jeśli coś nie brzmi dobrze sprawdzaj dalej*[375].

Wszystkie powyższe zalecenia i uwagi mają znakomite znaczenie w realizacji złożonych zadań z uwagi na ich walory praktyczne, gdyż zostały zweryfikowane w prowadzonych badaniach w ramach przedsięwzięć wywiadu gospodarczego.

## 5. Inicjowanie projektów badania rynku lub klienta biznesowego

Wprowadzenie gospodarki konkurencyjnej w Polsce ożywiło rynek, umożliwiło nowe spojrzenie ekonomiczne i gospodarcze, a także spowodowało wzrost zainteresowania podstawowymi badaniami rynku. Zyskały na znaczeniu wyniki tych badań szczególnie wówczas, gdy występowały problemy zagrażające firmie, a przykładowo: spada sprzedaż, udaje się podtrzymać sprzedaż tylko dzięki obniżce cen, starzeje się asortyment towarów firmy, nowa technologia wywiera wpływ na rynek. Co z tego wynika dla firmy w przyszłości? Jednym z wniosków może być poszukiwanie skutecznych metod badawczych kandydatów na kontrahentów.

Aktywny przedsiębiorca zajmie się zapewne prostymi działaniami, które leżą w jego możliwościach lub uzyska proste wsparcie dla przeprowadzenia badań wstępnych. Nawet proste metody badawcze i ich wyniki mogą być pomocne w ustaleniu celów działalności firmy, rozwiązywaniu niektórych problemów gospodarczych i kierowaniu rozwojem firmy, gdy postawiono zagadnienia badawcze, jak np.:

1. ustalenie celów badania, które ułatwiąoszacowanie wielkości rynku i sprecyzowanie kierunków rozwoju przedsiębiorstwa, a także wykorzystanie do określenia wielkości potencjalnych klientów oraz ułożenie planu sprzedaży;
2. rozwiązywanie problemów jako narzędzie analizy w celu ujawnienia przyczyn, np. niskich zysków firmy czy utraty udziału w rynku i możliwości jego odzyskania;
3. wspieranie rozwoju firmy oraz uzyskanie odpowiedzi na pytanie, dlaczego klienci wybierają określony produkt i co wpływa na ich wybór. Pozwala to również na ustalenie strategii nasilenia sprzedaży większej ilości produktów, osiągania lepszej ceny i pokonania konkurencji[376].

Cele badań wymienionych problemów powinny być ustalone w powiązaniu z możliwym działaniem lub podejmowaniem decyzji. Jeżeli badamy problem spadku sprzedaży określonego produktu, to musimy sprawdzić hipotezy, z których np. może wynikać, że:

- spadek sprzedaży został spowodowany działaniami konkurencji, która powiększyła swój udział w rynku;
- konkurenci zdobywają rynek, ponieważ ich produkty lepiej zaspokajają potrzeby odbiorców;
- konkurenci zdobywają rynek przy pomocy obniżki cen na swoje towary;
- system dystrybucji firmy nie obejmuje jakiejś części rynku;
- zła opinia o niezawodności produktu firmy wpłynęła na jego pozycję na rynku.

375 Tamże, s. 162.
376 P. N. Hague, P. Jackson, Badania rynku, Kraków 1991, s. 13 – 14.

Badanie rynku jest narzędziem analizy pomocnym przedsiębiorcy w wyjaśnianiu istoty określonych zdarzeń oraz ich przyczyny. Najczęściej w centrum jego zainteresowania pozostają następujące problemy: spadek sprzedaży, niska zyskowność i jej przyczyny oraz występująca niezdolność do zaspokojenia popytu i jej przyczyny.

Powody spadku sprzedaży mogą być wewnętrzne (np. ustalenie zbyt wysokich cen, wysłanie na rynek produktów niskiej jakości lub wadliwych, brak zapasów bądź środków produkcji, brak wsparcia sprzedaży dobrą reklamą). Zewnętrzne powody spadku sprzedaży to: agresywna konkurencja, wzrost liczby konkurentów na rynku, zmniejszenie się rynku wywołane różnymi przyczynami (np. spadkiem zainteresowania określonym produktem, wprowadzeniem nowego produktu o wysokich parametrach jakościowych i nowatorskich). Poznanie zarówno wewnętrznych, jak i zewnętrznych przyczyn spadku sprzedaży daje firmie możliwość przeciwdziałania tej niekorzystnej sytuacji.

Badanie rynku pomaga rozwinąć firmę, gdyż przyczynia się do uzyskania zasobów rynku, ujawnia przyczyny spadku czy wzrostu sprzedaży określonych produktów, jak również informuje o tym, dlaczego klienci kupują i w jaki sposób, a także pozwala poznać metody stosowane przez konkurencję.

Od dawna wiadomo, że właściwe decyzje gospodarcze można podejmować tylko wtedy, gdy dysponujemy rzetelną wiedzą o naszym partnerze biznesowym. Sukces przedsięwzięcia, które podejmujemy, zależy nie tylko od nas. Z tego względu przed sfinalizowaniem umów o współpracy, należy uzyskać wiedzę o partnerze, która pozwoli zminimalizować ryzyko niepowodzenia i uniknąć narażenia naszych interesów.

W kolejnej próbie usystematyzowania tej wiedzy wykorzystano znaną w kryminalistyce regułę tzw. siedmiu „złotych pytań". Racjonalne wykorzystanie odpowiedzi na te pytania w celu uzyskania gotowego wyniku może doprowadzić w konkluzji do celowego zaangażowania się w dalsze przedsięwzięcia mające na celu poprawę istniejącego stanu rzeczy. Może również stanowić przyczynek do dalszych rozważań lub ważny element w dociekaniach nad bezpieczeństwem firmy. Zatem, w zależności od określonych potrzeb warto próbować odpowiedzieć na następujące pytania:

1. KTO? Identyfikacja partnera. Rozpoznanie jego wiarygodności, standingu, pozycji w reprezentowanej dziedzinie, powiązań, kontaktów itp.
2. CO? Sprecyzowanie istoty wzajemnych zainteresowań partnerów biznesowych, zarówno aktualnych, jak i perspektywicznych. Ocena możliwości sprostania – przez obydwie strony – oczekiwaniom w tym zakresie.
3. KIEDY? Analiza całokształtu uwarunkowań czasowych, zarówno w odniesieniu do realizacji konkretnego przedsięwzięcia, jak również możliwych do przewidzenia zmian w otoczeniu zewnętrznym (zmiana przepisów, sezonowość cen, limity, kontyngenty, koncesje itp.).
4. GDZIE? Określenie nie tylko szczegółowych warunków przestrzennych i lokalizacyjnych, związanych z danym przedsięwzięciem, ale również rozpoznanie specyficznych dla kraju naszego partnera uwarunkowań prawnych, zwyczajowych i innych, mogących mieć wpływ na rezultaty przedsięwzięcia.
5. ZA POMOCĄ CZEGO? Wyspecyfikowanie „narzędzi" realizacji przedsięwzięcia: zarówno technicznych – umożliwiających jego fizyczną realizację – jak i finansowych, zapewniających jego powodzenie, oraz analiza ich dostępności i niezawodności.

6. DLACZEGO? Rozpoznanie rzeczywistych i deklarowanych uzasadnień i motywów działania naszego partnera i dokonanego przez niego wyboru.
7. W JAKI SPOSÓB? Przemyślenie i uporządkowanie uzyskanych ustaleń oraz stworzenie na tej podstawie planu działania uwzględniającego ewentualne, wynikające z rozpoznania zagrożenia oraz sposoby ich neutralizacji dla zabezpieczenia własnych interesów[377].

Uzyskanie wyczerpujących odpowiedzi na powyższe pytania, nie jest rzeczą łatwą, ale stanowić może podstawę do wstępnego rozpoznania partnera biznesowego. Nie gwarantuje to jednak przygotowania do pomyślnych negocjacji oraz właściwego przebiegu realizowanego przedsięwzięcia. Uzyskanie takich wstępnych danych może początkującego analityka wyprowadzić na manowce. Badania pozbawione aspektów ekonomicznych doprowadzą jedynie do identyfikacji ewentualnego partnera i jego pozycji w środowisku biznesowym. Zatem najważniejsze (ekonomiczne i konkurencyjne) cele badania zostaną pominięte. Mają jednak aspekt pozytywny. Wskazują bowiem na złożone problemy badawcze i konieczność poszukiwań metodologii przydatnej do konkretnego przypadku.

Wobec braku sprawdzonego zespołu wywiadu i kontrwywiadu gospodarczego w przedsiębiorstwie, optymalnym rozwiązaniem będzie zwrócenie się do profesjonalnej firmy, która mając bogate doświadczenia, zapewni należytą jakość badań i wniosków z opracowanej analizy.

Na zakończenie warto zacytować J.C. Mastermana, autora pracy *Brytyjski system podwójnych agentów,* b. oficera wywiadu, twórcy brytyjskiego systemu podwójnych agentów, który w przeddzień II wojny światowej powiedział: *Nie ma takiej wiadomości, która nie byłaby przydatna wywiadowi.*

## 6. Etyka zawodu wywiadowcy gospodarczego

Analizując zagadnienia motywacji, jakimi kierują się agenci służb specjalnych, policyjnych czy ochronnych, najczęściej badamy ich predyspozycję. Dotyczy to również wywiadowcy gospodarczego.

Na podstawie zbadanego naboru i szkolenia nowo przyjętych funkcjonariuszy w ABW, CBA, Policji i Straży Granicznej – NIK ocenia, że obecny system naboru daje gwarancję wyboru najlepszych kandydatów. Gorzej jest ze szkoleniem funkcjonariuszy. Po dobrze zorganizowanym kursie podstawowym dalszy cykl szkoleniowy jest przypadkowy i niekonsekwentny, a braki w systemie szkoleń specjalistycznych oraz niedoinwestowanie bazy szkoleniowej mogą się odbić na profesjonalizmie funkcjonariuszy[378].

Lakoniczne informacje podają media, których informacje mogą być zachęcające dla kandydatów do służb specjalnych, a przykładowo: „Chcesz zostać polskim Bondem lub analitykiem tajnych służb? Masz szansę, jeśli skończyłeś niedawno prestiżowy kierunek studiów, najlepiej prawo czy stosunki międzynarodowe, znasz dwa języki obce, lubisz ludzi.

Polskich szpiegów szkolą: Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu. ABW poszukuje więc agentów pracujących w Polsce, a AW stara się o kadry,

377 E. Cilecki, *Penetracja rynków zagranicznych. Wywiad gospodarczy*, Warszawa 1997, s. 44.
378 https://www.nik.gov.pl/aktualnosci/nik-o-systemie-naboru-do-policji-i-sluzb-specjalnych.html(6.05.2013)

które wysyła za granicę. Obie instytucje finansuje budżet państwa, a ich działalność objęta jest tajemnicą. Agent wysyłany na zagraniczne misje to najczęściej absolwent elitarnych kierunków studiów, np. prawa, stosunków międzynarodowych, matematyki czy informatyki. Musi znać przynajmniej dwa języki obce. Idealny układ to: język angielski jako pierwszy, a drugi nietypowy, np. rumuński czy chiński. Kandydat nie może być związany z żadną partią"[379].

Podający się za pracownika ABW przedstawia przykładowo motywacje, którymi powinien kierować się kandydat na agenta, jasno sformułowane przez służby amerykańskie. FBI wprowadziła do użytku akronim MICE – skrót od *money, ideology, compromise* i *ego*, czyli: pieniądze, ideologia, infiltracja i ambicje. Jeśli ktoś przyjdzie do służby i powie, że jest patriotą, który chce bronić ojczyzny, a na zarobkach w ogóle mu nie zależy, to obawiam się, że może nie przejść badań psychologicznych – twierdzi ekspert do spraw służb specjalnych i były pracownik UOP Piotr Niemczyk. Dalej podaje dane, jak kadrowiec z ABW, warunki przyjęcia do służby[380].

W literaturze przedmiotu brak jest wyników badań socjopsychologicznych. Zapewne będą wskazywać, że każdy może traktować wskazany problem indywidualnie, czyli nie zawsze chodzi o pieniądze. Niektóre osoby są odpowiednio uzdolnione i bez przeszkolenia mogłyby zostać wywiadowcą czy szpiegiem gospodarczym. Historia wyraźnie wskazuje, że nie każdy agent państwowy, który odniósł małe czy duże sukcesy był szkolony, a wielu z nich było bardzo skutecznych. Przydatne w tym były zapewne wrodzone zdolności połączone z wiedzą dotyczącą określonej branży, na przykład informatyki oraz kontakty, znajomości z osobami dysponującymi odpowiednimi informacjami. Niezbędne są jednak środki, czyli przede wszystkim pieniądze otrzymane od zleceniodawcy. To tylko niektóre narzędzia pozyskania informacji będących w zakresie zainteresowań wywiadowcy i jego zleceniodawców.

Kolejnym zagadnieniem jest sytuacja, w której dostaje się zlecenie z uwagi na miejsce pracy czy pełnione stanowisko. Wydaje się jednak, że zarówno szpiegiem, jak i wywiadowcą czy analitykiem informacji gospodarczych, uzyskującym znakomite efekty, może być jedynie profesjonalista. Wywiadowcą-analitykiem może zostać tylko ten, kto mimo braku odpowiedniego przygotowania i praktyki, posiada dostęp do odpowiednich informacji lub utrzymuje kontakty z osobami zatrudnionymi w przedsiębiorstwie czy instytucji, która jest przedmiotem zainteresowań konkurencji. Rodzaj zatrudnienia (pracownik stały, sezonowy czy na umowę) nie odgrywa roli. Liczy się zasób posiadanych informacji lub odpowiedni dostęp do informacji chronionych, a stanowiących przykładowo tajemnicę przedsiębiorstwa.

Zdarza się, że konkurencja zapewniając lepsze warunki materialne, przejmuje pracownika do swojego przedsiębiorstwa wraz z całym zasobem odpowiednich informacji. Nie każdy przedsiębiorca ma orientację co do zagrożeń, a także sposobu postępowania wówczas, gdy konkurencja przejmuje jego informatyka lub innego pracownika z odpowiednim zasobem cennych informacji będących tajemnicą przedsiębiorstwa.

Najistotniejsze są jednak motywy, które skłaniają do udzielania informacji stanowiących tajemnice organizacji. Indeks motywów może być bardzo zróżnicowany. Nie zawsze są to pieniądze i chęć poprawy warunków materialnych. Inne czynniki to na przykład: żal do pracodawcy, który dość szybko skłania do zwierzeń. Nałogi i zbocze-

379 D. Olszewska http://gazetapraca.pl/gazetapraca/1,91736,4000718.html(6.05.2013)
380 http://festbank.blox.pl/2010/02/Pracuje-w-ABW.html(15.06.2014)

nia seksualne wymagają zdobywania pieniędzy, jak również mogą stać się czynnikami kompromitującymi potencjalnego informatora. Zdarzają się też nieuczciwi dziennikarze, którzy rezygnują z publikacji ujawnionych faktów i sprzedają je wywiadowcy lub przedstawicielowi przedsiębiorstwa, zainteresowanemu pozyskaniem cennej informacji, a przykładowo pragnie zachować kompromitujące informacje w obawie przed utratą reputacji w biznesie.

Podstawowe różnice pomiędzy szpiegiem i wywiadowcą gospodarczym (detektywem) dotyczą legalności ich działań. Zdarza się, że szpieg gospodarczy działa ukierunkowany na zdobycie informacji chronionych, natomiast wywiadowca – analityk działa legalnie, jest nawet oficjalnym pracownikiem komórki analityczno-marketingowej w określonej firmie, która zajmuje się zbieraniem i analizowaniem informacji z zakresu zasad egzystencji konkurencji. Tylko w wyjątkowych przypadkach przedmiotem jego zainteresowań są informacje chronione.

Nigdy jednakże nie ma pełnej gwarancji; młody, zdolny i dynamiczny pracownik, w którego przedsiębiorstwo inwestowało, np. w ramach stypendiów zagranicznych, mimo podpisanej umowy o zachowaniu tajemnic przedsiębiorstwa, bez skrupułów, czyli wbrew zasadom etyki zawodowej, może, niestety, sprzedać poznane tajemnice firmie konkurencyjnej. Przeciętnie w ciągu roku toczy się kilka lub kilkanaście procesów cywilnych i karnych w tego typu sprawach. Inne fakty, które można również zaliczyć do kategorii „braku etyki zawodowej" mieszczą się w granicach ciemnej liczby przestępstw[381].

Porażki wywiadu zawsze są znane, natomiast o sukcesach w zasadzie nigdy się nie wspomina, a jeśli to dopiero po latach.

Niezwykle ważne są predyspozycje osobiste każdego wywiadowcy, jednakże powinien on przejść nie tylko właściwe przeszkolenie, ale również cykl sprawdzający, czy jako kandydat nadaje się do takich przedsięwzięć.

Istnieje powszechne przekonanie, że każdy wywiadowca musi umieć kłamać, grać, oszukiwać, kamuflować, wykorzystywać: określone sytuacje, cudzą psychikę, miłość i zaufanie.

Wywiadowcy – funkcjonariusze wywiadu państwowego są zakonspirowani najczęściej w ambasadach czy firmach handlowych. Niejednokrotnie posiadają immunitet dyplomatyczny, który ma ich uchronić przed zatrzymaniem. Taki wywiadowca nie może dać się zidentyfikować jako szpieg i nie powinien być zatrzymany. A jeśli zostanie zatrzymany na gorącym uczynku, nie może liczyć na litość czy wyrozumiałość, bowiem może być zastrzelony, powieszony, a w najlepszym przypadku uwięziony.

Natomiast zdekonspirowanie wywiadowcy gospodarczego nie grozi skutkami karnoprawnymi, o ile rozpoznany wywiadowca-detektyw nie naruszył przepisów prawa.

Wywiad gospodarczy opiera się również na różnorodnych metodach i technikach. Stosowane są zatem techniki niezwykle wyszukane, ale w wielu stosowanych metodach nie ma nic nieprzeciętnego. Agenci, czy jak kto woli detektywi gospodarczy często przesiadują po prostu na wystawach handlowych, skrupulatnie przeglądają witryny internetowe rywali, a także dokumentację biur patentowych. Analizują podróżnych na lotniskach i pokładach samolotów. Czasem jednak posuwają się dalej: robią zdjęcia

381 Ciemna liczba przestępstw jest związana z badaniem rzeczywistej, a nie statystycznej liczby przestępstw. Stanowi zatem jedno z węzłowych zagadnień kryminologii. Szerzej: J.W. Wójcik, *Kryminologia. Współczesne aspekty*, Warszawa 2014, s. 102-133.

konkurencyjnych fabryk i coraz częściej analizują informacje zawarte w Internecie przy wykorzystaniu nowoczesnego oprogramowania do szybkiego przeszukiwania baz danych, które umożliwia odnalezienie powiązań między strzępami informacji na temat konkurencji.

Celem takich działań firmy wywiadowczej jest zebranie wszelkich ogólnodostępnych faktów na temat danego rynku i obecnych na nim spółek. Dzięki temu można dostrzec rzeczy, których nie widzi konkurencja. Chociaż w korporacjach roi się od byłych agentów np. FBI, CIA, a w Europie służb poszczególnych krajów, istnieje jednak przekonanie, że większość ludzi zajmujących się wywiadem gospodarczym to z reguły księgowi, badacze rynku i absolwenci MBA, a więc osoby mające nieprzeciętne zdolności analityczne, potrafiące szybko zebrać i pogrupować ogromne ilości informacji.

Pod Waszyngtonem istnieje nawet związek branżowy zrzeszający 6,9 tys. detektywów ds. gospodarczych. Szkoły wyższe prowadzą wykłady na temat wywiadu gospodarczego, np. na uniwersytecie stanowym w Missouri studenci z powodzeniem uczą się stosowanej w przemyśle farmaceutycznym techniki, która na podstawie ogólnodostępnych informacji pozwala określić, nad jakimi lekami pracuje konkurencja. Podobne wykłady i specjalizacje wywiadowcy gospodarczego są prowadzone i planowane w kilku polskich wyższych uczelniach.

W wielu krajach uważa się, że najbardziej mrocznym aspektem wywiadu i szpiegostwa gospodarczego jest rola, jaką w całym procederze odgrywają służby specjalne poszczególnych państw. W USA reputację najbardziej agresywnych pod tym względem mają Francuzi, a na posiedzeniu Amerykańskiej Izby Handlowej w Waszyngtonie, dyrektor FBI Louis J. Freeh oświadczył, że Federalne Biuro Śledcze jest na tropie ośmiu państw, które za pomocą korupcji i innych podejrzanych metod wykradają amerykańskie tajemnice handlowe w celu przekazania ich zagranicznym spółkom. Jednakże FBI odmawia ujawnienia, o które kraje chodzi. Natomiast przedstawiciele państw europejskich oskarżyły o takie działania USA, a szczególnie o nadużywanie ogólnoświatowej sieci podsłuchowej do przechwytywania informacji i przekazywania ich spółkom po drugiej stronie Atlantyku. Jednak CIA i inne amerykańskie agencje wywiadowcze zarzekają się, że to nieprawda[382].

Od dawna wiadomo, że zarówno wywiad gospodarczy, jak i szpiegostwo gospodarcze to kwitnący biznes. Media udowadniają, że z Doliny Krzemowej zawsze płyną niezwykle interesujące informacje. Przykładowo, Oracle, drugi co do wielkości (po Microsofcie) producent oprogramowania, wynajął agencję wywiadowczą zlecając jej specjalne zadanie. Miała ona nieoficjalnie kupić przeznaczone na śmietnik dokumenty instytucji współpracujących z firmą Gatesa. Można jednak twierdzić, że jest to najprostsze zadanie dla wywiadowców. Dlaczego zatem podejmują się tego zadania wyspecjalizowane firmy, tym bardziej, że większość detektywów unika terminów wywołujących negatywne skojarzenia, zdecydowanie przedkładając nad „szpiegostwo" bardziej nobliwe określenie „wywiad wśród konkurencji". Jednak – bez względu na nazwę – zwyczaj szpiegowania rywali na trwałe zakorzenił się na rynku.

Mimo iż działalność komórek wywiadowczych w firmach z reguły uchodzi za etyczną, nie ma zgodności co do tego, kiedy i jak często przedsiębiorcy przekraczają granice przyzwoitości. W kręgu znawców panuje opinia, że operacja wertowania prze-

382 N. King, J. Bravin, *Wywiad gospodarczy kwitnie po obu stronach Atlantyku*, „The Wall Sreet Journal Europe", www.gazeta.pl (10 lipca 2000).

znaczonej na śmietnik dokumentacji Microsoftu zlecona przez korporację Oracle to niechlubny wyjątek.

Prawie w każdej dużej amerykańskiej firmie istnieje wyspecjalizowane biuro wywiadowcze. Wspomniane firmy twierdzą, że ich działalność bardziej zbliżona jest do wyspecjalizowanego doradztwa. Duże spółki mają swoje oddziały wywiadowcze niemal we wszystkich rozproszonych po całym świecie placówkach zagranicznych. Komórki specjalne bacznie obserwują rywali, tropią fuzje, podglądają nowe technologie, a nawet analizują morale w firmach, które są ich klientami. Oddział wywiadowczy dużej spółki, mający w branży dobrą opinię rzadko decyduje się na tego typu metody. Takie incydenty rzucają cień na zgodne z prawem działania wywiadu gospodarczego.

Dwa koncerny, amerykański P&G (Procter and Gamble) i brytyjsko-holenderski Unilever, toczyły od lat zaciętą wojnę o konsumenta na rynku kosmetyków i detergentów. Po siedmiu latach ciszy (od słynnej afery proszku Omo Power), ponowne starcie koncernów miało aspekty szpiegostwa gospodarczego. P&G uzyskał cenne informacje „znalezione" w kontenerach na śmieci w biurze Unilevera w Chicago.

Te wrażliwe informacje to trzyletni plan marketingowy (na 80 stronach druku) dotyczący sprzedaży szamponów na rynku USA, uzyskano ze śmieci Unilevera. Sprawa była nagłośniona w mediach amerykańskich. Podobno koncern P&G wynajął firmę Phoenix Consulting Group, która zatrudnia jako detektywów byłych pracowników CIA i to oni wertowali cenne śmieci.

Doszło do rozmów; Unilever domagał się jak najszybszego zwrotu utraconych informacji, oraz zapłaty **20** milionów USD jako formy zadośćuczynienia. W przeciwnym wypadku groził, że sprawę odda do sądu, z powodu zagrożenia żywotnych interesów firmy[383]. Warto wspomnieć, że przed laty amerykański P&G rozpętał kampanię dezinformacyjną w celu zdezawuowaniu nowego, rewelacyjnego ponoć proszku do prania Omo Power, wylansowanego przez koncern Unilever. Proszek ten miał jakoby wypalać dziury w tkaninach. W efekcie konsumenci stracili zaufanie do nowego produktu i zniknął on z półek sklepowych.

Zdarza się, że po negocjacjach dochodzi do ugody. Przykładowo, realizujący zlecenia przemysłu zbrojeniowego amerykański koncern Raytheon zgodził się pójść na ugodę i zapłacić wielomilionowe odszkodowanie, by uniknąć postępowania sądowego w sprawie wynajęcia prywatnych detektywów, którzy starali się wykraść tajne dokumenty, by przeszkodzić spółce. Ages Group w wygraniu przetargu na kontrakt z amerykańskim lotnictwem. Rzecznik Raytheona potwierdził fakt pójścia na ugodę, ale zaprzeczył, jakoby spółka w jakikolwiek sposób naruszyła prawo.

Eksperci są zgodni, że poza ewidentnymi przypadkami kradzieży, trudno w tym tajemniczym biznesie oddzielić to, co nielegalne, od tego, co wprawdzie nieetyczne, ale jeszcze mieści się w granicach prawa. Najlepiej chyba kierować się zdrowym rozsądkiem. Jednakże praktycy twierdzą, że częste badania kontenerów ze śmieciami przynoszą rezultaty. Nawet tam poszukuje się list klientów konkurencji. W tej kwestii panuje ogólnie przyjęta zasada: jeśli śmieci leżą na ulicy, sprawa jest czysta, ale jeśli znajdują się na czyimś terenie prywatnym, pojawiają się wątpliwości. Problem jest poważny, gdyż – jak twierdzą amerykańskie władze – wiele państw bez przerwy wysyła szpiegów, którzy mają za zadanie wykradać tajemnice amerykańskich spółek. Odparo-

383 M. Bos-Karczewska, *Afera wprost ze śmietnika*, „Rzeczpospolita" z 4 września 2001 r.

wując oskarżenia Amerykanów, Europejczycy wysunęli ostatnio podobne zarzuty pod adresem agencji szpiegowskich rządu USA[384].

Nie podlega kwestii teza, że duża ciemna liczba tego rodzaju przestępstw nie pozwala udowodnić, jak często łamane jest prawo i na jakie straty narażone są ofiary przestępstw. Udane operacje szpiegowskie z definicji nie wychodzą na jaw, więc trudno wszystko oszacować. Poza tym – jak twierdzą eksperci - spółki raczej niezbyt chętnie zgłaszają, że padły ofiarą działalności wywiadowczej, ponieważ nie chcą, by do środków masowego przekazu przedostały się informacje, które stawiają je w niekorzystnym świetle. W zasadzie wszelkie szacunki opierane są na badaniach ekonomicznych, niejednokrotnie anonimowych.

Najbardziej mrocznym aspektem wywiadu jest rola, jaką w całym zjawisku zarówno wywiadu, jak i szpiegostwa gospodarczego odgrywają służby specjalne niektórych państw. Jak wspomniano, reputację najbardziej agresywnych pod tym względem szpiegów mają Francuzi. Znane są jednak zaprzeczenia rządu w Paryżu, jakoby w ten sposób pomagał rodzimym spółkom[385].

Amerykańska ustawa o szpiegostwie gospodarczym z 1996 r. wyraźnie stanowi, że kradzież tajemnic handlowych jest przestępstwem federalnym. Jednak Departament Sprawiedliwości przyznaje, że w okresie pierwszych pięciu lat ujawniono tylko 22 przypadki postawienia firmy w stan oskarżenia na podstawie zapisów tej ustawy.

384 N. King, J. Bravin, *Wywiad gospodarczy kwitnie po obu stronach Atlantyku*, „The Wall Street Journal Europe", www.gazeta.pl(10 lipca 2000)

385 Tamże.

# Rozdział 9

# Regulacje prawne w ochronie informacji

## 1. Wprowadzenie

Mimo starań wielu organizacji, krajów i decydentów obowiązujący stan prawny nie jest w stanie uwzględnić wszystkich rozpoznanych zagrożeń. Wprawdzie okresowo dokonuje się systematycznych nowelizacji poszczególnych przepisów, lecz są to jedynie półśrodki, które nie mogą sprostać nasilającym się systematycznie zagrożeniom. W dobie powszechnego już wykorzystywania przekazu informacji, szczególnie poprzez Internet, niezwykle trudno jest rozpoznać i określić wszystkie występujące zagrożenia. Warto pamiętać o tych podstawowych, także omówionych w tej pracy, które powodują nie tylko straty finansowe, lecz mogą grozić bezpieczeństwu powszechnemu, a szczególnie życiu i zdrowiu obywateli czy bezpieczeństwu Państwa. Wiele krajów przygotowuje się nie tylko do kryminologicznego i kryminalistycznego, ale również interdyscyplinarnego przeciwdziałania różnego rodzaju sytuacjom kryzysowym, które mogą być spowodowane zarówno naruszeniem tajemnic zawodowych, jak np. tajemnicy przedsiębiorstwa, szpiegostwem gospodarczym, czy atakiem cyberterrorystycznym. Z tego względu zarówno służby specjalne, jak i resorty strategiczne, zgodnie z obowiązującym ustawodawstwem opracowują plany zabezpieczeń tzw. infrastruktury krytycznej, istotnej z punktu widzenia bezpieczeństwa narodowego i wewnętrznego.

Ważnym problemem stało się zagadnienie prawnej, a szczególnie karnoprawnej ochrony informacji, a ochrony informacji w cyberprzestrzeni – w szczególności.

## 2. Regulacje prawne Unii Europejskiej

Powszechna jest opinia, że obowiązujący stan prawny nie jest wystarczający do skutecznych działań zarówno rozpoznawczych, śledczych, jak i zapobiegawczych, tym bardziej, że nie ma już dziedziny życia społecznego, która nie korzysta z przepływu informacji w cyberprzestrzeni i baz danych.

Wśród znanych dotychczas sposobów ochrony baz danych, systemów i sieci teleinformatycznych obok zabezpieczeń natury administracyjno-organizacyjnej i technicznej istotną rolę w rozpoznawaniu i przeciwdziałaniu mogą odegrać systematycznie doskonalone regulacje karnoprawne.

Szczególne znaczenie w omawianej kwestii posiada Konwencja Rady Europy z 23 listopada 2001 roku o cyberprzestępczości, zawarta w Budapeszcie, która wprawdzie została podpisana przez Polskę, lecz z dużymi perturbacjami doszło do jej ratyfikowa-

nia ustawą z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.[386] Znacznie wcześniej Konwencja została ratyfikowana przez 24 kraje spośród 47 krajów członków Rady Europy, a także przez USA, a jej najważniejsze postanowienia dotyczą:

- harmonizacji narodowych systemów prawnych w sprawie zdefiniowania przestępstw,
- wypracowania standardów prowadzenia śledztw oraz procedur sądowych dostosowanych do zasad działania globalnej sieci,
- stworzenia szybkiego i skutecznego systemu współpracy międzynarodowej[387];

Typologia cyberprzestępstw według cytowanej Konwencji przedstawia się następująco:

1) przestępstwa przeciwko poufności, integralności i dostępności danych i systemów teleinformatycznych, jak:
   a) nielegalny dostęp do systemów teleinformatycznych - *hacking* (art. 2),
   b) podsłuch komputerowy (art. 3),
   c) nielegalna ingerencja w dane oraz nielegalna ingerencja w funkcjonowanie systemu, (art. 4),
   d) wytwarzanie, oferowanie, sprzedaż i posiadanie narzędzi hakerskich(art. 6)*;*
2) przestępstwa związane z użyciem komputera, jak:
   a) fałszerstwo komputerowe (art. 7);
   b) oszustwo komputerowe (art. 8);
3) przestępstwa związane z charakterem informacji stanowiących ich przedmiot, jak pornografia dziecięca (art. 9);
4) przestępstwa przeciwko własności intelektualnej;
5) inne przestępstwa mające związek z użyciem systemu teleinformatycznego.

Wiele uwagi omawianemu zagadnieniu poświęcają władze Unii Europejskiej. Niezwykle istotne znaczenie mają w szczególności:

1. Dyrektywa Rady 91/250/EWG z 14 maja 1991 r. o prawnej ochronie programów komputerowych[388];
2. Dyrektywa Rady 96/9/EWG z 11 marca 1996 r. o ochronie prawnej baz danych[389];
3. Decyzja ramowa Rady 2000/375/WSiSW z dnia 29 maja 2000 r. w sprawie zwalczania pornografii dziecięcej w Internecie;
4. Dyrektywa Parlamentu Europejskiego i Rady 2001/29/WE z dnia 22 maja 2001 r. o harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym[390];

386 Dz. U. z dnia 4 listopada 2014 r., poz. 1514.

387 Wcześniejsze dokumenty Rady Europy w tej kwestii to: Zalecenie nr R (89) 9 Computer-Related Crime, o przestępczości komputerowej i końcowe sprawozdanie Komitetu Problemów Przestępczości Rady Europy, Strasbourg 1989 oraz Zalecenie nr R (95) 13 Problems of Criminal Procedural Law Connected with Information Technology przyjęte przez Komitet Ministrów Rady Europy 11 września 1995 r.

388 Dz. Urz. L 122 z 17.05.1991.

389 Dz. Urz. L. 77 z 22.03.1996.

390 Dz. Urz. L 167/10 z 22.06.2001.

5. Decyzja ramowa Rady 2001/413/WSiSW z 28 maja 2001 r. w sprawie zwalczania oszustw i podrabiania bezgotówkowych środków płatniczych[391], która w art. 3 określa konieczność podjęcia działań wobec osób popełniających przestępstwo, poprzez: bezprawne wprowadzanie, zmienianie, usuwanie lub ukrywanie danych informatycznych, w szczególności danych umożliwiających identyfikację, lub bezprawne zakłócanie działania programu lub systemu informatycznego;
6. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. o prywatności i łączności elektronicznej dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej nakłada na dostawców ogólnodostępnych usług komunikacji elektronicznej obowiązek zadbania o bezpieczeństwo ich usług.
7. Rozporządzenie (WE) Nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[392].

## 3. Uregulowania w Kodeksie karnym związane z naruszeniem ochrony informacji

Wprawdzie do polskiego ustawodawstwa karnego, zarówno kodeksowego, jak i pozakodeksowego, wprowadzono nowe typy przestępstw, także cyberprzestępstwo na podstawie prawa unijnego, to jednakże nie nadążamy z implementacją ustawodawstwa w wielu zagadnieniach. Jest to o tyle niepokojące, że systematycznie rozpowszechniają się nowe techniki naruszania dóbr prawnych przy wykorzystywaniu technologii informacyjnych.

Omawiane w tym rozdziale regulacje Kodeksu karnego dotyczą szerszego zakresu czynów niż określone w rozdziale XXXIII k.k. Szereg czynów karalnych ma miejsce w formie manipulowania informacjami, dokumentami systemami i różnorodnymi dokumentami.

Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej[393] wprowadziła istotny porządek terminologiczny w aktualnych aktach prawnych; przyczyniła się również w tej kwestii kolejna nowelizacja dotycząca cyberprzestępczości w ramach ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw[394]. Zdaniem profesjonalistów niezbędne są dalsze zmiany.

### 3.1. Przestępstwa przeciwko Rzeczypospolitej Polskiej – rozdział XVII k.k.

#### 3.1.1. Szpiegostwo, szpiegostwo komputerowe albo wywiad komputerowy – art. 130 § 2 i 3 k.k.

§ 1. *Kto bierze udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10.*

§ 2. *Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypo-*

391 Dz. U. L 149 z 2.6.2001.
392 Dz. U. L 77 z 13.3.2004.
393 Dz. U. nr 171, poz. 1056.
394 Dz. U. Nr 214, poz. 1344.

*spolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3*.

§ 3. *Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2,* gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Przedmiotem przestępstwa jest obronność, bezpieczeństwo i gospodarka Rzeczypospolitej Polskiej. Czynność sprawcza polega na braniu udziału w obcym wywiadzie, któremu dostarczano informacje mogące wyrządzić szkodę RP.

Działalność w obcym wywiadzie skierowana przeciwko RP ścigana jest z art. 130 § 1 k.k. i przewiduje zagrożenie karą pozbawienia wolności od roku do lat 10. Wszystkie postacie przestępstwa mają charakter umyślny. Warto także podkreślić, że karalne są wszystkie rodzaje działalności wywiadowczej, a więc zbieranie lub udzielanie informacji o charakterze militarnym, przemysłowym, naukowym itp.

Kwalifikowaną postać szpiegostwa przewidują postanowienia § 2 tego artykułu, tj. branie udziału w obcym wywiadzie albo działanie na jego rzecz oraz udzielanie wiadomości, których przekazanie może wyrządzić szkodę interesom RP (np. o charakterze tajemnicy państwowej czy służbowej). Karalne jest również udzielanie, zbieranie, gromadzenie i przechowywanie wiadomości, tj. przygotowywanie się do zbrodni określonej w § 2, a nawet wyrażenie gotowości do przekazania informacji obcemu wywiadowi.

Szczególną formą tego przestępstwa, określoną w § 3, jest gromadzenie, przechowywanie wiadomości określonych w § 2 poprzez podłączenie się do systemu teleinformatycznego w celu uzyskania odpowiednich informacji. Istotą omawianego przestępstwa jest działanie celowe, a więc zbieranie, gromadzenie i przechowywanie informacji, które mają być przekazane obcemu wywiadowi, albo zgłaszanie gotowości działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej. Wspomniana regulacja określa zagrożenie karą pozbawienia wolności od 6 miesięcy do lat 8.

### 3.1.2. Wprowadzenie w błąd polskich organów państwowych w trakcie współpracy wywiadowczej – art. 132 k.k.

*Kto, oddając usługi wywiadowcze Rzeczypospolitej Polskiej, wprowadza w błąd polski organ państwowy przez dostarczanie podrobionych lub przerobionych dokumentów lub innych przedmiotów albo przez ukrywanie prawdziwych lub udzielanie fałszywych wiadomości mających istotne znaczenie dla Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10.*

Przedmiotem ochrony jest prawidłowość działania polskich organów państwowych, czyli właściwych służb wywiadowczych w zakresie uzyskiwania informacji od tajnych współpracowników. Przepis ma charakter profilaktyczny, gdyż ma chronić służby przed dezinformacją**.** Przestępstwo to ma charakter materialny. Może być dokonane przez działanie jak i zaniechanie. Do jego znamion należy skutek w postaci dania wiary fałszywym informacjom[395].

Zatem w trakcie współpracy ze służbami wywiadowczymi Rzeczypospolitej Polskiej, dostarczanie podrobionych lubprzerobionych dokumentów lub innych przedmiotów albo ukrywanie prawdziwych lub udzielanie fałszywych wiadomości mających istotne znaczenie, podlega karze pozbawienia wolności od roku do lat 10.

395 M. Mozgawa (red.) *Kodeks karny. Komentarz*, Warszawa 2014, s 350, 351.

## 3.2. Przestępstwa przeciwko bezpieczeństwu powszechnemu – rozdział XX k.k.

### 3.2.1. Sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach poprzez system informatyczny – art. 165 § 1 pkt 4 k.k.

§ 1. *Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach:*

1. *powodując zagrożenie epidemiologiczne lub szerzenie się choroby zakaźnej albo zarazy zwierzęcej lub roślinnej,*
2. *wyrabiając lub wprowadzając do obrotu szkodliwe dla zdrowia substancje, środki spożywcze lub inne artykuły powszechnego użytku lub też środki farmaceutyczne nie odpowiadające obowiązującym warunkom jakości,*
3. *powodując uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności urządzenia dostarczającego wodę, światło, ciepło, gaz, energię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia,*
4. *zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych,*
5. *działając w inny sposób w okolicznościach szczególnie niebezpiecznych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.*

§ 2. Jeżeli sprawca działa nieumyślnie, podlega karze pozbawienia wolności do lat 3.

§ 3. Jeżeli następstwem czynu określonego w § 1 jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, sprawca podlega karze pozbawienia wolności od lat 2 do 12.

§ 4. Jeżeli następstwem czynu określonego w § 2 jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Za przestępstwo odpowiada ten, kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach wówczas gdy jego czyn polega na zakłócaniu, uniemożliwianiu lub wpływaniu w inny sposób na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych w systemie informatycznym.

Z tego przepisu może odpowiadać sprawca, który zagroził bezpieczeństwu powszechnemu związanemu z funkcjonowaniem lotniska, stacji kolejowej, urządzeń dostarczających wodę, gaz, energię dla ludności, monitorowaniem danych na oddziale intensywnej terapii, chronionych obiektów bankowych, wojskowych itp. przykładowo poprzez wprowadzenie wirusa do programu komputerowego sterującego powyższymi czynnościami i mającego wpływ na bezpieczeństwo powszechne.

Omawiany przepis nie przynosi zamkniętego katalogu możliwych czynności wykonawczych. Zawiera bowiem zwrot „działając w inny sposób w innych okolicznościach szczególnie niebezpiecznych". Dotyczy to zwłaszcza sytuacji w której zagrożone jest życie ludzkie lub mienie w znacznych rozmiarach.

Kwalifikowana forma tego przestępstwa zachodzi wówczas gdy następstwem działania sprawcy jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób,

tj. wynikająca z regulacji zawartej w art.165 § 3 k.k., wówczas zagrożenie karą pozbawienia wolności sięga od lat 2 do lat 12.

### 3.2.2. Finansowanie terroryzmu poprzez system informatyczny – art. 165a k.k.

*Kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w celu sfinansowania przestępstwa o charakterze terrorystycznym, podlega karze pozbawienia wolności od lat 2 do 12.*

Przedmiotem ochrony jest bezpieczeństwo związane z przestępstwami o charakterze terrorystycznym. Jest to przestępstwo umyślne, bezskutkowe i powszechne[396]. Karalne jest gromadzenie, przekazywanie lub oferowanie środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych, innego mienia ruchomego lub nieruchomości w celu sfinansowania przestępstwa o charakterze terrorystycznym, które podlega karze pozbawienia wolności od lat 2 do 12.

Przestępstwem o charakterze terrorystycznym jest czyn określony w art. 115§ 20 k.k. jako czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu[397]. Formy działania sprawcy poprzez system informatyczny mogą być różnorodne[398].

Przestępstwo z art. 165a k.k. ma ścisły związek z czynami, które mogą być kwalifikowane z art. 299 k.k., tj. praniem pieniędzy[399].

## 3.3. Przestępstwa przeciwko wymiarowi sprawiedliwości – rozdział XXX k.k.

W polskim ustawodawstwie funkcjonują przepisy, które w sposób szczególny nakazują informowanie organów ścigania o zaistnieniu określonych przestępstw. W Kodeksie karnym zawarty jest obowiązek zgłoszenia właściwej informacji o zaistniałym, groźnym czy o terrorystycznym charakterze przestępstwie, pod groźbą kary pozbawienia wolności.

Kolejna regulacja zakazuje udzielania informacji, a także rozpowszechniania wiadomości z postępowania przygotowawczego czy sądowego mając na względzie nie tylko tzw. dobro śledztwa, lecz również dobro podejrzanego czy oskarżonego.

Według Kodeksu postępowania karnego niezbędny jest społeczny i instytucjonalny obowiązek zawiadomieniao zaistniałym przestępstwie, czyli działanie w interesie bezpieczeństwa i porządku publicznego.

396 Tamże s. 419.
397 Szerzej: J.W. Wójcik, Przeciwdziałanie finansowaniu terroryzmu, Warszawa 2007.
398 Szerzej w rozdziale 4 p. 5.2.
399 J.W. Wójcik, *Przeciwdziałanie praniu pieniędzy*, Kraków 2004.

### 3.3.1. Szczególny obowiązek informowania organów ścigania o popełnionym przestępstwie

*Art. 240. § 1. Kto, mając wiarygodną wiadomość o karalnym przygotowaniu albo usiłowaniu lub dokonaniu czynu zabronionego określonego w art. 118, 118a, 120-124, 127, 128, 130, 134, 140, 148, 163, 166, 189, 252 lub przestępstwa o charakterze terrorystycznym, nie zawiadamia niezwłocznie organu powołanego do ścigania przestępstw, podlega karze pozbawienia wolności do lat 3.*

§ 2. *Nie popełnia przestępstwa określonego w § 1, kto zaniechał zawiadomienia mając dostateczną podstawę do przypuszczenia, że wymieniony w § 1 organ wie o przygotowywanym, usiłowanym lub dokonanym czynie zabronionym; nie popełnia przestępstwa również ten, kto zapobiegł popełnieniu przygotowywanego lub usiłowanego czynu zabronionego określonego w § 1.*

§ 3. *Nie podlega karze, kto zaniechał zawiadomienia z obawy przed odpowiedzialnością karną grożącą jemu samemu lub jego najbliższym.*

Ten szczególny obowiązek dotyczy osób, które posiadają wiadomości o specjalnie niebezpiecznych przestępstwach, które zostały wymienione enumeratywnie. Przepis ten ma na celu dobro społeczne. Przedmiotem ochrony jest wymiar sprawiedliwości, a ściślej ujmując, jego interes wyrażający się w tym, aby zamach na dobra prawne chronione przepisami wymienionymi w art. 240 § 1 został ujawniony, a jego sprawca ujęty, zaś w sytuacji gdy jest to możliwe, aby zapobiec wskazanym tam przestępstwom.

## 3.4. Przestępstwa przeciwko ochronie informacji – rozdział XXXIII k.k.

Nieuprawnione zdobywanie informacji może wywołać wiele szkód o zróżnicowanym charakterze, a szczególnie: gospodarczym, technologicznym, finansowym, czy związanym z bezpieczeństwem państwa.

Prawnokarna ochrona informacji ma charakter wielopłaszczyznowy, gdyż chroni jej integralność, dostępność i poufność[400]. Natomiast ochrona poufności informacji to ochrona informacji stanowiących różnorodne tajemnice. Zatem rodzajowym przedmiotem ochrony wszystkich przepisów zawartych w tym rozdziale jest informacja, którą należy rozumieć jako sumę wiadomości o osobie albo o stanie rzeczy, dotyczącą faktów, stanowiącą logiczną całość[401].

### 3.4.1. Ujawnienie informacji niejawnej o klauzuli „tajne" i „ściśle tajne" – art. 265 § 1 k.k.

§ 1. *Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne" lub „ściśle tajne", podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

§ 2. *Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.*

400 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 26-29.

401 B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości.* Rozdział XXX i XXXIII *Kodeksu karnego. Komentarz,* Warszawa 2002, s. 391.

§ 3. *Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

Regulacje zawarte w art. 265 i 266 k.k. odgrywają istotne znaczenie w zakresie ochrony informacji niejawnych. W art. 265 § 1 przewidziany jest podstawowy typ przestępstwa ujawnienia informacji niejawnych o klauzuli „tajne" lub „ściśle tajne". Sprawca, który ujawnia lub wbrew przepisom ustawy wykorzystuje takie informacje podlega karze pozbawienia wolności od 3 miesięcy do 5 lat.

### 3.4.2. Ujawnienie informacji niejawnej o klauzuli „tajne" i „ściśle tajne" na rzecz podmiotu zagranicznego – art. 265 § 2 k.k.

Podmiotami zagranicznymi są osoby fizyczne posiadające obce obywatelstwo, a w przypadku podwójnego obywatelstwa rozstrzygać powinno miejsce zamieszkania, także osoba prawna lub jednostka organizacyjna z siedzibą za granicą np. przedsiębiorca zagraniczny.

Ujawnienie omawianych informacji osobie działającej w imieniu lub na rzecz podmiotu zagranicznego stanowi czyn kwalifikowany ze względu na osobę, wobec której ujawniono informacje niejawne i sprawca podlega wyższej karze, tj. od 6 miesięcy do lat 8 pozbawienia wolność.

### 3.4.3. Nieumyślne ujawnienie informacji niejawnej – art. 265 § 3 k.k.

*Jeżeli sprawca nieumyślnie ujawnił informację opatrzoną klauzulą jak w § 1 – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

### 3.4.4. Ujawnienie lub wykorzystanie informacji uzyskanej w ramach tajemnicy zawodowej – w związku z pełnioną funkcją – art. 266 § 1 k.k.

§ 1. *Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§ 2. *Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.*

§ 3. *Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.*

Omawiany przepis przewiduje penalizację naruszenia tzw. tajemnicy zawodowej, określanej także jako funkcyjna i prywatna – art. 266 § 1 k.k. oraz służbowa art. 266 § 2 k.k.

Jednakże nieuprawnione ujawnienie tych informacji musi zagrażać enumeratywnie wymienionym w ustawie oraz zróżnicowanym adekwatnie co do nadanej klauzuli, dobrom, tj. w przypadku informacji ściśle tajnych – wyrządzić szkodę wyjątkowo poważną, informacji uznanych za tajne – szkodę poważną, informacji poufnych – szkodę, a w przypadku informacji zastrzeżonych – będzie zauważalny szkodliwy wpływ na realizację wymienionych w ustawie działań.

Przedmiotem ochrony z tego przepisu, jak w art. 265 k.k., jest poufność informacji. Przepis chroni stosunek zaufania pomiędzy dysponentem a depozytariuszem informacji, który jest warunkiem prawidłowości wykonywania określonych zawodów, pełnienia funkcji czy prowadzenia pewnych działalności. Ochroną objęty jest również interes prywatny, w których chodzi szczególnie o sferę prywatności, jak i inne interesy, w które godzi ujawnienie tajemnicy służbowej (z § 2). Przy przestępstwie z art. 266 § 1 k.k. rodzajowym przedmiotem ochrony jest dyskrecjonalność informacji, zaś przedmiotem ochrony bezpośredniej prawo zachowania określonych informacji w tajemnicy, także prawidłowego wykonywania niektórych zawodów lub prowadzenia określonej działalności w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, w których szczególne znaczenie odgrywa stosunek zaufania. Na stosunek ten uwagę zwrócił Sąd Najwyższy[402].

Termin tajemnica zawodowa ma miejsce wówczas, gdy wiadomość nią objęta została uzyskana przez osobę reprezentującą określony zawód, z tytułu wykonywania którego było możliwe wejście w posiadanie cudzej tajemnicy[403]. Ustalenie obowiązku zachowania tajemnicy zawodowej może wynikać wprost z przepisów regulujących tryb i zasady wykonywania określonych zawodów bądź z przyjęcia nasiebie zobowiązaniaco do nieujawniania faktów poznanych w związku z wykonywaną pracą zawodową. Uzasadnione w tej kwestii są poglądy, że źródłem obowiązku zachowania dyskrecji w przypadku tajemnicy zawodowej nie muszą być wyraźne przepisy prawne, lecz także zasady etyki zawodowej. Tajemnica zawodowa może obejmować zarówno wiadomości, które dotyczą stylu czy zasad życia określonych osób, uzyskane w ramach wykonywania rutynowych czynności zawodowych, jak i w ramach pełnionych funkcji, a także informacje dotyczące sposobu ich wykonywania.

Istnieje jednak uzasadniony pogląd, że przepis § 1 dotyczy także każdej tajemnicy poznanej w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, które określono jako tajemnicę funkcyjną404. Natomiast tajemnicą prywatną mogą być informacje dotyczące prywatnej sfery życia dysponenta informacji[405].

Karalne są wszystkie naruszenia tajemnicy zawodowej, w których przepisy nakładają obowiązek jej dochowania. Natomiast art. 266 § 1 k.k. stanowi normę niezabezpieczoną, czyli nie przewiduje wprost sankcji karnych za naruszenie obowiązku tajemnicy. Zatem sankcje karne przewidują określone ustawy szczegółowe. Jednakże warto zwrócić uwagę, że omawiany przepis może mieć zastosowanie tam, gdzie przepis ustawy szczegółowej nie przewiduje wprost zachowania tajemnicy zawodowej, lecz charakter zawodu czy prowadzonej działalności umożliwia uzyskanie wiadomości poufnych, szczególnie z zakresu życia prywatnego[406]. Zatem ochrona przewidziana w art. 266 § 1 k.k. może również dotyczyć każdej cudzej tajemnicy[407].

Zdarza się, że mylone są podstawowe terminy i pojęcia. Należy zatem podkreślić, że podstawowym kryterium odróżniającym tajemnicę zawodową od służbowej jest pierwszorzędność interesów. Ta pierwszorzędność chroniona jest przez zakazy

402 Szerzej: Postanowienie SN z dnia 21 marca 2013 r., III KK 267/12, LEX nr 1293801.
403 M. Mozgawa (red.), *Kodeks karny*, wyd. cyt. s. 666-669.
404 B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji, wyd. cyt. s.* 445.
405 M. Mozgawa (red.), *Kodeks karny,* wyd. cyt. s. 666.
406 Tamże s. 666.
407 Tamże.

ujawniania informacji objętych rodzajami tajemnic. Obowiązek zachowania tajemnicy służbowej ma charakter publiczny i uzasadniony jest przede wszystkim interesem społecznym, natomiast tajemnica zawodowa obejmuje swoim zakresem informacje dotyczące najczęściej sfery życia osobistego i odnosi się do interesów osobistych czy też prywatnych i indywidualnych[408].

Zakaz ustawowy lub przyjęte zobowiązanie nakłada prawny obowiązek ujawnienia lub wykorzystania informacji, z którą sprawca zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową. Naruszenie tych zakazów podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Ściganie powyższego przestępstwa następuje na wniosek pokrzywdzonego.

### 3.4.5. Ujawnienie informacji niejawnej o klauzuli „zastrzeżone" lub „poufne" przez funkcjonariusza publicznego – art. 266 § 2 k.k.

Podlega karze funkcjonariusz publiczny, który ujawnił osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację uzyskaną w związku z wykonywaniem czynności służbowych. Tym samym ochroną w tym przepisie objęty jest także interes prywatny oraz sfera prywatności, jak też inne interesy, w które godzi ujawnienie informacji niejawnych, a ich ujawnienie może narazić na szkodę prawnie chroniony interes o klauzuli „poufne" lub „zastrzeżone"[409]. Taki czyn podlega karze pozbawienia wolności do lat 3.

Zgodnie z regulacją zawartą w art. 115 § 13 k.k. funkcjonariuszem publicznym jest: Prezydent Rzeczypospolitej Polskiej, poseł, senator, radny, poseł do Parlamentu Europejskiego, sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postępowania przygotowawczego lub organu nadrzędnego nad finansowym organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w organach dyscyplinarnych działających na podstawie ustawy; osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych; osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe; osoba zajmująca kierownicze stanowisko w innej instytucji państwowej; funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej; osoba pełniąca czynną służbę wojskową oraz pracownik międzynarodowego trybunału karnego, chyba że pełni wyłącznie czynności usługowe.

Należy mieć na uwadze, że jeżeli sprawcą czynu z art. 266 § 1 k.k. może być tylko ten na kim spoczywa obowiązek zachowania tajemnicy, to sprawcą czynu z art. 266 § 2 k.k. może być funkcjonariusz publiczny. Ściganie naruszenia tajemnicy zawodowej ma miejsce jedynie na wniosek pokrzywdzonego, a ściganie naruszenia tajemnicy przez funkcjonariusza publicznego następuje z urzędu.

408 J. Preussner-Zamorska, *Zakres prawnie chronionej tajemnicy w postępowaniu cywilnym, „Kwartalnik Prawa Prywatnego" 1998, z. 2,* s. 310.

409 M. Mozgawa (red.) *Kodeks karny.* wyd. cyt., s. 667

### 3.4.6. Nielegalne uzyskanie cudzej informacji, systemu teleinformatycznego, pokonanie zabezpieczeń i kradzież informacji – *hacking komputerowy* – art. 267 § 1 k.k.

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte *pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§ 2. *Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.*

§ 3. *Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.*

§ 4. *Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 -3 ujawnia innej osobie.*

§ 5. *Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.*

Przedmiotem ochrony jest poufność informacji, prawo do dysponowania informacją z wyłączeniem innych osób, a także bezpieczeństwo jej przekazywania[410]. Przepis ten dotyczy kilku form działania, a mianowicie są to: uzyskanie dostępu do cudzej informacji bez uprawnienia, a zatem w sposób nielegalny, otwarcie zamkniętego pisma, które nie było adresowane do sprawcy, a także podłączenie się do sieci telekomunikacyjnej, a więc zarówno telefonicznej, jak i informatycznej, a także przełamanie albo omijanie elektronicznych, magnetycznych, informatycznych lub innych szczególnych jej zabezpieczeń. Natomiast istotą występku, o jakim mowa w art. 267 § 1 k.k., jest uzyskanie informacji dyskrecjonalnej, nieprzeznaczonej dla sprawcy. Jednakże uzyskanie dostępu do informacji przesądza, że warunkiem dokonania tego przestępstwa nie jest dojście treści informacji do wiadomości sprawcy[411].

Nieuprawnione wejście do systemu teleinformatycznego przez naruszenie zastosowanych zabezpieczeń i manipulowanie w bazie danych od dawna określane jest jako „włamanie do komputera" i kradzież danych, co jest popularnie określane jako *hacking*[412]. Sprawcami tych przestępstw są najczęściej wyspecjalizowane osoby – hakerzy.

Zgodnie z art. 2 cytowanej dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne, określa się, że system informatyczny oznacza urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń w celach ich eksploatacji, użycia, ochrony lub utrzymania.

Warto mieć na uwadze, że zgodnie z art. 7 pkt 2a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych przez system informatyczny rozumie się zespół współ-

410 A. Adamski, Prawo karne komputerowe, wyd. cyt., s. 42.

411 M. Mozgawa (red.) *Kodeks karny,* wyd. cyt., s. 670.

412 Szerzej: J. W. Wójcik, *Przestępstwa komputerowe, cz. 1 - Fenomen cywilizacji i cz. 2 - Techniki zapobiegania,* CIM, Warszawa 1999.

pracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych[413].

Przepis ten stanowi również, że przełamanie czy omijanie elektronicznego zabezpieczenia czyli *hacking,* polega na usunięciu szczególnych konstrukcji, „osłon", które służą uniemożliwieniu dostępu do informacji zgromadzonych w systemie. Jest to każda czynność, która ma *ułatwić* **s**prawcy dostęp do informacji; może polegać na usunięciu zabezpieczenia przez jego zniszczenie lub oddziaływanie na zabezpieczenie w celu zniwelowania jego funkcji ochronnych nawet bez ich zniszczenia. Obojętny jest zatem rodzaj urządzenia, gdyż chodzi o wszystkie urządzenia, także telekomunikacyjne, czy teleinformatyczne, służące przekazywaniu informacji. Również nie jest istotny cel wejścia do sieci czy systemu[414].

Także otwarcie zamkniętego pisma może nastąpić w dowolny sposób, który np. polega na usunięciu zabezpieczenia, uniemożliwiającego dotarcie do jego treści, nawet bez niszczenia opakowania (np. przez prześwietlenie[415]. Wiadomo, że inny jest *modus operandi* sprawcy otwierającego cudzy list, czy podsłuchującego rozmowę telefoniczną, a inny jeszcze sprawcy działającego poprzez naruszanie zabezpieczeń systemu teleinformatycznego, ich przełamanie czy ominięcie. Obojętny jest zatem rodzaj pokonanego zabezpieczenia. Istotą omawianego przestępstwa jest uzyskanie informacji przez hakera, któremu grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

### 3.4.7. Nielegalne uzyskanie dostępu do całości lub części systemu informatycznego – art. 267 § 2 k.k.

Karalne jest skuteczne działanie, które doprowadziło do uzyskania dostępu bez uprawnienia do całości lub do części systemu informatycznego poprzez założenie urządzenia podsłuchowego lub wizualnego.

### 3.4.8. Nielegalne uzyskanie informacji poprzez urządzenie podsłuchowe, wizualne albo inne urządzenie lub oprogramowanie – art. 267 § 3 k.k.

Karalne jest także działanie, które polega na nielegalnym posługiwaniu się urządzeniem podsłuchowym, wizualnym lub innym, czyli takim, które służy do rejestracji dźwięku i obrazu, za pomocą którego można uzyskać informację, a więc może to być: kamera, aparat fotograficzny, magnetofon, dyktafon czy inne urządzenie. Karalne jest także instalowanie specjalistycznego oprogramowania, tj. takiego programu komputerowego lub innego oprogramowania, które służy do nieuprawnionego pozyskania informacji, lub posługiwanie się tym programem w celu nieuprawnionego uzyskania informacji.

Przechwytywanie wszelkich informacji, w tym także stwarzanie poważnych zagrożeń dla systemów teleinformatycznych umożliwiają zdobycze współczesnej techniki. Możliwy jest nawet zdalny podsłuch i podgląd, czyli prowadzenie pełnej kontroli bez wiedzy i zgody właściciela systemu.

413 t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.

414 M. Mozgawa (red.) *Kodeks karny,* wyd. cyt., s. 670-673.

415 I. Andrejew i inni (red.) *System Prawa Karnego, t. 4, O przestępstwach w szczególności, cz. 1*, T. Bojarski, *Naruszenie tajemnicy korespondencji, Ossolineum 1989, s.* 72.

### 3.4.9. Nielegalne przekazanie informacji uzyskanej wbrew przepisom prawa – art. 267 § 4 k.k.

Karalne jest również przekazanie innej osobie informacji uzyskanej w sposób określony w ramach stanów prawnych wymienionych w paragrafach 1-4 art. 267 k.k., tj. *hackingu*, jak i podsłuchu komputerowego, podglądu komputerowego, otwarcia cudzej korespondencji, a także udzielenia ujawnionych w ten sposób informacji osobom trzecim – danych bez względu na rodzaj uzyskanej i przekazanej tajemnicy czy klauzuli ich chroniących. Może to być zatem zarówno informacja niejawna, czy inna zawodowa jak np.: handlowa, bankowa, czy dotycząca innych niejawnych danych.

Norma tego artykułu ma charakter ogólny, bowiem prawo nie odgrywa tu specjalnej roli zapobiegawczej. Przeciwdziałanie podsłuchowi i podglądowi komputerowemu przypada przede wszystkim specjalistom w zakresie ochrony systemów i sieci teleinformatycznych.

Zasadniczym celem ochrony jest poufność przekazywanych lub przesyłanych informacji przy użyciu środków technicznych, a także ochrona prywatności każdego człowieka przed różnymi formami nieuprawnionej inwigilacji, jak np. podglądanie czy podsłuchiwanie, a w tym czytanie cudzej korespondencji.

Wszystkie czyny z art. 267 k.k. zagrożone są grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat 2. Natomiast ściganie tych występków następuje na wniosek pokrzywdzonego.

Warto dodać, że ochrona korespondencji, bez względu na jej formę, realizowana jest również przez prawo cywilne szczególnie zaś, gdy zaistniały określone skutki. Artykuł 25 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny[416] pozwala na żądanie usunięcia skutków, a jeśli zaistniała szkoda majątkowa, poszkodowany może żądać naprawienia jej w ramach przepisów ogólnych. W zakresie odpowiedzialności za czyny niedozwolone art. 415 k.c. stanowi *Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia* oraz art. 416 k.c. – o*soba prawna jest obowiązana do naprawienia szkody wyrządzonej z winy jej organu.*

Omawiany problem w świetle prawa cywilnego dotyczy także ochrony nadawcy korespondencji. Może tu zachodzić przykładowo, przesłanie korespondencji bez zabezpieczenia jej treści kopertą, z odpowiednimi kodami kryptograficznymi w przypadku poczty elektronicznej. Zatem ochrona cywilnoprawna ma większy zakres niż ochrona karnoprawna.

### 3.4.10. Niszczenie informacji – art. 268 § 1 - 3 k.k.

§ 1. *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§ 2. *Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.*

§ 3. *Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

§ 4. *Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.*

416 Dz. U. Nr 16, poz. 93, ze zm.

Przedmiotem ochrony są integralność (nienaruszalność) informacji oraz dostępność, czyli możliwość korzystania z niej przez uprawnione podmioty. Natomiast ochrona integralności zapisu informacji ma zapewnić jej kompletność i poprawność[417].

Formy niszczenia polegają na różnorodnym działaniu, jak np.: nielegalna ingerencja w dane, utrudnianie zapoznania się i niszczenie istotnej informacji, uszkodzenie, wymazanie danych, zmiana zapisu, dodanie nowych elementów czy udaremnienie. Takie działanie polegać będzie na całkowitym uniemożliwieniu zapoznania sięz informacją przez osobę uprawnioną. Utrudnienie polega natomiast na wprowadzeniu przeszkód w zapoznaniu się z informacją oraz w zrozumieniu jej sensu.

Podkreślić należy, iż zakazane jest działanie związane z naruszeniem integralności zapisu informacji na nośniku teleinformatycznym, które może nastąpić w wyniku bezprawnego zniszczenia, uszkodzenia, usuwania lub zmiany zapisu istotnej informacji albo udaremnienie czy utrudnienie osobie uprawnionej zapoznanie się z nią.

Kara przewidziana jest bez względu na sposób niszczenia zapisu informacji np. w bazie danych, w trakcie przetwarzania informacji, poprzez wprowadzenie (do programu czy sieci) wirusa, hasła lub zmianę albo jakiekolwiek inne utrudnienie dostępu do informacji osobie upoważnionej. Dotyczy także spowodowania zakłóceń, o ile podłączono do sieci urządzenia pozwalające na przetwarzanie lub rejestrowanie danych, a także poprzez dopisanie nowych danych lub zmianę istniejącego zapisu.

Zgodnie z § 1 karalne jest działanie takiego sprawcy, który nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią. Jeżeli takie działanie dotyczy zapisu na komputerowym nośniku informacji, to zgodnie z § 2 czyn ten zagrożony jest karą pozbawienia wolności do lat 3, a nie jak to ma miejsce w poprzednim paragrafie do lat 2.

Mamy tu do czynienia z przestępstwa skutkowym, a skutkami czynów z § 1 i 2 są zniszczenie, uszkodzenie, usunięcie lub zmiana zapisu informacji, a także znaczna szkoda majątkowa.

Kwalifikowany typ omawianych czynów zaistnieje wówczas, gdy sprawca dopuścił się znacznej szkody majątkowej. Zgodnie z § 3 podlega wówczas karze pozbawienia wolności od 3 miesięcy do lat 5. Jednakże ściganie przestępstw określonych we wszystkich trzech paragrafach następuje na wniosek pokrzywdzonego.

### 3.4.11. Spowodowanie szkody w systemach informatycznych – art. 268a § 1 k.k.

§ 1. *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.*

§ 2. *Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

§ 3. *Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.*

Przedmiotem ochrony jest bezpieczeństwo elektronicznie przetwarzanej informa-

417 A. Adamski, *Przestępstwa komputerowe, wyd. cyt., s. 28, 29.*

cji, baz danych i systemów informatycznych. Składa się na nie poufność, integralność i dostępność, atakże prawidłowość funkcjonowania programów komputerowych oraz konsekwentna dostępność do informacji i korzystania z nich przez osoby uprawnione. Dla zaistnienia omawianego przestępstwa nie mają znaczenia rodzaj informacji ani charakter związanych z nią dóbr i interesów. Istotą działania sprawcy jest zatem utrudnianie przetwarzania i niszczenie danych informatycznych.

Przestępstwo to związane jest z bezprawnym niszczeniem, uszkadzaniem, usuwaniem, zmienianiem lub utrudnianiem dostępu do danych informatycznych albo zakłócaniem (utrudnianie, przeszkadzanie) w przetwarzaniu lub uniemożliwianiem automatycznego przetwarzania, gromadzenia lub przekazywania takich danych.

Zakłócanie to utrudnianie, przeszkadzanie w przetwarzaniu, gromadzeniu czy przekazywaniu danych; to każda czynność, której skutkiem jest nieprawidłowy przebieg tych procesów, ich spowolnienie, zniekształcenie lub modyfikacja. Natomiast uniemożliwianie to uczynienie tych czynności niemożliwymi do ich wykonania418.

Termin przetwarzanie danych informatycznych należy rozumieć jako różnorodne operacje wykonywane na danych, takich jak utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, które wykonuje się w systemach informatycznych. Ma ono charakter automatyczny, jeśli jakaś część tego procesu odbywa się za pomocą urządzeń sterujących, bez ingerencji człowieka lub z jego ograniczonym udziałem. Natomiast gromadzenie to zbieranie danych, a przekazywanie to udostępnianie ich innej osobie. Przekazywaniem będzie zarówno transmisja danych, jak i przekazanie nośnika danych.

Karalne jest zatem modyfikowanie danych lub programów komputerowych. Różni się ono od niszczenia tym, że sprawca dokonuje nieuprawnionej ingerencji w treść danych, przykładowo poprzez dopisanie nowych danych lub zmianę istniejącego zapisu.

Zabronione jest zatem wprowadzanie zmian do zapisu istotnej informacji przechowywanej w systemie teleinformatycznym. Czyn taki polega na naruszeniu integralności danych oraz naruszeniu dóbr właściciela czy osoby uprawnionej. Związane jest to z prawem do niezakłóconego posiadania zapisu informacji, bez względu na jej rangę oraz prawem do prywatności[419].

### 3.4.12. Wyrządzenie znacznej szkody majątkowej w bazach danych – art. 268a § 2 k.k.

Analizowane przestępstwa z art. 268a k.k. mają charakter skutkowy. Skutki te według § 1 to zniszczenie, uszkodzenie, usunięcie, zmiana danych lub zakłócenie czy też uniemożliwienie ich przetwarzania, gromadzenia i przekazywania danych informatycznych. Natomiast według § 2 skutkiem jest znaczna szkoda majątkowa. Czyny mogą być popełnione zarówno przez działanie, jak i zaniechanie. Są to czyny umyślne i mogą być popełnione przez każdego sprawcę, są zatem powszechne. Czynem kwalifikowanym jest wyrządzenie znacznej szkody majątkowej, zagrożone karą pozbawienia wolności od 3 miesięcy do lat 5. Natomiast ściganie karne zarówno z § 1, jak i § 2 następuje na wniosek pokrzywdzonego.

418 M. Mozgawa (red.) *Kodeks karny,* wyd. cyt., s. 676.
419 Tamże.

### 3.4.13. Sabotaż komputerowy – art. 269 § 1 i 2 k.k. oraz 269a k.k.

#### 3.4.13.1. Sabotaż komputerowy w formie zniszczenia istotnej informacji dla obronności i bezpieczeństwa lub funkcjonowania organów administracji – art. 269 § 1 i 2 k.k.

§ 1. *Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.*

§ 2. *Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.*

Omawiane przepisy dotyczą zagadnienia sabotażu komputerowego poprzez nielegalną ingerencję w funkcjonowanie systemu informatycznego. Natomiast termin sabotaż definiowany jest jako umyślne niewypełnienie albo wypełnianie wadliwie swoich obowiązków w zamiarze wywołania dezorganizacji, strat i szkód. Sabotaż ma na celu uniemożliwienie lub utrudnienie prawidłowego funkcjonowania zakładów albo urządzeń lub instytucji o poważnym znaczeniu dla działania państwa[420]. Powyższe czyny są ścigane z urzędu.

Sabotaż komputerowy  to termin związany z systemami informatycznymi, który według raportu Komitetu Ekspertów Rady Europy stanowi „wprowadzenie, modyfikację, wymazanie lub usunięcie danych (informacji) lub programów komputerowych albo inne oddziaływanie na system komputerowy mające na celu wywołanie zakłóceń w funkcjonowaniu systemu komputerowego lub telekomunikacyjnego”[421].

Cytowana wcześniej nowelizacja Kodeksu karnego w zakresie cyberprzestępczości w ramach ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw miała na celu implementację postanowień cytowanej również Konwencji Rady Europy z 23 listopada 2001 roku o cyberprzestępczości. W ustawodawstwie polskim wprowadzono zatem nowe przestępstwo określane najczęściej jako sabotaż komputerowy czy też zakłócenie pracy systemu komputerowego. Jest to realizacja postanowień art. 5 cytowanej Konwencji, w którym nakazuje się spenalizowanie poważnego zakłócania funkcjonowania systemu teleinformatycznego przez wprowadzenie, transmisję, niszczenie, kasowanie, uszkadzanie lub zmianę danych informatycznych.

Karalność sabotażu została wzbogacona o przepisy art. 269a oraz 269b k.k., które mają chronić bezpieczeństwo elektronicznie przetwarzanej informacji, systemów komputerowych i sieci teleinformatycznej[422].

Przedmiotem ochrony z tego przepisu jest bezpieczeństwo elektroniczne przetwarzanych informacji, a także systemów komputerowych w ramach ich integralności,

420 http://pl.wikipedia.org/wiki/Sabota%C5%BC(11.02.2015)

421 Council of Europe, Computer-Related Crime: Recommendation No. R (89) 9 on computer- related crime and final report of the European Committee on Crime Problems, Strasburg 1989, s. 46-49.

422 *W. Wróbel*, *Kodeks karny. Część. szczególna. Komentarz*, t. II, Warszawa 2008, s. 1316.

a przede wszystkim obronność kraju, bezpieczeństwo w komunikacji, funkcjonowanie administracji rządowej, organów i instytucji państwowych oraz samorządowych.

Przepis określa przestępstwo sabotażu komputerowego, wyróżnionego ze względu na rodzaj danych informatycznych stanowiących przedmiot bezpośredniego oddziaływania sprawcy.

Istotą mającą wpływ na karalność sabotażu komputerowego, zgodnie z § 1 zdaniem ustawodawcy, jest uniemożliwienie automatycznego gromadzenia, przetwarzania lub przekazywania informacji mających szczególne znaczenie dla bezpieczeństwa wewnętrznego kraju, a szczególnie: obronności, bezpieczeństwa w komunikacji, funkcjonowania administracji publicznej, czy innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. *Modus operandi* sprawcy może polegać przede wszystkim na niszczeniu, uszkadzaniu, usuwaniu lub zmianie danych informatycznych. Karalne jest niszczenie, uszkadzanie, usuwanie lub zmiana danych, a także uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Czyn ten podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Natomiast w myśl § 2 takiej samej karze podlega również ten, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

### 3.4.13.2. Sabotaż komputerowy w formie utrudnienia dostępu do systemu oraz stosowanie innych destruktywnych działań – art. 269a k.k.

*Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

Przedmiotem ochrony z tego przepisu, podobnie jak w art. 269 k.k., jest bezpieczeństwo elektroniczne przetwarzanych informacji, a także systemów komputerowych.

Nowelizacja tego przepisu polegała na dodaniu terminu „utrudnienie dostępu". Zatem otrzymał on nowe brzmienie o treści: *kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

Przestępstwo sabotażu komputerowego polega na zakłócaniu lub paraliżowaniu funkcjonowania systemów teleinformatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli. Jest to kwalifikowana forma czynu z art. 268 § 2 k.k., tj. niszczenie informacji – z uwagi na wyższe zagrożenie karą. Dodać należy, że ustawodawca oprócz formy sabotażu związanej z niszczeniem informacji wyróżnia także działanie polegające na zakłócaniu lub uniemożliwianiu automatycznego gromadzenia lub przekazywania informacji.

Sabotaż komputerowy może wystąpić także w formie różnorodnych działań, a w szczególności niszczenia lub wymiany nośnika informacji, niszczenia lub uszkodzenia urządzeń służących do automatycznego przetwarzania, gromadzenia lub przesyłania informacji (art. 269 § 2 k.k.).

Przestępstwo ma charakter powszechny, może być popełnione przez każdego lecz tylko przez umyślne działanie oraz jest przestępstwem skutkowym.

### 3.4.14. Dysponowanie urządzeniami hakerskimi i zakłócanie pracy w sieci – 269b § 1 k.k.

§ 1. *Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.*

§ 2. *W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.*

Wspomniana wcześniej nowelizacja Kodeksu karnego dotyczy również art. 269b § 1 k.k., który otrzymał nowe brzmienie, a dotyczy on wytwarzania, pozyskiwania, oferowania, zbywania i posiadania tzw. narzędzi oraz urządzeń hakerskich lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a k.k.

Karalne jest również posiadanie: haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci informatycznej.

Przedmiotem ochrony we wszystkich artykułach związanych z ochroną informacji komputerowych i sabotażu komputerowego jest bezpieczeństwo elektronicznie przetwarzanych informacji i systemów komputerowych, na które składa się ich poufność, integralność i dostępność. Istotą tego przepisu jest przeciwdziałanie wszelkim zakłóceniom pracy w sieci.

Przepis ten zawiera penalizację czynności, które stanowią swoiste przygotowanie do popełnienia wymienionych typów przestępstw. Są to specjalistyczne urządzenia lub programy, kody, hasła czy inne dane umożliwiające zarówno dostęp do informacji, jak i ich przystosowane do popełnienia omawianych z zakresu sabotażu komputerowego. Specjalistyczne urządzenia do popełnienia tych przestępstw, to tzw. narzędzia hakerskie. W świetle tego przepisu obojętne jest wytworzenie tych narzędzi przez sprawcę, czy też ich zakupienie. Największe zagrożenia w tej kwestii stanowią różnego rodzaju programy szpiegowskie.

Wszystkie czynności sprawcze mogą być popełnione zarówno przez działanie, jak i zaniechanie. W zasadzie jedynie czynność wytwarzania może polegać tylko na działaniu. Natomiast wszystkie czynności sprawcze omawianej regulacji mają charakter skutkowy. Oznacza to, że w przypadku wytwarzania skutkiem jest wytworzenie zarówno nowego urządzenia, jak i programu komputerowego czy czegoś, co zostanie wymyślone czy odkryte przez uzdolnionych hakerów. Natomiast w przypadku pozyskania skutkiem będzie objęcie ich we władztwo czy uzyskanie do nich dostępu przez inną osobę. Omawiane przestępstwo ma charakter umyślny, może być popełnione przez każdego, czyli jest przestępstwem powszechnym[423]. Powyższe czyny są zagro-

423 M. Mozgawa (red.) *Kodeks karny,* wyd. cyt., s. 678-679.

żone karą pozbawienia wolności do lat 3. Ponadto sąd orzeka przepadek urządzeń czy programów. Sąd może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

### 3.5. Przestępstwa przeciwko wolności, wolności seksualnej i obyczajowości związane z manipulowaniem informacji – rozdział XXIII k.k.

Art. 190a § 1. *Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3*.

§ 2. *Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej*.

§ 3. *Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzo-nego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.*

§ 4. *Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego*

Powszechne korzystanie z różnorodnych środków komunikowania się osób, jak telefonów i poczty elektronicznej niejednokrotnie przybiera formy bezprawnego zachowania pomiędzy zainteresowanymi osobami. Dochodzi wówczas do popełnienia wielu tradycyjnych przestępstw, jak zniewaga, zniesławienie, groźby karalne, ujawnienie informacji niejawnych, danych osobowych czy rozpowszechniania zakazanych prawem treści dotyczących swobody seksualnej (pornografia) czy politycznej (faszyzm).

#### 3.5.1. Uporczywe nękanie innej osoby – *stalking* – art. 190a k.k. § 1 k.k.

Przepis art. 190a został wprowadzony przez ustawę z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny[424], która weszła w życie z dniem 6 czerwca 2011 r.

Przedmiotem ochrony działania polegającego na uporczywym nękaniu innej osoby, określane powszechnie jako *stalking* czy *cyberstalking,* jest szeroko rozumiana wolność, zarówno w aspekcie wolności „od czegoś" (strachu, nagabywania, niechcianego towarzystwa innej osoby) i wolności do zachowania swojej prywatności[425]. Przestępstwo stalkingu ma charakter powszechny, formalny i może być popełnione jedynie w zamiarze kierunkowym.

#### 3.5.2. Kradzież tożsamości – art. 190a k.k. § 2 k.k.

W art. 190a § 2 k.k. kryminalizowane jest podszywanie się pod inną osobę, **wy**korzystywanie jej wizerunku lub innych| danych osobowych w celu wyrządzenia szkody majątkowej lub osobistej. Wynika z tego, że penalizowane jest rozszerzające się zjawisko „przywłaszczenia" tożsamości pokrzywdzonego. Istotą przepisu powinno być jednak zapobiegawcze znaczenie ochrony tożsamości osoby fizycznej i ewentualnego skutku. Omawiany czyn zagrożony jest karą pozbawienia wolności do lat 3.

424 Dz. U. Nr 72, poz. 381.

425 Tamże, s. 470-471 oraz K. Garstka, P. Przygucki, *Stalking jako przestępstwo. Nowelizacja polskiego kodeksu karnego a doświadczenia prawodawstwa angielskiego*, „Wiedza Prawnicza" 2011, nr 2.

Należy uznać, że sprawca musi się podszywać pod inną, rzeczywiście istniejącą osobę, a nie postać fikcyjną. Słusznie zauważa się, że dane dotyczące osoby nieistniejącej w realnym świecie nie są danymi osobowymi w świetle ustawy, a także sprawca czynu z art. 190a § 2 k.k. musi działać w celu wyrządzenia szkody konkretnej osobie[426].

Pojęcie danych osobowych określone zostało w rozdziale 2 tej książki. Natomiast wyjaśnieniu podlega wyrażenie „podszywa się"; zgodnie z językowym znaczeniem jest to podawanie się fałszywie za kogoś innego[427].

Wyjaśnieniu podlega również określenie „wizerunek428 lub inne jej dane osobowe". Zatem należy uważać, że wizerunek jest naturalnym składnikiem danych osobowych. Ponadto, należy mieć na uwadze, że regulacje prawne dotyczące rozpowszechniania wizerunku, w sensie podobizny, zostały unormowane w art. 81 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[429]. Wizerunek podlega również ochronie na podstawie przepisów dotyczących ochrony dóbr osobistych zgodnie z art. 23 i 24 ustawy z dnia 23 kwietnia 1964 r – Kodeks cywilny[430].

Przestępstwo z art. 190a § 2 k.k. ma charakter powszechny, formalny, może być popełnione przez każdego i jest ścigane na wniosek pokrzywdzonego.

### 3.5.3. Kradzież tożsamości ze skutkiem śmiertelnym – art. 190a k.k. § 3 k.k.

W przepisie § 3 ujęto typ kwalifikowany, czyli oznaczający, że następstwem czynu określonego w § 1 jest targnięcie się pokrzywdzonego na własne życie. Wówczas sprawca podlega karze pozbawienia wolności od roku do lat 10. Przestępstwo to ma charakter powszechny, skutkowy. Jest ścigane z urzędu.

### 3.5.4 Uwodzenie i wykorzystywanie seksualne dzieci przez Internet – *grooming* – art. 200a k.k.

§ 1. *Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3.*

§ 2. *Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu*

426 M. Mozgawa (red.) *Kodeks karny,* wyd. cyt., s. 470-475.

427 Może również oznaczać: grać, grać rolę kogoś, kreować się, markować, naśladować, odgrywać, odgrywać rolę kogoś, odstawiać, odwalać, podawać się za kogoś, pozorować, pozować, pozować na kogoś, przedrzeźniać, przybierać maskę kogoś, przybrać maskę kogoś, rżnąć, stroić się w cudze piórka, strugać, stylizować się, symulować, udawać, upodabniać się, upozowywać się, urządzać maskaradę, występować jako ktoś, zgrywaćhttp://synonim.net/synonim/podszywa%C4%87+si%C4%99(18.02.2015)

428 *Słownik języka polskiego* zna dwa znaczenia terminu wizerunek: „czyjaś podobizna na rysunku, obrazie, zdjęciu itp." oraz „sposób, w jaki dana osoba lub rzecz jest postrzegana i przedstawiana" http://sjp.pwn.pl/szukaj/wizerunek(15.02.2015).

429 t. j. Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.

430 Dz. U nr 16, poz.93 z późn. zm.

*treści pornograficznych, i zmierza do jej realizacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*.

*Grooming czy child grooming* oznacza działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później seksualnie wykorzystać. Jest to także mechanizm używany, by nakłonić dziecko do prostytucji czy udziału w pornografii dziecięcej[431]. Czyny określane jako *grooming* obejmują kilka przepisów i form przestępstwa. Karze podlega ten kto dokonuje takich czynów z małoletnim poniżej lat 15 jak: zgwałcenia (art. 197 §3 p. 2 k.k.) obcowania płciowego, dopuszcza się innej czynności seksualnej czy prezentuje wykonanie takiej czynności (art. 200 §3 k.k.) albo produkuje lub utrwala treści pornograficzne za pośrednictwem systemu teleinformatycznego lub sieci teleinformatycznej, nawiązuje kontakt za pomocą wprowadzenia go w błąd, wyzyskuje błąd lub niezdolność do należytego pojmowania sytuacji albo składa propozycje obcowania płciowego lub wykonania innej czynności seksualnej lub udziału w produkcji lub utrwalaniu treści pornograficznych[432].

Do omawiane grupy przestępstw, w których istotną rolę odgrywa przekazywanie informacji lub manipulowanie nią można również zaliczyć szereg innych regulacji Kodeksu karnego, a przykładowo:

6. propagowanie pedofilii – art. 200b k.k.;
7. rozpowszechnianie, przechowywanie oraz posiadanie treści pornograficznych przedstawiających małoletniego – art. 202 § 4b k.k.;
8. nawoływanie do popełnienia występku lub przestępstwa, pochwalanie tych czynów – art. 255 k.k.
9. rozpowszechnianie lub prezentowanie treści mogących ułatwić dokonanie aktu terrorystycznego – 255a k.k.;
10. propagowanie faszyzmu – art. 256 § 1 i 2 k.k.

## 3.6. Przestępstwa przeciwko wiarygodności dokumentów – rozdział XXXIV k.k.

### 3.6.1. Pojęcie dokumentu

Dokumentem w rozumieniu prawa karnego, na podstawie definicji zawartej w art. 115 § 14 k.k. jest *każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne*[433].

431 http://pl.wikipedia.org/wiki/Child_grooming (30.01.2013).

432 Szerzej: M. Mozgawa (red.) *Kodeks karny,* wyd. cyt., s. 513-515.

433 Przytoczenie definicji dokumentu jest niezbędne, gdyż często jest przedmiotem kontrowersji. Dotyczy to nawet Prokuratury Generalnej, która stwierdziła, że Raport o likwidacji WSI nie był dokumentem, a sporządzający raport nie był urzędnikiem. W celu wyrobienia własnego zdania, warto zatem osobiście zapoznać się z tym raportem pt.: *Raport o działaniach żołnierzy i pracowników WSI oraz wojskowych jednostek organizacyjnych realizujących zadania w zakresie wywiadu i kontrwywiadu wojskowego przed wejściem w życie ustawy z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych w zakresie określonym w art. 67. ust. 1 pkt 1-10 ustawy z dnia 9 czerwca 2006 r. „Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz ustawę o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego" oraz o innych działaniach wykraczających poza sprawy obronności państwa i*

Zagadnieniom związanym z dokumentami należy poświęcić więcej uwagi, gdyż obok kartki papieru, taśmy magnetofonowej, telefonu, innego elektronicznego środka mobilnego, komputera, pendrivea, taśmy filmowej, są one nośnikami informacji, a ze względu na zapisaną treść mogą stanowić dowód prawa. Skopiowanie zapisu informacji (przepisanie, wykonanie kserokopii lub fotokopii z nośnika elektronicznego), jak wykazuje praktyka śledcza, w trakcie tych czynności możliwe jest dokonanie fałszerstwa dokumentu, również na nośniku elektronicznym.

Przedmiotem ochrony w tym rozdziale są: wiarygodność dokumentów, zaufanie obywateli do autentyczności dokumentów wystawianych przez właściwych urzędników. Zatem powinna istnieć pewność, że informacje zawarte w dokumentach są autentyczne.

Termin dokument pojawia się w wielu artykułach kodeksu karnego, a przykładowo w takich art. jak: 271§ 1, 272, 273, 274, 275 § 1 i 2, 276, 297 § 1, 303 § 1 i 310 § 1 i 3 k.k. Natomiast terminy informacja i dokument w art. 311 k.k.

Kodeks karny traktuje na jednej płaszczyźnie dokumenty urzędowe i dokumenty prywatne. To samo dotyczy dokumentów krajowych i zagranicznych[434]. Omawianej problematyce wielu autorów poświęca dużo uwagi, gdyż dokument jest jednym ze źródeł dowodowych[435].

### 3.6.2. Fałszerstwo dokumentu i używanie za dokument autentyczny – art. 270 § 1 k.k.

§ 1. *Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5.*

§ 2. *Tej samej karze podlega, kto wypełnia blankiet, zaopatrzony cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo takiego dokumentu używa.*

§ 2a. *W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§ 3. *Kto czyni przygotowania do przestępstwa określonego w § 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*.

Nielegalne angażowanie profesjonalistów i dostęp do najnowszych technologii umożliwia ingerencję, podrabianie i przerabianie wszelkich dokumentów, także w formie zapisu elektromagnetycznego, tj. odczytywanego i drukowanego przez specjalistyczne urządzenia. Podrabiane są również dobrze zabezpieczone znaki pieniężne. Ma to szczególne znaczenie w świetle znanej w kryminalistyce prawidłowości, że fałszowanie dokumentów publicznych (tożsamości czy finansowych) to czynności przygotowawcze do oszustwa. Szczególnie niebezpieczne jest fałszerstwo intelektualne[436].Planując oszustwo, przestępcy zaopatrują się w kradzione dokumenty tożsamości, inne fałszują wyrabiając na fikcyjne nazwisko. Odpowiednie zapisy mogą być natomiast poświadczone autentycznymi lub podrobionymi podpisami i stemplami

*bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polskiej* http://www.iniejawna.pl/pomoce/przyc_pom/raport.pdf(18.06.2014)

434 Uchwała SN z dn. 4 VI 1973 r. (VI KZP 8/73, OSNKW 1973, nr 9, poz. 103); uchwala SN z dnia 12 III 1996 r. (I KZP 39/95, OSN 1996, nr 3-4, poz. 17).

435 Przykładowo, A. Marek, *Kodeks karny. Komentarz*, Warszawa 2004, s. 555-564.

436 J.W. Wójcik, *Fałszerstwa dokumentów publicznych*, Warszawa 2005, s. 270 i n.

urzędowymi na rzecz fikcyjnej osoby. Także są podrabiane podpisy cyfrowe i używane jako autentyczne.

Kodeks karny określa w konkretnych regulacjach: podrabianie, przerabianie i używanie za autentyczne dokumentów w przestępstwie zwanym fałszem materialnym dokumentu. Dobrem chronionym jest bezpieczeństwo obrotu prawnego opierającego się na zaufaniu do wszelkiego rodzaju dokumentów, a także prawa i stosunki prawne, których istnienie lub nieistnienie dany dokument stwierdza.

Dokument jako nośnik wszelkiego rodzaju informacji wykorzystywany jest do różnego rodzaju działań sprzecznych z prawem. Wymaga zatem na omówienie kilu pojęć.

Podrabianie dokumentu polega na nadawaniu jakiemuś przedmiotowi pozoru dokumentu w całości lub w jakiejś jego części. Nie podlega kwestii, że użycie nielegalnych sposobów celem uzyskania dokumentu nie jest równoznaczne z jego podrobieniem. Dokument jest podrobiony wówczas, gdy pochodzi od osoby, w której imieniu został sporządzony. Natomiast podpisanie innej osoby jej nazwiskiem na dokumencie mającym znaczenie prawne, nawet wówczas, gdy wyrazi ona na to zgodę, wypełnia znamię podrabiania jako przestępstwa fałszerstwa dokumentu[437].

Przerabianie dokumentu polega na dokonywaniu zmian w tekście istniejącego dokumentu i czynieniu go w ten sposób nieprawdziwym poprzez różnorodne dopiski, usuwanie fragmentów. Dla stwierdzenia znamienia przerabiania dokumentu nie jest istotne, czy dokonane w nim zmiany odpowiadały rzeczywistości. Nie można w związku z tym poprawiać np. omyłkowego zapisu daty czy kwoty. Okoliczność ta może być jedynie brana pod uwagę przy ocenie stopnia społecznej szkodliwości i może oddziaływać na wymiar kary.

ałszerstwo intelektualne polega na bezprawnym wystawieniu przez uprawnioną instytucję dokumentu potwierdzającego nieprawdę, jak np. fałszywe dane personalne.

Przestępstwo podrobienia lub przerobienia dokumentu dokonane jest wówczas, gdy podjęto czynności pozorujące jego autentyczność oraz przy użyciu go za autentyczny, tj. przy każdym przedstawieniu dokumentu, gdy ma on znaczenie prawne.

Sprawca, który podrobił lub przerobił dokument, a następnie posłużył się nim dla doprowadzenia innej osoby do niekorzystnego rozporządzenia mieniem, dopuszcza się dwóch przestępstw: fałszerstwa dokumentu z art. 270 § 1 k.k. oraz oszustwa z art. 286 § 1 k.k.

Uzyskany w ten sposób dokument ma wszelkie cechy dokumentu autentycznego i może być podstawą do wydania legalnych dokumentów przez instytucje, władze samorządowe czy administracyjne oraz służyć do zawierania umów o charakterze prawno-finansowym, transakcji handlowych i usługowych, przykładowo: wyrobienia zezwolenia na działalność gospodarczą, uzyskanie numeru Regonu, wypożyczenie samochodu, otwarcie rachunku bankowego, uzyskanie karty płatniczej czy uzyskanie kredytu bankowego, a także uzyskanie informacji.

Nie podlega kwestii, że same druki lub formularze nie stanowią dokumentu. Nabierają takiego charakteru wtedy, gdy zostały wypełnione treścią, z którą związane jest prawo albo gdy ich treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne[438]. Listy (spisy członków) i pisma ewidencyjne organizacji społecznej lub politycznej mogą mieć walor dokumentu w wypadku, gdy dane w nich

437 Wyrok SN z dnia 25 X 1979 r., II KR 10/79, (OSNPG 1980, nr 11, poz. 127).

438 Por. wyrok Sądu Najwyższego z dnia 4 VI 1974 r. (VI KZP 8/73, OSN 1973, nr 9, poz. 103).

zawarte albo one same stanowią podstawę do ustalenia istnienia stosunku prawnego lub okoliczności mającej znaczenie prawne[439].

Bardziej wyrafinowana forma fałszerstwa może polegać na wprowadzeniu do pamięci komputera informacji w zakresie nieprawdziwych danych, które następnie są powielane. Oznacza to, że znajdują się one zarówno w przekazywanych informacjach, jak i w każdym kolejnym wydruku obejmującym te dane.

Zastosowanie komputera powoduje dużą atrakcyjność sfałszowanego dokumentu pod względem techniki wykonania, wydajności i mniejszych możliwości wykrywczych. W związku z tym fałszerze rezygnują ze stosowanych dotychczas metod kserograficznych a posługują się komputerami i skanerami. Daje to szeroki zakres możliwości w postaci produkcji i rozpowszechniania fikcyjnych lub podrabianych dokumentów, takich jak np.: pieczątki, stemple bankowe, dokumenty finansowe, polecenia przelewu czy wpłaty.

Fałszerstwo komputerowe jest specyficzną formą fałszerstwa i należy je rozpatrywać w trzech aspektach, a mianowicie jako:

1. komputerowe fałszerstwo dokumentów, w którym komputer, oprogramowanie i peryferia są narzędziem do fałszowania dokumentów w tradycyjnym tego słowa znaczeniu;
2. fałszerstwo dokumentów elektronicznych, polegające na wprowadzaniu zmian w utworzonych i funkcjonujących dokumentach elektronicznych czy bazach danych, zawierających informacje dotyczące np. ksiąg handlowych i podatkowych, dokumentów magazynowych, kartotek pracowników firmy, list płac, ewidencji pojazdów, danych o klientach banków i ich rachunkach itp.
3. fałszerstwo zapisu na innych elektronicznych nośnikach informacji dotyczących na przykład karty identyfikacyjnej czy karty płatniczej.
4. Fałszerstwo dokumentu określane jest jako fałszerstwo materialne, które dzieli się na podrabianie i przerabianie dokumentów. Ma ono charakter powszechny. Może być dokonane umyślnie w zamiarze bezpośrednim. Natomiast przy użyciu spreparowanego dokumentu w taki sposób, aby był rozpatrywany jako autentyczny dopuszczalny jest zamiar ewentualny wówczas, gdy sprawca przewiduje i godzi się na to, że dokument, którego użył nie jest autentyczny. Regulacje karnoprawne nie przeprowadzają rozróżnienia między dokumentami prywatnymi a publicznymi, ani też między zagranicznymi a krajowymi; udziela im jednakowej ochrony prawnej. Fałszowany może być zarówno oryginał, jak i odpis dokumentu lub wyciąg z niego, jeśli taki odpis lub wyciąg ma cechy dokumentu. Pod omawiane pojęcie fałszowania dokumentów podpada również fałszowanie papierów wartościowych, jeśli papiery te są imienne, a nie na okaziciela.

Sprawca, który sfałszował dokument bez względu na jego postać np. wydruk komputerowy będący, przykładowo, dokumentem księgowym lub manipulował elektronicznym zapisem informacji, przez co doszło do naruszenia autentyczności danych będących np. zapisem księgowym, zawierającym wykazy mające znaczenie prawne, kartoteki klientów itp., a przechowywanym na dysku twardym, bazie danych czy innych nośnikach teleinformatycznych, w celu użycia za autentyczny przerobił lub podrobił dokument lub takiego używa jako autentyczny, podlega odpowiedzialności karnej z art. 270 § 1 kk, a jego czyn zagrożony

439 Por. postanowienie Sądu Najwyższego z dn. 10 X 1991 r. (I KZP 27/91, OSN KW 1992, nr l, poz. 7).

jest grzywną, karą ograniczenia wolności albo karą pozbawienia wolności od 3 miesięcy do lat 5.

### 3.6.3. Fałszerstwo dokumentu w formie wypełnienia blankietu z cudzym podpisem i użycie tego dokumentu – art. 270 § 2 k.k.

Wypełnienie jakiegokolwiek blankietu i zaopatrzenie go cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo użycie takiego dokumentu jako autentycznego zagrożone jest odpowiedzialnością karną w formie grzywny, karą ograniczenia wolności albo karą pozbawienia wolności od 3 miesięcy do lat 5.

### 3.6.4. Czynności przygotowawcze do fałszerstwa dokumentu – art. 270 § 3 k.k.

Czynności przygotowawcze do popełnienia przestępstwa fałszerstwa dokumentu, a szczególnie ich forma i zakres uzależnione są od rodzaju zaplanowanego przestępstwa, czyli rodzaju dokumentu, który ma być sfałszowany. Może to być zarówno dokument papierowy lub elektroniczny. Istotne jest aby fałszowany przedmiot wyczerpywał definicję dokumentu. Wspomniane czynności przygotowawcze zagrożone są grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat 2.

### 3.6.5. Poświadczenie nieprawdy przez funkcjonariusza publicznego – art. 271 § 1 i 2 k.k.

§ 1. *Funkcjonariusz publiczny lub inna osoba uprawniona do wystawienia dokumentu, która poświadcza w nim nieprawdę co do okoliczności mającej znaczenie prawne, podlega karze pozbawienia wolności od 3 miesięcy do lat 5*.

§ 2. *W wypadku mniejszej wagi, sprawca podlega grzywnie albo karze ograniczenia wolności.*

§ 3. *Jeżeli sprawca dopuszcza się czynu określonego w § 1 w celu osiągnięcia korzyści majątkowej lub osobistej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.*

Działanie sprawcy polega na poświadczeniu w formie stwierdzenia czy poręczenia prawdziwości, wiarygodności czy tożsamości osoby lub rzeczy w wystawianym dokumencie. Jest to wprowadzenie do tego dokumentu nieprawdziwych danych co do okoliczności mającej znaczenie prawne. Takie działanie określa się w języku prawniczym jako fałsz intelektualny. Wystawiony przez sprawcę dokument wydaje się autentyczny, pochodzi bowiem od osoby, instytucji czy urzędu, który wystawił w majestacie swoich uprawnień. Jednakże treść dokumentu, jaką mu nadał wystawiający, nie odpowiada rzeczywistości.

O. Górniok trafnie stwierdza, że istotą tego przestępstwa jest fakt, aby poświadczenie nieprawdy odnosiło się do okoliczności mającej znaczenie prawne. Natomiast autor poświadczenia musi być uprawniony do potwierdzania takich okoliczności. Obojętne jest, czy poświadczenie danej okoliczności, tj. poświadczenie nieprawdy ma postać całego, samoistnego dokumentu czy też dotyczy jakiegoś jego fragmentu mającego znaczenie prawne. Niezbędne jest zaznaczenie, że dokonanie przestępstwa następuje dopiero z chwilą wydania dokumentu, a zatem stworzenia, przynajmniej abstrakcyjnej możliwości zrobienia z niego użytku.

Omawiane przestępstwo ma szczególną wymowę. Związana z nim jest dezinformacja organu państwowego przez dostarczenie organom państwowym fałszywych dokumentów, co jest ścigane z art. 132 k.k.

Strona podmiotowa fałszu intelektualnego, czyli przestępstwa z art. 271 k.k. polega na umyślności. Jednakże nie jest przestępstwem z tego artykułu poświadczenie nieprawdy przez pomyłkę czy poprzez podstępne wprowadzenie w błąd (art. 272 k.k.) wystawiającego dokument, nawet wówczas, gdy można byłoby zarzucić mu działanie z lekkomyślności lub niedbalstwa. Wystawca dokumentu, będący funkcjonariuszem publicznym, może jednak być pociągnięty do ewentualnej odpowiedzialność z art. 231 § 3 k.k., jeżeli spełnione zostały rygory tego przepisu[440].

Z treści cytowanego poniżej wyroku można wnosić, iż zwykłymi uczestnikami obrotu prawnego są tylko osoby będące stronami nawiązywanych w tym obrocie stosunków prawnych, a zatem: *Według ogólnej prezentowanej w dotychczasowym orzecznictwie wykładni sprawcą przestępstwa poświadczania nieprawdy może być tylko ta osoba, która czyni to w ramach uprawnień szczególnych związanych z przedmiotem i zakresem działania służbowego (np. lekarz wydaje zaświadczenie o stanie zdrowia pacjenta, upoważniony pracownik zakładu wydaje zaświadczenie o wysokości zarobków danego pracownika, magazynier, kasjer itp.), nie zaś osoby będące zwykłymi uczestnikami powszechnego obrotu prawnego. Skoro przepis przewiduje analogiczną odpowiedzialność funkcjonariusza publicznego, jak też osoby upoważnionej do wystawiania dokumentu, to upoważnienie takie nie może wynikać jedynie z ogólnego, przysługującego każdemu prawa uczestnictwa w obrocie prawnym*[441].

Przestępstwo popełnia funkcjonariusz publiczny lub inna osoba uprawniona do wystawienia dokumentu, która poświadcza w nim nieprawdę co do okoliczności mającej znaczenie prawne, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Natomiast w wypadku mniejszej wagi, to uprzywilejowany typ przestępstwa i zgodnie z § 2sprawca podlega grzywnie albo karze ograniczenia wolności.

### 3.6.6. Poświadczenie nieprawdy przez funkcjonariusza publicznego w celu osiągnięcia korzyści – art. 271 § 3 k.k.

Jeżeli sprawca działa w celu osiągnięcia korzyści majątkowej lub osobistej, to popełnia kwalifikowany typ przestępstwa i zgodnie z § 3podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

### 3.6.7. Wyłudzenie poświadczenia nieprawdy, czyli fałsz pośredni – art. 272 k.k.

*Kto wyłudza poświadczenie nieprawdy przez podstępne wprowadzenie w błąd funkcjonariusza publicznego lub innej osoby upoważnionej do wystawienia dokumentu, podlega karze pozbawienia wolności do lat 3*.

Przestępstwo to polega na podstępnym wprowadzaniu w błąd i zagrożone jest karą pozbawienia wolności do lat 3. Sprawcą tego przestępstwa również może być każdy

440 L. Gardocki, *Prawo karne*, Warszawa 2003, s. 303.

441 Wyrok SA w Łodzi z dnia 30 X 1996 r., II A KA 59/96. Stanowisko to potwierdza również Sąd Najwyższy, który określił, że „upoważnienie", w omawianym przepisie, musi odnosić się do poświadczania jakichś okoliczności mających znaczenie prawne, a nie do „oświadczania" o nich we własnym interesie. Wyrok z dnia 24 X 1996 r., V KKN M/96, OSNKW 1997, nr 1-2, poz. 8 oraz uchwała z dnia 12 III 199G r., OSNKW 1996, nr 3-4, poz. 17.

kto wyłudził, zarówno w sposób podstępny, jak i wypraszający poświadczenie nieprawdy poprzez podstępne wprowadzenie w błąd. Zachodzi wówczas, gdy sprawca działał umyślnie i w zamiarze bezpośrednim. Jeżeli jednak poświadczający nieprawdę działał w dobrej wierze, choć był funkcjonariuszem publicznym, który nie dopełnił wymaganego sprawdzenia poświadczanych okoliczności, może on ponosić odpowiedzialność karną na podstawie art. 231 k.k., tj. za przekroczenie uprawnień lub niedopełnienie obowiązków.

Nie budzi wątpliwości stwierdzenie, że jest to przestępstwo skutkowe. O. Górniok wyjaśnia, że *jego dokonanie następuje wraz z uzyskaniem przez wprowadzającego w błąd poświadczenia nieprawdy. Podstępne zabiegi zmierzające do tego stanowią usiłowanie, które w zależności od użytych przez sprawcę środków może być uznane za nieudolne*[442]. Inny pogląd prezentuje J. Wojciechowski. Zdaniem tego autora przestępstwo to jest dokonane już wówczas, gdy sprawca podejmuje działania zmierzające do uzyskania poświadczenia nieprawdy[443].

### 3.6.8. Używanie dokumentu poświadczającego nieprawdę – art. 273 k.k.

*Kto używa dokumentu określonego w art. 271 lub 272, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Przedmiotem czynu jest użycie dokumentu zawierającego poświadczenie nieprawdy. Przestępstwo to ma miejsce przy każdym akcie przedstawienia takiego dokumentu osobie lub instytucji, dla której jego treść musi być bezpośrednio związana z wykorzystaniem znaczenia prawnego i dowodowego. Ujęte jest łączne używanie dokumentu, w którym funkcjonariusz publiczny lub osoba uprawniona do jego wystawienia poświadczyła nieprawdę, a także używanie dokumentu, w którym poświadczenie nieprawdy zostało przez podstępne wprowadzenie w błąd tych osób wyłudzone. Sprawcą przestępstwa może być każdy, kto działał umyślnie, czyli używał dokumentu wyłudzonego, w tym także osoba, która poświadczenie nieprawdy w dokumencie podstępnie wyłudziła. Wspomniany czyn zagrożony jest grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat 2[444].

442 O. Górniok, S. Hoc, M. Kalitowski, S. M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny. Komentarz*, Gdańsk 2002, s. 1157.

443 J. Wojciechowski, *Kodeks karny. Komentarz. Orzecznictwo*, Warszawa 1997, s. 477.

444 W uzupełnieniu omawianej problematyki warto dodać, że w polskim ustawodawstwie istnieje jeden przepis zezwalający na posługiwanie się fikcyjnymi dokumentami tożsamości, czyli tzw. dokumentami legalizacyjnymi. Dotyczy on sytuacji wyjątkowych, tj. wystawiania i posługiwania się dokumentami legalizacyjnymi używanymi przez policję i służby specjalne podczas tajnych operacji (tzw. „pod przykryciem"). Najczęściej są to dowody osobiste, legitymacje czy paszporty wystawione na fikcyjne dane personalne, które mają pomóc w ukryciu tożsamości funkcjonariuszy w celu ich ochrony. Dotyczy to wykonywania czynności operacyjno-rozpoznawczych, w których policjanci mogą posługiwać się dokumentami, uniemożliwiającymi ustalenie autentycznych danych identyfikujących oraz środków, którymi posługują się przy wykonywaniu zadań służbowych. Zatem organy administracji rządowej i organy samorządu terytorialnego obowiązane są do udzielania policji, w granicach swojej właściwości, niezbędnej pomocy w zakresie wydawania i zabezpieczania dokumentów legalizacyjnych. W związku z tym art. 20a ust. 3a ustawy z dnia 6 kwietnia 1990 roku o Policji stanowi, że:

1. ie popełnia przestępstwa: kto poleca sporządzenie lub kieruje sporządzeniem dokumentów legalizacyjnych,
2. kto sporządza dokumenty legalizacyjne,
3. kto udziela pomocy w sporządzeniu dokumentów legalizacyjnych,
4. policjant lub inna upoważniona osoba wymieniona, jeżeli dokumentami legalizacyjnymi posługują się przy wykonywaniu czynności operacyjno-rozpoznawczych.

### 3.6.9. Zbycie własnego lub cudzego dokumentu stwierdzającego tożsamość – art. 274 k.k.

*Kto zbywa własny lub cudzy dokument stwierdzający tożsamość, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Przedmiotem ochrony jest wiarygodność dokumentów stwierdzających tożsamość danej osoby. Ustawa nie wymienia dokumentu z nazwy, a czyn ma charakter umyślny i powszechny.

Sprawcą tego przestępstwa może być każdy, nie tylko obywatel polski, na którym ciąży ustawowy obowiązek posiadania dokumentu poświadczającego tożsamość. Zatem strona podmiotowa obejmuje umyślność w obu postaciach. Działanie polega na zbyciu dokumentu stwierdzającego tożsamość zarówno własnego, jak i cudzego np. dowodu osobistego, paszportu, książeczki wojskowej czy prawa jazdy.

Istotne jest zachowanie sprawcy, które przepis określa jako zbycie. Ma ono szerszy zasięg znaczeniowy od sprzedaży. Zdaniem M. Bojarskiego i W. Radeckiego odnosi się bowiem do wszelkich zachowań polegających na przeniesieniu władania jakimś przedmiotem na inną osobę, a także nieodpłatnie albo za świadczenie wzajemne nie polegające na uiszczeniu opłaty czy zamianie.

Nie jest konieczne, aby przy bycie tego przestępstwa, nastąpiło przekazanie dokumentu. Przestępstwo to jest bowiem już dokonane w momencie zawarcia umowy czy dojścia do porozumienia co do przekazania dokumentu.

Wspomniany czyn zagrożony jest grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat 2.

### 3.6.10. Posługiwanie się, kradzież lub przywłaszczenie cudzego dokumentu tożsamości – art. 275 k.k.

§ 1. *Kto posługuje się dokumentem stwierdzającym tożsamość innej osoby albo jej prawa majątkowe lub dokument taki kradnie lub go przywłaszcza, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§ 2. *Tej samej karze podlega, kto bezprawnie przewozi, przenosi lub przesyła za granicę dokument stwierdzający tożsamość innej osoby albo jej prawa majątkowe.*

Każdy może być sprawcą tego przestępstwa. Natomiast strona podmiotowa obejmuje umyślność tylko w zamiarze bezpośrednim. Ustawodawca, mając na względzie skalę tego rodzaju czynów, a szczególnie ich skutki w obrocie prawnym, gospodarczym i finansowym penalizuje takie zachowania. Zatem przedmiotem czynu są dokumenty stwierdzające tożsamość innej osoby lub jej prawa majątkowe. Wymienia się trzy, najczęściej rozpoznawane w działaniu sprawców znamiona czasownikowe, a więc: *posługuje się, kradnie, przywłaszcza*[445].

Odpowiedzialność z tego artykułu dotyczy także dokumentów stwierdzających prawa majątkowe innej osoby. Natomiast ochrona dokumentów dotyczy identycznego zakresu i zawarta jest w art. 275 § 2 k.k., który penalizuje bezprawne przewożenie, przenoszenie lub wykonywanie innych czynności przez sprawcę, w wyniku których wymienione dokumenty, znalazły się za granicą. Ponadto, dokument nie musi znaleźć się w wyniku tych działań za granicą, gdyż dla dokonania tego przestępstwa wystarczy samo podjęcie powyższych czynności.

Czyny z art.275 § 1 i 2 k.k. zagrożone są grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat 2.

445 O. Górniok i inni, wyd. cyt., s 1159.

### 3.6.11. Zniszczenie lub pozbawienie mocy dowodowej dokumentu – art. 276 k.k.

*Kto niszczy, uszkadza, czyni bezużytecznym, ukrywa lub usuwa dokument, którym nie ma prawa wyłącznie rozporządzać, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Karalne jest niszczenie, uszkadzanie, ukrywanie, czynienie bezużytecznym lub usuwanie dokumentu, którym sprawca nie ma prawa wyłącznie rozporządzać. Jednakże na podstawie wyroku Sądu Najwyższego można stwierdzić, że nie stanowi przestępstwa z art. 276 k.k. zniszczenie własnego dowodu osobistego[446].

Każdy może być sprawcą tego przestępstwa, które polega wyłącznie na działaniu umyślnym. Przedmiotem czynu jest dokument, którego sprawca jest czasowym i nieuprawnionym posiadaczem. Nie ma prawa nim rozporządzać, lecz jednak niszczy go, uszkadza, czyni bezużytecznym, ukrywa lub usuwa.

Warto podkreślić, że znaczenie określenia bezprawne, w kontekście tego przepisu, jest takie zachowanie sprawcy, gdy postępuje on z dokumentem wbrew decyzji czy woli właściciela dokumentu albo z naruszeniem zakazu administracyjnego zawartego w ustawie. Warto wskazać, że w interpretacji tego przepisu O. Górniok określa, że:[447]

1. w sytuacji, gdy dla sprawcy wynikają z posiadanego dokumentu pewne prawa lub obowiązki, a ich realizacja zależy tylko od niego, ma on wówczas prawo do wyłącznego rozporządzenia dokumentem;
2. jeżeli jednak prócz sprawcy dokument nadaje również prawa innym osobom, nie może nim wyłącznie rozporządzać;
3. w sytuacji, gdy dokumenty cudze zostaną komuś powierzone na przechowanie, nie ma on w ogóle prawa do rozporządzania nimi;
4. w sytuacji, gdy dokumenty sporządzono w większej ilości egzemplarzy, dla wszystkich osób, których praw dotyczą, każda z nich ma prawo swoim egzemplarzem dokumentu rozporządzać.

Sprawca, który sfałszował wydruk komputerowy lub manipulował elektronicznym zapisem informacji przez co doszło do naruszenia autentyczności danych będących przykładowo dokumentem księgowym, zawierającym wykazy, czy informacje mające znaczenie prawne, kartoteki klientów itp., a przechowywane na dysku twardym albo na innym nośniku informacji lub takiego dokumentu jako autentycznego używa, podlega odpowiedzialności karnej. Takie działanie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

## 3.7. Inne kodeksowe przestępstwa związane z przekazem fałszywych lub podejrzanych informacji poprzez systemy informatyczne oraz w inny sposób.

Opierając się na typologii omawianych czynów według terminologii cytowanej Konwencji Rady Europy o cyberprzestępczości dodać należy, iż w dobie powszechnej komputeryzacji trzeba wziąć pod uwagę możliwość szerszego zakresu przestępstw komputerowych, w których przekazywanie informacji występuje jako istotny zapis w systemie informatycznym. Zatem zgodnie z art. 115 § 14 k.k. taki zapis jest dokumen-

446 Wyrok SN z 8. l. 1975 r., Rw 644/74, OSNKW 1975, Nr 5, poz. 65.

447 O. Górniok i inni, wyd. cyt., s. 1161.

tem. W związku z tym należy mieć na uwadze przestępstwa przeciwko wiarygodności dokumentów, obrotowi gospodarczemu i finansowemu oraz zawartych w nich informacjach, a w szczególności:

1. finansowanie terroryzmu – gromadzenie, przekazanie lub oferowanie środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innego mienia ruchomego lub nieruchomości w celu sfinansowania przestępstwa o charakterze terrorystycznym (określonego w art. 115 § 20 k.k.) – art. 165a k.k.,
2. karalna niegospodarność – nadużycie zaufania poprzez działanie na niekorzyść spółki, nadużycie uprawnień lub niedopełnienie obowiązków przez kierownictwo – art. 296 k.k.,
3. oszustwo kredytowe – przedkładanie fałszywych lub nierzetelnych dokumentów w celu wyłudzenia kredytu, pożyczki, poręczenia, gwarancji, akredytywy dotacji subwencji czy zamówienia publicznego – art. 297 k.k.,
4. oszustwo ubezpieczeniowe – przedkładanie sfałszowanych dokumentów z nieprawdziwych czynności w celu uzyskania odszkodowania – art. 298 k.k.,
5. pranie pieniędzy – obrót wartościami uzyskanymi w wyniku przestępstwa lub z działalności w ramach szarej strefy – art. 299 k.k.,
6. przestępstwa na szkodę wierzycieli – działania w celu udaremnienia lub ograniczenia zaspokojenia należności przez wierzycieli, np. sprzedaż majątku, doprowadzanie do upadłości, tworzenie nowej spółki – art. 300, 301, 302 k.k.,
7. nierzetelne prowadzenie dokumentacji działalności gospodarczej – nieprowadzenie dokumentacji, jej nierzetelność lub niezgodność z prawdą m.in. w ramach kreatywnej księgowości – art. 303 k.k.,
8. rozpowszechnianie nieprawdziwych informacji w obrocie papierów wartościowych lub ich ukrywanie przez emitentów papierów wartościowych – art. 311 k.k.,
9. fałszowanie znaków wartościowych – art. 313 k.k.,

### 3.8. Inne pozakodeksowe przepisy karne

Kolejne regulacje prawne, które mogą mieć związek z cyberprzestępstwami polegającymi na wymianie informacji, szczególnie chronionych, wymagają analizy wielu ustaw, w odrębnych publikacjach. Zawierają one przepisy karne dotyczące cyberprzestępczości i ochrony informacji, przykładowo z:

1. ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[448].
2. ustawy zdnia 29 sierpnia 1997 r. o ochronie danych osobowych[449],
3. ustawy z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej[450],
4. ustawy z dnia 27 lipca 2001 r. o ochronie baz danych[451],
5. ustawy z dnia 18 września 2001 r. o podpisie elektronicznym[452],
6. ustawy z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym[453].

448 Dz. U. z 1993 r., nr 47, poz. 211 ze zm.
449 Dz. U. z 2002 r. Nr 101,
450 Dz. U. z 2003 r. nr 119, poz. 1117.
451 Dz. U. z 2001 r, nr 128, poz.1402.
452 Dz. U. *2001* nr 130 poz. 1450.
453 Dz. U. z 2002 r. Nr 126, poz. 1068;

7. ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[454]
8. ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[455], które dotyczą infrastruktury krytycznej, jak: systemy zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej. Ma na celu również ochronę baz danych.
9. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[456],

Powyższe, a także kolejne przepisy prawa mają istotne znaczenie profilaktyczne i represyjne. Zagadnienia te szeroko omawiane są w literaturze przedmiotu[457].

454 Dz. U. z 2002 r. Nr 144, poz. 1204,

455 Dz. U. Nr 89, poz. 590, ze zm.

456 Dz. U. Nr 182, poz. 1228 ze zm..

457 Szerzej np.: J.W. Wójcik, *Cyberprzestępczość. Wybrane zagadnienia kryminologiczne i prawne*, Problemy Prawa i Administracji, nr 1/2011,oraz tegoż autora Kryminologia. Współczesne aspekty, Warszawa 2014, s.137-187.

# Rozdział 10

# Kryminologiczne, kryminalistyczne i prawne aspekty ochrony informacji oraz bezpieczeństwa w biznesie – podsumowanie

## 1. Znaczenie informacji w biznesie

Pojęcie informacji jest jednym z podstawowych pojęć we współczesnym świecie, nauce, we wszystkich dziedzinach badań podstawowych i stosowanych oraz w każdej dziedzinie działalności człowieka. Praktyka potwierdza, że na tle współczesnego rozwoju cywilizacji, a szczególnie techniki, nie istnieje jedna, uznana powszechnie, zadawalająca definicja informacji. Co więcej, w badaniach naukowych często rezygnuje się z definiowania tego pojęcia poprzestając bądź na jego intuicyjnym, potocznym rozumieniu, bądź uzupełniając je określeniami pomocniczymi. Znane są różnorodne klasyfikacje informacji, a żadna nie neguje faktu, iż jest ona bezwzględnie konieczna do funkcjonowania w obecnym świecie. Wielość definicji jest odzwierciedleniem złożonych poglądów na ten istotny termin. Popularne powiedzenie głosi, że kto ma informacje ten ma władzę. Im bardziej wiarygodna informacja i im więcej jej jest, tym bardziej wzrastają szanse na optymalną decyzję w każdej dziedzinie zarządzania czy gospodarki. Szybki dostęp do informacji może stać się potężną bronią dla wywiadowcy czy szpiega gospodarczego.

Panuje powszechne przekonanie, że informacja jest jednym z najcenniejszych towarów jako kluczowy element biznesu. Z tego względu informacji nie należy traktować jako zasobu bazy danych, gdyż jest szczególnym zasobem stanowiącym aktualną podstawę sukcesów podjętych zmian. Stanowi bowiem podstawę do oceny stosowanej strategii działania osoby fizycznej czy przedsiębiorstwa. Nic więc dziwnego, że współczesny świat dąży do maksymalnego zdobywania, przetwarzania i zbywania informacji. Działalność ta, nie zawsze jest zgodna z prawem, a jedną z jej zalet w określonych środowiskach są kolosalne zyski.

Nowoczesna technologia dostępna w każdym zakątku globu powoduje, że szybki dostęp do informacji może być potężną bronią. Każdy ma prawo do informacji, a słowo to budzi istotne zainteresowanie. Jako termin interdyscyplinarny ma kilka znaczeń i definiowany jest różnie w różnych dziedzinach nauki. Informacja pochodzi od łacińskiego *informatio* – wyobrażenie, pomysł, przedstawienie, wizerunek oraz *formatio* – kształt, zarys; *informare* – kształtować, przedstawiać. Termin ten najogólniej oznacza właściwość pewnych obiektów, relację między elementami

zbiorów pewnych obiektów, której istotą jest zmniejszanie niepewności (nieokreśloności)[458]. Ponadto:

- informacją jest wiadomość lub określona suma wiadomości o sytuacjach, stanach rzeczy, wydarzeniach i osobach. Może być przedstawiona w formie pisemnej, fonicznej, wizualnej i każdej innej możliwej do odbioru przy pomocy zmysłów[459];
- informacja to każdy czynnik, dzięki któremu człowiek lub urządzenia automatyczne mogą przeprowadzić bardziej sprawne, celowe działanie; powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, pouczenie, a także komórka w urzędzie udzielająca informacji[460].

Uprzedzając wszelkie definicje i klasyfikacje warto zaznaczyć, co nie każdy zainteresowany dostrzega, że z prawnego punktu widzenia regulatorem jest właśnie prawo, które z jednej strony ułatwia dostęp do informacji, a w niektórych postanowieniach wyraźnie go utrudnia. Zatem mamy informacje jawne i niejawne, czyli:

1. informacje mogą zawierać treści powszechnie dostępne, a każdy ma możliwość prowadzenia interesujących go badań w ramach białego wywiadu, który jest stanowi 80-90% zbieranych danych. To informacje jawne, ich otwartym źródłem jest przede wszystkim Internet (a w szczególności media społecznościowe), odgrywające istotną rolę nawet w służbach specjalnych[461]. Przy czym wiadomo, że analizowaniem informacji z tych źródeł zajmują się nie tylko agendy państwowe, lecz również przestępcy, czyli krąg korzystających jest nieograniczony;
2. niektóre informacje są dostępne według regulacji ustawowych, czyli określony jest indeks osób uprawnionych do ich dostępu, jak i do jego ograniczania, co dotyczy również informacji z zakresu tajemnicy zawodowej;
3. istnieje jednak pewien zakres informacji kategorycznie chronionych na podstawie przepisów prawa, czyli dostęp do takich informacji mogą uzyskać jedynie osoby ściśle określone procedurami szczegółowymi, dotyczą one informacji niejawnych czy innych tajemnic chronionych. Osoby nieuprawnione zdobywają takie informacje w ramach szarego i czarnego wywiadu, co szacuje się na 5-10% zbieranych danych.

Pojęcie informacji i tajemnicy działania określonych podmiotów stanowi przedmiot rozważań wielu pozycji literatury[462] oraz regulacji prawnych. W polskim stanie prawnym wyróżnia się 54 różne tajemnice zawodowe, od informacji niejawnych po tajemnicę przedsiębiorstwa czy tajemnicę spowiedzi.

Istotne są postanowienia ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[463], istotne ze względu na bezpieczeństwo państwa, a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[464] zawierają chronione tzw. dane sensytywne, które stanowią katalog zamknięty obejmujący: pochodzenie rasowe lub

458 http://pl.wikipedia.org/wiki/Informacja (dostęp18.06.2010)

459 B. Michalski, Prawo dziennikarza do informacji, Kraków 1974, s. 9-10.

460 Leksykon PWN, Warszawa 1972, s. 444.

461 W. Filipkowski, W. Mądrzejowski, *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012 oraz B. Seremak, *Biały wywiad w służbach specjalnych: znaczenie i perspektywy* w: Z. Siemiątkowski, A. Zięba, *Służby specjalne we współczesnym państwie*, Warszawa 2016, s. 153-168.

462 Szerzej: J.W. Wójcik, *Ochrona informacji, a wywiad gospodarczy. Zagadnienia kryminalistyczne, kryminologiczne i prawne,* Warszawa 2016.

463 Dz.U. nr 182, poz. 1228.

464 t. j. Dz.U. z 2014 r. poz. 1182.

etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, i kodzie genetycznym, dane o nałogach, dane o życiu seksualnym i dane dotyczące wyroków sądowych.

Istotą przepisu z art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[465] są informacje, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Tajemnica przedsiębiorstwa wynika z art. 11 ust. 1-4 ustawy, a jej zakres dotyczy: informacji o charakterze technicznym, technologicznym, organizacyjnym lub innym posiadającym wartość gospodarczą. Są to informacje poufne, co oznacza, że nie zostały ujawnione do wiadomości publicznej, a przedsiębiorca podjął niezbędne działania w celu zachowania poufności takich informacji ze względu na ich gospodarcze znaczenie.

## 2.Wybrane zagrożenia związane z manipulowaniem informacją

To kluczowe zagadnienie systematycznie omawiane zarówno w mediach, jak i w literaturze powoduje, że współczesne zagrożenia zmuszają do zmiany filozofii ochrony informacji i bezpieczeństwa przedsiębiorstwa. Najłatwiej wykazać zagrożenia w dziedzinie informatyki stosowanej. Znane jest powiedzenie, że prawdopodobieństwo ataku hakerów jest dziś wyższe niż pożaru. Znany ekspert w dziedzinie zabezpieczeń systemów informatycznych Bob Ayers, twórca i szef Programu Zabezpieczania Systemów Informatycznych w Departamencie Obrony USA, konsultant rządów Wielkiej Brytanii i Szwecji, wykładowca na Uniwersytecie Bezpieczeństwa Narodowego i Akademii Wywiadu USA – już dawno stwierdził, że zmiana polega na przejściu od unikania zagrożeń do zarządzanie ryzykiem. Przykładowo, po kilku latach inwestowania w nowe systemy informatyczne okazało się, że zasada unikania ryzyka w ochronie informacji jest nieskuteczna, gdyż koszty nowego programu informatycznego tworzonego dla indywidualnego odbiorcy są za wysokie w stosunku do możliwości (kompatybilność, wszechstronność, bezpieczeństwo i koszt poprzednich wersji). Warto zatem zakupić nowoczesne oprogramowanie[466].

Nabyte doświadczenia i praktyka ochrony informacji wskazują, że nie jest możliwe zbudowanie całkowicie bezpiecznego systemu informatycznego. Wykazali to właśnie eksperci zajmujący się budowaniem takich systemów. Nie ma także sieci całkowicie bezpiecznych. Bez względu na rodzaj zastosowanych zabezpieczeń zawsze znajdzie się ktoś, kto je przełamie.

W tej sytuacji okazało się, że niezbędna jest nowa filozofia. Tak powstało „zarządzanie ryzykiem". Najogólniej rzecz biorąc nowa filozofia powstała z tej przyczyny, że wybitny specjalista może przewidzieć zagrożenia spowodowane czynnikami naturalnymi, nie jest natomiast w stanie przewidzieć ataków kierowanych przez „inteligentne istoty', czyli intruzów, którzy powodują poważne zagrożenia i olbrzymie straty materialne.

Jeżeli zagrożenie jest wypadkową wielu przypadków i sterowanych zdarzeń, to każde z tych zdarzeń może być wynikiem oddziaływania przypadków lub celowej działalności człowieka.

465 t. j. Dz. U Nr 153, poz. 1503.

466 B. Ayers, *Bezpieczeństwo informacji w 21 wieku. Zapobieganie i unikanie ryzyka – sztuka dla sztuki*, „Internet Developer" 1997, nr 2.

Pierwszy rodzaj zagrożeń stosunkowo łatwo przewidzieć, drugi – powoduje więcej problemów, gdyż celowe zagrożenie jest rezultatem połączenia trzech czynników. Zdaniem B. Ayersa są to: motyw, sposób działania i okazja. Motywem może być przykładowo niezadowolenie z pracy, którego skutkiem staje się skasowanie plików z systemu informatycznego firmy. Każdy szpieg ma zlecone zadania do wykonania na rzecz obcego wywiadu. Podobnie szpieg gospodarczy. Innymi motywami kieruje się haker.

Sposób, czyli *modus operandi* związany jest z umiejętnościami niezbędnymi do włamania się do systemu. Umożliwiają to połączenia sieciowe i wiedza, w tym również informacje zawarte w Internecie. Przykładem jest napisany swego czasu program SATAN dla administratorów, a wykorzystywany przez hakerów.

Okazja to ułatwiony dostęp do komputerowej bazy danych. Należy pamiętać, że podłączenie określonego komputera do sieci umożliwia kontakt z całym światem, ale również cały świat ma dostęp do tego komputera. Zatem wniosek jest prosty: właśnie ten komputer jest zagrożony przez cały czas połączenia ze światem.

Warto zauważyć, że punktem wyjścia do dalszych rozważań może być zasadna teza, że dla każdego społeczeństwa, dla każdego systemu politycznego czy ekonomicznego istnieje niezbędny i określony zakres informacji, ważny dla członka tej społeczności, by mógł świadomie i w sposób pełny wykonywać obowiązki ciążące na nim jako na członku grupy społecznej, zawodowej, aby mógł spełniać swoje obowiązki jako obywatel państwa. Istnieje ścisła korelacja między wiedzą obywatela a możliwością spełniania przez niego obowiązków obywatelskich. Zadaniem państwa i jego organów jest staranne analizowanie tego zakresu informacji i takie organizowanie procesów informacyjnych, aby obywatel miał dostęp do nich w optymalnej formie, zakresie, języku, miejscu i czasie, jako do dobra publicznego[467].

W dobie powszechnego wykorzystywania Internetu dla różnorodnych celów, niezwykle trudno jest rozpoznać i określić wszystkie występujące zagrożenia. Warto pamiętać o tych podstawowych, które powodują nie tylko straty finansowe, lecz mogą grozić bezpieczeństwu powszechnemu, a szczególnie życiu i zdrowiu obywateli. Jednakże wiele krajów, na podstawie zaistniałych już ataków, przygotowuje się nie tylko do prawnego, kryminologicznego i kryminalistycznego, ale również interdyscyplinarnego przeciwdziałania różnego rodzaju sytuacjom kryzysowym, w tym przede wszystkim atakom cyberterrorystycznym na obiekty strategiczne wojskowe i cywilne. W aktualnej sytuacji politycznej liczne kraje są szczególnie zagrożone, zarówno w Europie, jak i w Ameryce. Z tego względu także polskie resorty strategiczne, zgodnie z obowiązującym ustawodawstwem opracowują plany zabezpieczeń tzw. infrastruktury krytycznej istotnej z punktu widzenia bezpieczeństwa narodowego. Tu warto zwrócić uwagę na rosyjskich hakerów, którzy spowodowali wiele zamieszania podczas wyborów prezydenta w USA.

W wielu współcześnie rozpoznanych aferach ujawnia się brak nadzoru i kontroli zobowiązanych instytucji państwowych. Wciąż jeszcze brak jest bezpiecznego systemu w sieci oraz zasad jego stosowania[468]. Ponadto, istnieje obawa przed utratą reputacji w przypadku ujawnienia skutecznego ataku hakerskiego i spowodowania strat materialnych. Z tego względu niechętnie powiadamia się organy ścigania.

467 J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Warszawa 2006, s. 51.

468 Szerzej: *Dwadzieścia jeden złotych recept czyli jak skutecznie chronić bazy danych, systemy teleinformatyczne i inne elektroniczne urządzenia mobilne* w: J.W. Wójcik, *Kryminologia, Współczesne aspekty,* Warszawa 2014, s. 231-249.

Każdy obywatel, ma obowiązek znać podstawowe zasady moralne i przepisy prawne. Jest to w jego interesie jako podstawowa zasada bezpieczeństwa. Wiadomo bowiem, że racjonalne działanie pozwoli na uniknięcie wielu kłopotów. Jednakże w sieci jest o wiele trudniej działać bezpiecznie. Przykładowo, eksperci ds. bezpieczeństwa w sieci twierdzą, że *Nie ma takiej strony, nie ma takiego serwera, którego dałoby się w stu procentach zabezpieczyć.* Podobnie z kradzieżą tożsamości przez hakerów, zjawisko to jest nasilone w wielu krajach. Przykładowo, w USA prezydent Barack Obama powiedział: *Miliony Amerykanów padły ofiarą kradzieży tożsamości. Te przestępstwa zagrażają poczuciu bezpieczeństwa klasy średniej.* W listopadzie 2013 roku w USA sprawcy włamali się do systemów informatycznych sieci handlowych. Hakerzy przez kilka tygodni mieli dostęp do danych klientów, którzy robili zakupy w 1800 sklepach sieci Target na terenie całych Stanów Zjednoczonych. Okazało się, że hakerzy z grupy Dragonfly wraz z 40 milionami numerów kart kredytowych pozyskali nazwiska ich posiadaczy, daty ważności i kody bezpieczeństwa, czyli łącznie przeszło 70 mln adresów, numerów telefonicznych i innych wrażliwych danych, które skradziono z potężnych serwerów koncernu. Wprowadzenie złośliwego oprogramowania umożliwiło kradzież tożsamości na dużą skalę[469].

Kradzież tożsamości, a ściślej fałszerstwo tożsamości można zdefiniować jako celowe używanie danych osobowych innej osoby, a także adresu zameldowania, numeru PESEL, najczęściej w celu dokonania oszustwa dla osiągnięcia korzyści majątkowej**.** Przestępstwo to polega na podszywaniu się pod czyjeś dane, a nie na usunięciu danych ofiary. Zachodzi zatem zawładnięcie cudzymi danymi osobowymi i bezprawne posługiwanie się nimi. Takie czyny karalne są z przepisów kodeksu karnego, przykładowo z art. 190a k.k. za kradzież tożsamości. Sprawca może również odpowiadać za fałszerstwo dokumentów, które jest ścigane z art. 270 - 276, czy z art. 286 k.k. za oszustwo. Z zagadnieniem tym związane są afery w instytucjach finansowych poprzez wykorzystywanie tzw. „słupów"[470].

Trudno jednak pociągnąć do odpowiedzialności karnej profesjonalistów, którzy jako warsztat pracy wykorzystują biały wywiad. Słynny Raport Coxa, który miał za zadanie wyjaśnić kto dostarczył Chinom materiały na unowocześnienie rakiet balistycznych, modernizacji arsenału nuklearnego, łodzi podwodnych i super szybkich komputerów - zaskoczył nie tylko Amerykanów. Wprawdzie wynika z niego m.in., że działalność wywiadów wielu państw, miała istotny wpływ na poważny rozwój techniki i gospodarki w wielu dziedzinach. Brak jednak zarzutów pod adresem chińskich szpiegów. Niewątpliwie jest to sukces białego wywiadu zastosowanego przez wywiad chiński.

## 3. Przestępstwa związane z ochroną informacji

Mając na względzie złożoną materię omawianego zagadnienia, warto wnieść uwagę ogólną, związaną z możliwościami skutecznej ochrony informacji. Zagadnienie realizacji przepisów prawa karnego, a szczególnie rozpoznawania, wykrywania i zapobiegania cyberprzestępczości, wciąż jeszcze stanowi swoiste *novum* w aspektach

469 Szerzej: J.W. Wójcik, *Ochrona informacji, a wywiad gospodarczy…* s. 282.

470 J.W. Wójcik*, Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008, s. 190.

kryminologicznych i kryminalistycznych, a przede wszystkim w systemie prawa oraz wkracza bardzo głęboko w sferę techniczną działania systemów przetwarzających dane.

Obecnie informacja jest nie tylko przedmiotem kradzieży danych, lecz przede wszystkim przedmiotem różnorodnych manipulacji w formie fałszowania różnego rodzaju informacji i danych. Przestępstwa te są ścigane na podstawie ustawy z dnia 6 czerwca 1997 r. Kodeks karny[471]. Przykładowo, przestępstwa przeciwko ochronie informacjizawarte są w rozdziale XXXIII k.k., a w szczególności:

- ujawnienie lub wykorzystanie informacji uzyskanej w ramach tajemnicy zawodowej w związku z pełnioną funkcją – art. 266 § 1 k.k.
- nielegalne uzyskanie cudzej informacji, z systemu teleinformatycznego, pokonanie zabezpieczeń i kradzież informacji – *hacking komputerowy* – art. 267 § 1 k.k. oraz 267 § 2 k.k., a także poprzez urządzenie podsłuchowe, wizualne albo inne urządzenie czy oprogramowanie – art. 267 § 3 k.k.
- niszczenie informacji – art. 268 § 1 - 3 k.k.
- spowodowanie szkody w systemach informatycznych – art. 268a § 1 k.k.
- sabotaż komputerowy – art. 269 § 1 i 2 k.k. oraz 269a k.k., 269 § 1 i 2 k.k., 269a k.k.
- kradzież tożsamości art. 190a k.k. § 2 k.k. oraz kradzież tożsamości ze skutkiem śmiertelnym – art. 190a k.k. § 3 k.k.

Przestępstwa przeciwko obrotowi gospodarczemu zawarte są w rozdziale XXXVI k.k., a w szczególności: nadużycie zaufania, niegospodarność w formie działania na niekorzyść spółki – art. 296 k.k., oszustwo kredytowe – art. 297 k.k., oszustwo ubezpieczeniowe – art. 298 k.k., pranie pieniędzy – art. 299 k.k., przestępstwa na szkodę wierzycieli – art. 300, 301, 302 k.k., nierzetelne prowadzenie dokumentacji działalności gospodarczej - art. 303 k.k., a także oszustwa informacyjne emitentów papierów wartościowych – rozpowszechnianie nieprawdziwych informacji lub ich ukrywanie – art. 311 k.k.

Problematyka przestępstw przeciwko ochronie informacji była i nadal będzie przedmiotem rozważań w podręcznikach, komentarzach, artykułach, glosach i uzasadnieniach wyroków sądowych, tym bardziej że wiele z nich wykazuje tendencję wzrastającą. *Modus operandi* tych przestępstw charakteryzuje się nie tylko manipulowaniem i fałszerstwem informacji, szczególnie o charakterze ekonomicznym, a kryminologiczna analiza i skala tych przestępstw wskazuje, że należy je aktualnie określić jako ekonomiczne problemy współczesnej kryminologii[472].

W cieniu statystyki policyjnej i życia społecznego pozostają jednak czyny dotyczące ujawnienia tajemnicy przedsiębiorstwa, czyli czyny z cytowanej ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji. Szczególnie należy mieć na uwadze czyny z art. 23 ust. 1, tj. bezpodstawne ujawnienie tajemnicy przedsiębiorstwa oraz z art. 23 ust. 2 szpiegostwo gospodarcze, które to czyny, w przypadku poważnej szkody, są zagrożone karą pozbawienia wolności do lat 2. Analizując dane zawarte w statystyce policyjnej okazuje się, że takie czyny rozpoznawane są zaledwie jednostkowo lub nie rozpoznaje się ich wcale.

471 Dz. U. z 1997 r. Nr 88, poz. 553.

472 Szerzej: J.W. Wójcik, *Ochrona informacji a bezpieczeństwo biznesu. Aspekty kryminologiczne i kryminalistyczne.* Referat wygłoszony przez autora na Ogólnopolskiej Konferencji Naukowej Wywiad i kontrwywiad w teorii i praktyce biznesu w dniu 25 maja 2017 r. zorganizowanej przez Wszechnicę Polską Szkołę Wyższą w Warszawie i Fundację Instytut Wywiadu Gospodarczego w Krakowie.

Mało ryzykowne jest zatem stwierdzenie iż aktualne ustawodawstwo, mimo wielu nowoczesnych regulacji, nie jest czynnikiem, który zapewnia ochronę informacji i tajemnicę przedsiębiorstwa mających strategiczne znaczenie w biznesie.

## 4. Wybrane kierunki i formy profesjonalnego zapobiegania utraty informacji w biznesie

Należy mieć na uwadze fakt, że wszystkie nowe technologie nastawione są na pozyskiwanie informacji za pomocą systemów informatycznych. Przykładowo:

- technologie wyspecjalizowanych analityków-wywiadowców, którzy wyszukują informacje na zamówienie,
- inteligentne interfejsy wyszukujące odpowiednie informacje z najróżnorodniejszych typów serwerów,
- raporty wywiadowców-analityków i wywiadowców gospodarczych oparte na programach umożliwiających realizację określonego polecenia,
- przeciwdziałanie szpiegostwu w cyberprzestrzeni, wspierane m.in. poprzez: skanowanie i analizowanie poczty elektronicznej, bazy danych, poczty wewnętrznej i szeregu innych.

W trakcie analizy obszernej i złożonej problematyki ochrony informacji, należy wyłonić podstawowe zagadnienia, które stanowić mogą węzłowe tematy, czyli jako podstawową i przydatną tematykę analityczno-badawczą nie tylko w omawianych aspektach. Szczególnie wyróżnić należy:

1. systematyczne rozpoznawanie kierunków i form nasilających się zagrożeń;
2. zapewnienie wysokiego poziomu przygotowania zawodowego tych analityków informacji, którzy posiadają wiedzę umożliwiającą racjonalne rozpoznawanie i przeciwdziałanie omawianej przestępczości;
3. stosowanie procedur bezpieczeństwa adekwatnych do występujących zagrożeń, przy świadomości, że statystyka policyjna nie obejmuje ciemnej liczby przestępstw[473];
4. w ramach badań kryminalistycznych i kryminologicznych należy analizować i postulować modyfikowanie systemu prawnego, który z oczywistych względów nie nadąża we wspomaganiu systemu zapobiegania;
5. niezbędne jest większe zaufanie do specjalistów z zakresu analizy informacji gospodarczej, czyli wywiadu gospodarczego w przedsiębiorstwie. Ich właściwe przygotowanie zawodowe umożliwia umiejętnie zebrać niezbędne dane, przeprowadzić odpowiednie badania i przedstawić zarządowi istotne wnioski dla przedsiębiorstwa. Specjaliści powinni ułatwić ważne, a niejednokrotnie strategiczne decyzje zarządowi przedsiębiorstwa na przykład w stosunku do najnowszych poczynań konkurencji.

Wybitny specjalista w zakresie bezpieczeństwa biznesu, profesor Jerzy Konieczny, określił model bezpiecznego działania firmy, także w zakresie bezpieczeństwa informacji. Osiągnięcie stanu idealnego nie jest możliwe, ale warto orientować się, że w

473 Szerzej: J.W. Wójcik, *Kryminologia,* wyd. cyt., s. 102-133.

tej modelowej sytuacji niezbędne jest zaistnienie trzech podstawowych warunków, a mianowicie:

1. rozpoznanie działań podejmowanych przeciwko naszej firmie;
2. personel naszej firmy jest wobec niej lojalny, a w szczególności wykluczone są przypadki ujawniania na zewnątrz informacji niejawnych, nie dochodzi także do kradzieży ani innych form destrukcji zasobów materialnych ze strony zatrudnianych osób;
3. firma jest chroniona przed zamachami przestępczymi, w rodzaju włamań, napadów, ataków terrorystycznych i tym podobnych[474].

Prowadzenie działalności kontrwywiadowczej, czyli ochrony przed czynnościami obcego wywiadu gospodarczego musi być działaniem systemowym. Chodzi bowiem o aki system polityki bezpieczeństwa przedsiębiorstwa, który problem ten będzie traktował kompleksowo. Natomiast w zapobieganiu zagrożeniom istotą sprawy jest dalsze skuteczne wypracowywanie systemu inteligentnego, który powinien polegać na:

- wszechstronnym profesjonalnym rozpoznawaniu zagrożeń,
- opracowaniu i uruchomieniu sygnałów wczesnego ostrzegania,
- analizowaniu i poszukiwaniu odpowiednich, tj. skutecznych metod zapobiegania.

W rozpoznawaniu zagrożeń uczestniczyć powinni analitycy informacji zajmujący się wywiadem i kontrwywiadem gospodarczym. Są to najczęściej specjaliści z zakresu wywiadu ekonomicznego, technologicznego, przemysłowego, handlowego, konkurencyjnego, finansowego, strategicznego, biznesowego, naukowego, strategii marketingowej personelu, wiedzy o personelu, promocjach, cenach, o klientach, o Internecie, o benchmarkingu i innych w ramach potrzeb.

Istnieje wiele obszarów, w których przedsiębiorca, menedżer czy biznesmen powinni być lepiej zorientowani. Zakres tej wiedzy jest szeroki. Dotyczy przede wszystkim przestrzegania prawa, ale również właściwego kierowania bezpieczeństwem firmy, a w tym również działań szczegółowych, przykładowo postaci dokumentowania rozmów z partnerami handlowymi, czy badania lojalności pracowników firmy.

Wraz z wiedzą dotyczącą ochrony informacji związanych z prowadzonym biznesem, transakcjami finansowymi, marketingiem i wielu innych jeszcze niezwykle ważnych problemów, chociażby natury prawno-finansowej, handlowej – trzeba zdawać sobie sprawę z tego, że konieczne jest przede wszystkim opracowanie i stosowanie własnej kompleksowej strategii bezpieczeństwa firmy, na miarę jej potrzeb i rozpoznanych zagrożeń. Zatem najważniejszą rzeczą jest opracowanie polityki bezpieczeństwa, która powinna obejmować przykładowo:

- politykę informacyjną,
- ochronę informacji niejawnych,
- ochronę danych osobowych,
- politykę bezpieczeństwa systemu teleinformatycznego,
- zasady ochrony tajemnicy przedsiębiorstwa lub innych tajemnic zawodowych firmy,
- zapobieganie przestępstwom na szkodę firmy, a szczególnie fałszerstwom i oszustwom,

474 J. Konieczny: *Wstęp do etyki biznesu*, Warszawa 1998, s. 73.

- zasady ochrony fizycznej i technicznej,
- inne polityki związane z bezpieczeństwem (np. polityka kadrowa, płacowa, szkoleniowa),
- profesjonalne przestrzeganie obowiązujących przepisów, a szczególnie ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla przedsiębiorstwa.

W działaniach szczegółowych niezbędne jest stosowanie m.in. takich zasad bezpieczeństwa informacji, jak np.:

- racjonalne rozmieszczenie właściwych zabezpieczeń mechanicznych i elektronicznych;
- dokładne rozpoznanie sytuacji prawno-finansowej klientów czy kontrahentów i zastosowanie programów weryfikujących ich autentyczność w działalności biznesowej;
- w zakresie bezpieczeństwa finansowego czy operacyjnego niezbędne jest korzystanie z usług profesjonalnych i sprawdzonych wywiadowni gospodarczych przed rozpoczęciem działalności z nową firmą lub nawiązaniem zobowiązań prawnych, finansowych, handlowych itp., a nie wówczas, gdy wystąpiły skutki braku wiarygodności kredytowej, handlowej czy przemysłowej kontrahenta;
- nagrywanie rozmów biznesmenów (za ich zgodą), które w przypadku sytuacji kryzysowej może mieć istotne znaczenie dowodowe w sądzie;
- w uzasadnionych przypadkach stosowanie badań antypodsłuchowych. Działania te należy prowadzić rutynowo przed wszystkimi posiedzeniami zarządów banków, towarzystw ubezpieczeniowych, spółek giełdowych, jednostek naukowych lub badawczo-rozwojowych, przedsiębiorstw, które wykonują prace zlecone objęte ochroną prawną informacji tych wszystkich instytucji czy organizacji, które omawiać będą cele strategiczne i inne problemy wymagające tajności czy poufności obrad. Modelem idealnym byłoby instalowanie pomieszczeń ekranowanych, które zapewniają bezpieczeństwo obrad. Natomiast w przypadku poważnych zagrożeń związanych z planowaniem przedsięwzięć strategicznych możliwe jest przygotowanie odpowiedniego pomieszczenia na zasadzie klatki Faradaya (tzw. "bąbel"), która zapewnia pełne bezpieczeństwo rozmów;
- zasadne powinno być wykorzystywanie możliwości badań poligraficznych personelu zajmującego się bezpieczeństwem organizacji;
- profesjonalne szkolenia zawodowe w zakresie teoretycznego i praktycznego stosowania najnowocześniejszych i sprawdzonych metod bezpieczeństwa, a także wypracowanie reakcji pracowników na możliwość zaistnienia sytuacji kryzysowej w przedsiębiorstwie.

## 5. Postulat badań kryminalistycznych i kryminologicznych

Inspiracją do kryminalistycznego, kryminologicznego i prawnego spojrzenia na potrzebę rozpoznawania, ochrony informacji i bezpieczeństwa funkcjonujących w cyberprzestrzeni systemów informatycznych, a w tym również innych mobilnych zasobów informacyjnych jest wiele różnorodnych zagadnień, z których warto wyróżnić i objąć badaniami przynajmniej następujące:

- uzasadniona jest potrzeba analizowania wzrastającej systematycznie tendencji zagrożeń przestępczością ukierunkowaną na informacje chronione, zasoby w cyberprzestrzeni oraz jej związków z obrotem finansowym, gospodarczym, przedsiębiorstwami i instytucjami finansowo-bankowymi, której skutkami są poważne szkody ekonomiczne i społeczne. Należy zdawać sobie sprawą z faktu, że mamy do czynienia z profesjonalnym przeciwnikiem. To również intelektualista, wykształcony specjalistycznie, niejednokrotnie znane mu są procedury administracji publicznej, instytucji finansowych, a w tym stosowane systemy zabezpieczeń;
- niezbędna jest świadomość jak powszechne są cyberzagrożenia. Większość kontaktów, uzgodnień i transakcji dokonywanych jest poprzez środki elektroniczne, co niewątpliwie umożliwia profesjonalne zabezpieczenie dowodowych śladów transakcyjnych w formie dokumentów papierowych, jak i w formie elektronicznych śladów transakcyjnych;
- ataki hakerów na firmy nakierowane są najczęściej na kradzież danych. Wiele źródeł wskazuje, że blisko połowa z nich kończy się wyciekiem lub blokadą informacji. Jednakże wykrywalność jest daleka od pożądanej pomimo stosowania najnowszych środków jakim jest np. analiza kryminalna;
- charakterystyczny jest brak kompleksowej i profesjonalnej analizy oraz oceny istniejących zagrożeń, czego oczywistym skutkiem jest brak kryminologicznej diagnozy i prognozy;
- typowy jest wyrafinowany *modus operandi* sprawców, których kreatywne działania znacznie utrudniają skuteczne czynności rozpoznawcze i wykrywcze, a przede wszystkim zapobiegawcze. Na tym tle wyłania się szczególne znaczenie dowodowe w zakresie zabezpieczania elektronicznych śladów transakcyjnych, niezbędnych w rozpoznawaniu afer gospodarczych, a oszustw finansowych w szczególności[475]. Zatem przy odpowiednim stanie prawnym i wiedzy informatycznej, niezbędne jest właściwe zabezpieczanie dowodowych śladów elektronicznych o charakterze transakcyjnym[476];
- analizowane przestępstwa ujawniane są przypadkowo, a w dużej mierze z powodu błędów popełnianych przez sprawców. Z tego względu prewencyjna rola śledztwa oraz wyroku sądowego jest niezwykle ograniczona;
- ważna rola w zapobieganiu omawianej przestępczości przypada samym użytkownikom systemów informatycznych, bowiem sprawcy najczęściej wykorzystują błędy w administrowaniu i ochronie systemów, a także lekceważenie podstawowych zasad bezpieczeństwa;
- występuje niedostateczna lub bardzo ogólnikowa świadomość społeczna na temat zagrożeń, na które narażone są wszystkie instytucje i przedsiębiorstwa z powodu

475 Na tym tle zarysowała się potrzeba zastosowania nowej terminologii naukowej. Przydatne stało się utworzenie nowego terminu kryminalistycznego w formie „elektronicznego śladu transakcyjnego", który jest ważnym odzwierciedleniem potrzeby rozpoznawania najnowszych zagrożeń kryminalistycznych i kryminologicznych. Szerzej: *J.W. Wójcik,Oszustwa finansowe…* s. 78.

476 J.W. Wójcik, *Cyberprzestrzeń – kryminologiczne i kryminalistyczne zagadnienia śladu transakcyjnego i elektronicznego,* w: E. Gruza, M. Goc, T. Tomaszewski (red.), *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości,* Warszawa 2010, s. 375-407.

atrakcyjności ich produkcji, prowadzonej działalności, posiadanych baz informacji, czy innych form inspirujących zainteresowania agresywnej konkurencji, wywiadu i szpiegostwa gospodarczego, oszustów i fałszerzy, innych cyberprzestępców, a być może cyberterrorystów;

- niezbędna jest edukacja mająca na celu wyjaśnianie rodzajów i rozmiarów zagrożeń, a także rozpoznawania *modus operandi* sprawców, stosowanie obowiązującego prawa oraz wdrażania nowoczesnych zasad zapobiegania. Zasadne jest wdrożenie specjalistycznych zasad nauczania i edukacji w tym zakresie nie tylko studentów, lecz również funkcjonariuszy wszystkich służb policyjnych i specjalnych, prokuratorów i sędziów. Istotna rola w tej kwestii przypada intensywnie rozwijającej się kryminalistyce informatycznej, określanej również jako informatyka śledcza, która ma za zadanie ujawnianie i zabezpieczanie dla celów dowodowych kryminalistycznych śladów elektronicznych, a w tym śladów transakcyjnych. Kolejnym pozytywnym przykładem jest rozwijająca się od kilkunastu lat nowa dziedzina badań kryminalistycznych analiza kryminalna, która ma istotne znaczenie w wykrywaniu zorganizowanej przestępczości[477].
- pomimo wzrostu wydatków związanych z cyberbezpieczeństwem szefowie wielkich organizacji, jak i małych firm wciąż jeszcze zbyt mało uwag przykładają nie tylko do właściwej ochrony informacji i systemów informatycznych, a też do kompleksowego systemu ochrony i zabezpieczeń, czyli do polityki bezpieczeństwa organizacji, bezpieczeństwa wewnętrznego, a także w zakresie zarządzania kryzysowego.

Należy mieć również na uwadze, że zarówno w ramach nieuczciwej konkurencji, jak i w działalności gospodarczej lub wprost w ramach wywiadu gospodarczego rozpoznano kolejne nowe zagrożenie, które określono jako cyberszpiegostwo. Ostrzeżeniem może być sytuacja, w której firma działająca w określonej branży nagle zaczyna przegrywać przetargi, choć były one organizowane w różnych częściach kraju, a zawsze wygrywa jeden konkurent, którego oferty tylko nieznacznie różniły się od propozycji firmy, można podejrzewać cyberszpiegostwo. Uzasadnione staje się zatem wynajęcie informatyków śledczych, którzy profesjonalnie sprawdzą dane z firmowego sprzętu. Nie trudno bowiem ustalić, czy winę za wyciek dokumentacji ponosi technologia na podejrzanych usługach (konkurencja zdalnie włamała się do systemu), czy czynnik ludzki. A może należy wnioskować, że w firmie jest kret, który donosi konkurencji i kradnie cenne informacje jako szpieg gospodarczy.

## 6. Zdobycze nauki dla bezpieczeństwa w biznesie

We wszystkich dziedzinach życia społecznego, również w zakresie bezpieczeństwa przedsiębiorstwa, niezwykle cenne są osiągnięcia nauki. Warto również pamiętać, że przez wiele lat naukowców traktowano jako siłę napędową wszelkiego rozwoju. Dzisiaj wywiad gospodarczy zbiera więcej informacji w kilka dni niż niejeden utalentowany profesor robił to przez całe życie.

Kiedyś uważano, że tylko uczeni zmieniają świat. Dzisiaj, w dużej mierze robią to praktycy przy udziale naukowców w oparciu o kapitał intelektualny[478]. Musimy

477 P. Chlebowicz, W. Filipkowski, *Analiza kryminalna. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011.

478 J.W. Wójcik, *Walory informacji i wiedzy w wywiadzie gospodarczym*, "Zeszyty Naukowe WSIZiA", nr 1(34) 2016.

mieć świadomość, że nikt obecnie nie ma monopolu na bezpieczeństwo w biznesie. Ani policja, czy służby specjalne, ani eksperci czy specjaliści w zakresie wszelkiego rodzaju zabezpieczeń, ani nawet naukowcy – nie zrobią nic osobno. Niezbędna jest koordynacja i większa niż dotąd integracja wszystkich tych podmiotów i środowisk oraz szeroka współpraca, której podstawowym celem powinno być profesjonalne działanie przeciwko tym, którzy zajmują się wykradaniem cudzych i chronionych prawem informacji.

Wciąż jeszcze nie wszyscy mamy świadomość faktu, że współcześnie istnieje szereg okoliczności techniczno-elektronicznych, z których korzystamy w ramach prawa, lecz które wręcz ułatwiają działanie intruzom. Przykładowo, szpiegostwo komputerowe jest obecnie bardzo efektywnym działaniem. Wiąże się bezpośrednio z możliwościami technicznymi, jakie stwarza komputer, gdyż na małej przestrzeni znajduje się duży zbiór informacji, nie zawsze dobrze zabezpieczony.

Kolejne współczesne możliwości to zdalny podsłuch i podgląd wizyjny czy komputerowy i inne działania, które mogą skutecznie naruszyć strategię ochrony informacji i bezpieczeństwa przedsiębiorstwa. Jednakże prognostycznie rzecz biorąc, przewiduje się dalszy rozwój nauki. Znany jest również postulat: *każdy pracownik jest wywiadowcą na rzecz swojej firmy*[479] i być może, że tego typu zadania będą zapisane w zakresie obowiązków, po odpowiednim przygotowaniu personelu nie tylko w zakresie działań wywiadowczych, lecz przede wszystkim w zakresie kontrwywiadowczym.

Warto zapamiętać, że zagrożenia są powszechne, lecz nie zawsze doceniane, gdyż stosowane metody są niezwykle zróżnicowane: od kradzieży informacji z komputerowej bazy danych aż po szpiegostwo gospodarcze, czyli od podstępnego działania pracownika firmy aż po wywiad satelitarny.

479 B. Martinet, Y.M. Marti: *Wywiad gospodarczy...,* s. 325.

# BIBLIOGRAFIA

## LITERATURA


Adamczyk A., *Klasyfikacja informacji i danych prawnie chronionych*, Poznań 2005,

Adamski A., *Prawo karne komputerowe*, Warszawa 2000,

Aleksandrowicz T.R., *Analiza informacji w administracji i biznesie*, Warszawa 1999,

Ayers B., *Bezpieczeństwo informacji w 21 wieku. Zapobieganie i unikanie ryzyka – sztuka dla sztuki*, „Internet Developer" 1997, nr 2.

Bafia J., Mioduski K., Siewierski M*., Kodeks karny. Komentarz*, Warszawa 1987,

Bagiński Z., *Wywiad*, Warszawa 1975,

Bajer L., *Wywiad gospodarczy*, Warszawa 1979,

Bakker G.C.M (red.), *Financial investigation of crime. A toll of the integral law enforcement approach*, The Hague 2003, Liszewski K., Najmoła D., Wiciak K., *Śledztwo finansowe. Podstawy prawne i czynności policjanta służące pozbawianiu sprawców owoców przestępstwa,* Szczytno 2006.

Bennet D., Riley M., *Szpieg, który zarabiał. Jak amerykańska firma consultingowa zmieniła się w najbardziej zyskowną organizację wywiadowczą świata,* „Blomberg Businessweek" z 24-30 czerwca 2013.

Bieńkowska Higgins E., *Agent James Bond w biznesmena przemieniony*, „Rzeczpospolita" z 16 października 1998 r.

Biskup M. (red.) *Historia dyplomacji polskiej*, Warszawa 1982,

Błaszczak G., *Oszuści udający bank*, „Rzeczpospolita" z 17 lipca 2014 r.

Bojarski T. (red.), *Kodeks karny. Komentarz*, Warszawa 2011,

Bos-Karczewska M., *Afera wprost ze śmietnika*, „Rzeczpospolita" z 4 września 2001 r.

Bowcott O., Hamilton S., *Hackerzy i włamywacze i komputery*, Warszawa 1993,

Brustein J., *Big data. Eksperci z amerykańskich firm mówią o szansach i pułapkach,* „Blomberg Businessweek" nr 12(89)2014 z 24-30 marca 2014 r.

Bukowska J., Ćwiek J., *Człowiek z ukradzionym nazwiskiem*, „Rzeczpospolita" z 29-30 marca 2014 r.

Ciechomska M., *Ile tajemnic w kontraktach*, „Rzeczpospolita" z 4 września 2014 r.

Ciecierski M., *Wywiad gospodarczy w walce konkurencyjnej przedsiębiorstw*, Warszawa 2007,

Cilecki E., *Penetracja rynków zagranicznych. Wywiad gospodarczy*, Warszawa 1997,

Clarridge D.R., *Po prostu szpieg*, Warszawa 2001, (Tytuł oryginału: *A Spy for all Seasons*. *My life in the CIA*).

Collin B., *The future of cyberterrorism*, „Crime and Justice International" Marzec 1997,

Cornwall H., Datatheft. *Computer Fraud. Industrial Espionage and Information Crime*, Londyn 1990,

Cyrek P., *Rzeczywistość a przekaz medialny* w: A. Letkiewicz, A. Misiuk (red.) *Państwo, administracja, policja*, Szczytno 2012,

Czub K., *Ochrona prawna know-how*, „Rzeczpospolita" z dnia 20 czerwca 2011 r.

Czubkowska S., *Informatyka śledcza, czyli po e-mailu do kłębka*, „Dziennik" z 24-26 września 2010 r.

Czuchnowski W., *Afera podsłuchowa. Służby ograne i bezradne*, „Gazeta Wyborcza" z 17 lipca 2015 r.

Czuchnowski W., *Czy służby tolerowały podsłuchy?* „Gazeta Wyborcza" z 17 lipca 2015 r.

Dahlgaard J., Kristensen K., Kanji G.K., *Podstawy zarządzania jakością*, Warszawa 2004,

Darewicz K., *Agenci kosztują*, „Rzeczpospolita" z 21 grudnia.1999 r.

Darewicz K., *Szpiegostwo bez szpiegów*, „Rzeczpospolita" z 7 czerwca 1999 r.

Dawkins R., *The Blind Watchmaker*, New York 1986,

Ronfeldt D., *Networks and Netwars*, Santa Monica 2001,

Deptuła T., *Kredytowe oszustwa bez precedensu*, „Rzeczpospolita" z 7 lutego 2013 r.

Domagalski M., *Prawda sądowa nie musi być całą prawdą*, „Rzeczpospolita" z 24 marca 2011 r.

Dretske F.I., *Knowledge and the Flow of Information*, Cambridge 1981,

Drzewiecki R., *System wyceny człowieka*, „Dziennik Gazeta Prawna" z dnia 21-23 marca 2014 r.

Dubiński K., Jurczenko I., *Być szpiegiem*, Warszawa 1994,

Dunaj B. (red.) *Słownik współczesny języka polskiego*, Warszawa 1998,

Duńczyk J., Klimkiewicz Z., *Cyberterroryzm w aspekcie entropii informacji* w: T. Jemioło, J. Kisielnicki, K. Rajchel, *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009,

Duszczyk M., *Cyberprzestępcy w ataku na Polskę*, „Rzeczpospolita" z 3 lipca 2014 r.

Duszczyk M., *Hakerzy celują w rząd. Szukają złóż?* „Rzeczpospolita" z 7 lipca 2014 r.

Duszczyk M., *Polska to raj dla hakerów*, „Rzeczpospolita" z 20 listopada 2014 r.

Duszczyk M., *Polski biznes rajem złodziei*, „Rzeczpospolita" z 16 października 2014 r.

Duszczyk M., *Polskie firmy na celowniku szpiegów*, „Rzeczpospolita" z 16 października 2014 r.

*Encyklopedia Powszechna PWN*, Warszawa 1987,

*Encyklopedia szpiegostwa*, Praca zbiorowa, Warszawa 1995,

Ferbrache D., *Patologia wirusów komputerowych*, Warszawa 1993,

Filipkowski W., Mądrzejowski W., *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012,

Flakiewicz W., *Systemy informacyjne w zarządzaniu*, Warszawa 2002,

Galata S., *Strategiczne zarządzanie organizacjami. Wiedza, intuicja, strategie, etyka*, Warszawa 2004,

Galińska-Ręczy 1., *Opinia prawna w sprawie interpretacji pojęcia „tajemnica handlowa"*, „Zeszyty Prawnicze" nr 4(40) 2013,

Gardocki L., *Prawo karne*, Warszawa 2003,

Garfinkel S. Spafford G., *Bezpieczeństwo w UNIXIE i Internecie*, Warszawa 1997,

Garrin A.P., Berkman R., *The Art of Being Well Informed*, New York 1996,

Gilad B., *Business Intelligence System: A New Tool for Competitive Advantage*, „Amazon" 1988,

Gilowska A., *Nie każda informacja może być utajniona*, „Rzeczpospolita" z 28 stycznia 2014 r.

Gleick J. *Informacja, bit, wszechświat, rewolucja*, Kraków 2012,

Goold B.J., *CCTV and Policing. Public Area Surveilliance and Police Practices in Britain*, New York 2004,

Grabek A, *Matura na podsłuchu*, „Rzeczpospolita" z 28 października 2014 r.

Grabek A., *Hejt nasz powszedni*, „Rzeczpospolita" z 26 stycznia 2015 r.

Gut D., *To ja się włamałem*, „Gazeta Wyborcza" – Komputer z 10 marca 1998 r.

Hague P. N., Jackson P., *Badania rynku*, Kraków 1991,

Hague W., C*yberprzestrzeń: szansa i niebezpieczeństwo*, „Rzeczpospolita" z dnia 18 października 2011 r.

Hanausek T., *Kryminalistyka. Zarys wykładu*, Warszawa 2009,

Hartley R.V.L., T*ransmission of Information*, „Bell System Technical Journal", Nr 7, 1928,

Heracleous L., *Better than the Rest: making Europe the Leader in the Next Ware of Innovation and Performance,* „Long Range Planning", February 1998.

Hoc S., *Karnoprawna ochrona informacji*, Opole 2009,

Hoffman R., *Niewidzialna ręka amerykańskiej agencji. Świat w szpiegowskiej siatce*, „Trybuna" z 27 października 1999 r.

Hołyst B., *Terroryzm*, Warszawa 2009,

Janczak J., *Zakłócanie informacyjne*, Warszawa 2001,

Jemioło T., Kisielnicki J., Rajchel K. (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009,

Kaliski M., Kierzkowska A., Tomaszewski G., *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa oraz lojalność personelu*, w: J. Kaczmarek, M. Kwieciński, *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010,

Kamińska A., *Polacy masowo ruszyli po pożyczki do Internetu*, „Rzeczpospolita" z 22 sierpnia 2014 r.

Karwowski A. *Leksykon PWN*, Warszawa 1972,

Kaźmierska A., *Etyka szpiegowania,* „Rzeczpospolita" *z 29.10. 2013 r.*

*Kharif O., Innowacje. Karta pod kontrolą*. „Blomberg Businessweek" Nr 25(102)2014 z 23-29.06.2014 r.

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Warszawa 2005,

Knoppek K., *Dokument w procesie cywilnym*, Poznań 1993,

Koch E,R, Sperber J., Infomafia, *Szpiegostwo komputerowe, handel informacją, tajne służby*, Gdynia 1999,

Kołtuniak M., *Administrator bezpieczeństwa informacji powinien być jak inspektor*, „Rzeczpospolita" z 30 grudnia 2014 r.

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

Konieczny J., *Wstęp do etyki biznesu*, Warszawa 1998,

Kopaliński W. (red.), *Słownik języka polskiego*, Warszawa 1985,

Korzeniowski L., *Firma w warunkach ryzyka gospodarczego*, Kraków 2001,

Korzeniowski L., Pepłoński A., *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005,

Kościelniak P., *Amerykańskiej policji udało się złapać króla spamu*, „Rzeczpospolita" z 2-3 czerwca 2007 r.

Kościelniak P., *Hakerzy umysłów*, „Rzeczpospolita" z 23-24 sierpnia 2014 r.

Kościelniak P., *Nieetyczny eksperyment na Facebooku*, „Rzeczpospolita" z 1 lipca 2014 r.

Kościelniak P., *Spamerzy wykorzystują zamieszanie na rynku akcji*, „Rzeczpospolita" z 11-12 sierpnia 2007 r.

Kościelniak P., *Spamerzy żerują na MH17*, „Rzeczpospolita" z 23 lipca 2014 r.

Kowalczuk P., *Rosjanie podsłuchują przywódców*, „Rzeczpospolita" z 31.10-1.11.2013 r.

Kozieł H., *Światowa cyberprzestrzeń cały czas jest areną wojny. Ostatnio konflikt się nasilił*, „Rzeczpospolita" z 4 listopada 2014 r.

Krupa – Dąbrowska R., *Hejt wygrywa z prawem*, „Rzeczpospolita" z 21 września 2015 r.

Krwawicz M., Marciniak S., *Rola informacji w budowie bazy planistyczno – normatywnej controllingu strategicznego* w: R. Borowiecki, M. Kwieciński (red.) *Informacja w zintegrowanej Europie. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001,

Krywko J., *Podglądani przez własne laptopy* „Gazeta Wyborcza" z 31.12.2013-1.02.2014 r.

Księżyk M., *Podstawowe zagadnienia ekonomii*, Zakamycze 2000,

Kublik A., *Rosyjscy szpiedzy szperają w Yahoo!*, „Gazeta Wyborcza" z 17 marca 2017 r.

Kuligowski Ł., *Zamiast pieniędzmi coraz częściej płacimy danymi*, „Rzeczpospolita" z 5 listopada 2014 r.

Kunicka-Michalska B., *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości*. Rozdział XXX i XXXIII *Kodeksu karnego*, Warszawa 2000,

Kunicka-Michalska B., *Przestępstwa przeciwko tajemnicy państwowej i służbowej*, w: *System Prawa Karnego* 1989,

Kunicka-Michalska B., *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości*. Rozdział XXX i XXXIII *Kodeksu karnego. Komentarz*, Warszawa 2002,

Kwieciński M., *Wywiad gospodarczy jako meta koncepcja zarządzania przedsiębiorstwem* w: J. Kaczmarek, M. Kwieciński M. (red.) *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010,

Kwieciński M., *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa-Kraków 1999,

Lawrence D., *Poszukiwani: tysiące dobrych hakerów*, „Bloomberg Businessweek" nr 19(96)2014 z 12-18.05.2014 r.

*Leksykon PWN*, Warszawa 1972,

Lendzin J.P., Stankiewicz-Mróz A., *Wprowadzenie do organizacji i zarządzania*, Kraków 2005,

Lorenz W., *Kreml stawia na szpiegów*, „Rzeczpospolita" z dnia 7-9 kwietnia 2012 r.

Marek A., *Kodeks karny*. *Komentarz*, Warszawa 2004,

Marenches H., *Dans les secrets desprinces*, Paris 1986,

Marszałek A., *Wiadomość jako towar*, „Rzeczpospolita" z dnia 9 czerwca 1998 r.

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

Masny A. Osika A., *Wykorzystanie technologii informacji i komunikacji w samorządach* w: R. Borowiecki, M. Kwieciński (red.), *Informacja w zintegrowanej Europie. Koncepcje i narzędzia wobec wyzwań i zagrożeń*, Warszawa 2006,

Masterman J.C., *The Double Cross System in the War of 1939 – 1945*, Yale University Press 1972.

Mazurkiewicz P., *Cyfrowy analfabetyzm w Polsce ma się dobrze*, „Rzeczpospolita" z 25 sierpnia 2014 r.

Mądrzejowski W., *„Biały wywiad" w Policji* (w:) W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*. Warszawa 2012,

Mejssner B., *Mroczna strona Facebooka*, „Rzeczpospolita" z 5 marca 2015 r.

Mejsner B., *Hakerzy i wirusy mają ułatwione zadania*, „Rzeczpospolita" z 18 września 2014 r.

Mejssner B., *W powodzi niechcianych informacji*, „Rzeczpospolita" z 30 listopada 2006 r.

Michalak A., *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, Warszawa 2006,

Michalski B., *Prawo dziennikarza do informacji*, Kraków 1974,

Miecik I. T., *Ośmiornica czy krewetka*, „Polityka" nr 26 z 24 czerwca 2000 r.

Mitnick K., Simon W., *Sztuka podstępu*, Gliwice 2003,

Mozgawa M. (red.), *Kodeks kamy*. *Komentarz*, Warszawa 2014,

Noaka I., Takanachi H., *Kreowanie wiedzy w organizacji*, Warszawa 2000,

*Nowa Encyklopedia Powszechna PWN*, Warszawa 1997,

Nowak M.J., *Które informacje zachować w tajemnicy*, „Rzeczpospolita" z 4 września 2014 r.

Nowak T., *Dowód z dokumentu w polskim procesie karnym*, Poznań 1994,

Olczyk E., *Sekretne nagrania wagi ciężkiej*, „Rzeczpospolita" z 18 lipca 2012 r.

Oleński J., *Ekonomika informacji. Metody*, Warszawa 2003,

Oleński J., I*nfrastruktura informacyjna państwa w globalnej gospodarce*, Warszawa 2006,

Oleński J., *Standardy informacyjne w gospodarce*, Warszawa 1997,

Olesiński J., *Ekonomika informacji. Metody*, Warszawa 2003,

Osowski S., *Prawo dostępu do informacji publicznej jako bierny i czynny obowiązek informowania – wprowadzenie*, [w] „Jurysta" nr 1, 2002, s. 2,

Owczarek K., Żurak-Owczarek C., *Bezpieczeństwo informacji w handlu elektronicznym* w: R. Borowiecki, M. Kwieciński M. (red.) *Informacja w zintegrowanej Europie. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001,

Polmar N., Allen T. B., *Księga szpiegów. Encyklopedia*, Warszawa 2000,

Preussner-Zamorska J., *Zakres prawnie chronionej tajemnicy w postępowaniu cywilnym*, „Kwartalnik Prawa Prywatnego" 1998, z. 2,

Przewoźniak M., Mazurków E., *Pomysłowy szpieg przemysłowy. Sprzątaczka-informatyk kradła dane konkurencji*, Życie Warszawy z 17 listopada 2003 r.

Pytlakowski P., *Służby nie-specjalne*, „Polityka" nr 28 (2966) z 7.07. – 15.07.2014 r.

Radzimirski M., *Miliardowe interesy szarej strefy*, „Rzeczpospolita" z 17 lipca 2014 r.

Raszkowska G., *Certyfikat dla łowcy głów*, „Rzeczpospolita" z 16 lutego 2011 r.

Reck D., Kowolik T., *Due diligence chroni przed nieodpowiednią fuzją*, „Rzeczpospolita" z 4.03.2015 r.

Riley M., Elgin B., Lawrence D., Matlack C., Cel: *karty kredytowe. Kulisy jednego z największych skoków hakerskich w historii*, „Bloomberg Businessweek" Nr 15(92)2014 14-21 kwietnia 2014 r.

Rochwicz P., *Przestępcy coraz częściej pukają do drzwi doradców*, „Rzeczpospolita" z 10-11.05.2014 r.

Romanowska M., *Kształtowanie wartości firmy w oparciu o kapitał intelektualny*, w: R. Borowiecki, M. Romanowska (red.), *System informacji strategicznej*, Warszawa 2001,

Rusbridger J., *Gra wywiadów. Iluzje i pozory szpiegostwa międzynarodowego*, Warszawa 1993,

Small R.A., *„Know Your Customer" Policy* (w) Financial Action Task Force, Money Laundering Symposium, March 2-5, Warsaw 1993,

Solak M., *Benchmarking jako skuteczne narzędzie wywiadu gospodarczego*, w: J. Kaczmarek, M. Kwieciński (red.) *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010,

Sopińska A. *Rola systemu informacyjnego w procesie zarządzania strategicznego* w: R. Borowiecki, M. Romanowska (red.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001,

Sopińska A., *Podstawa informacyjna zarządzania strategicznego przedsiębiorstwem*, Warszawa 2000,

Stevens R., *Understanding Computers*, Oxford 1986,

Stolarczyk C., *Wielkie ucho Wielkiego Brata*, „Angora" nr 27 z 8 lipca 2012 r.

Szpyra R., *Militarne operacje informacyjne*, Warszawa 2003,

Szwaja J., *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, Warszawa, 2006,

Szymczak M. (red.), *Słownik języka polskiego*, t. 1, Warszawa 1988,

Szymowski L., *Szpieg w biznesie*, „Angora" nr 5(1129) z 5 lutego 2012 r.

Świderek T., *Szukam dobrych stron złych informacji*, „Rzeczpospolita" z 27 października 2014 r.

Świerczyńska K., *Raczej zrezygnujemy z telewizji i komórki niż z dostępu do sieci*, „Dziennik" z dnia 23 lipca 2009 r.

Taradejna R. i M., *Ochrona informacji w działalności gospodarczej, społecznej i zawodowej oraz życiu prywatnym*, Warszawa 2004,

Kwieciński M. (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010,

Walczak S., *Szpiegostwo przemysłowe*, „Rzeczpospolita" z dnia 15 stycznia 1998 r.

Walewska D., *Sprzątaczka, czyli Bond po polsku*, „Rzeczpospolita" 9-11 listopada 2013 r.

Walkowiak J., *Misja firmy a etyka biznesu*, Warszawa 1998,

Waszkiewicz P., *Wpływ monitoringu wizyjnego na pracę policji*, w: E. Gruza, T. Tomaszewski, M. Goc., „Problemy Współczesnej Kryminalistyki", nr 12, Warszawa 2008,

Wawak T. (red.) *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Bielsko-Biała 2007,

Wawrzyniak B., *Raport o Zarządzaniu* nr 5, „MBA", nr 1, 2001,

Wątor J., *Jedno kliknięcie i stajesz się oszustem*, „Gazeta Wyborcza" z 11 lipca 2014 r.

Wiewiórkowski W., Wierczyński G., *Informatyka prawnicza. Technologia informacyjna dla prawników i administracji publicznej*, Warszawa 2008,

Wojciechowski J., *Kodeks karny. Komentarz. Orzecznictwo*, Warszawa 1997,

Wojciechowski T., *Wywiad gospodarczy*, „Firma" 1991, nr 7-8,

Wolak D., *Firmy nie dbają o bezpieczeństwo*, „Rzeczpospolita" z 10 grudnia 2013 r.

Wójcik J. W*, Przestępstwa komputerowe, cz. 1 – Fenomen cywilizacji*, Warszawa 1999.

Wójcik J. W, *Przestępstwa komputerowe, cz. 2 – Techniki zapobiegania*, Warszawa 1999.

Wójcik J. W., *Kryminalistyczne i dowodowe znaczenie śladu transakcyjnego*. Referat wygłoszony na konferencji naukowej „Dokumenty a prawo" w ramach Jubileuszu 200-lecia Wydziału Prawa i Administracji UW, Warszawa 24 października 2008 r. w: E. Gruza (red.), *Dokumenty we współczesnym prawie*, Warszawa 2009,

Wójcik J. W., *Weryfikacja podejrzenia popełnienia przestępstwa prania pieniędzy*, „Prokuratura i Prawo" 2005, nr 9.

Wójcik J.W., *Fałszerstwa dokumentów publicznych. Rozpoznawanie i zapobieganie*, Warszawa 2005.

Wójcik J.W., *Blokada poczty elektronicznej jako zagrożenie bezpieczeństwa obrotu gospodarczego*, „Zeszyty Naukowe WSIZiA" w Warszawie, Nr 1(6) 2007.

Wójcik J.W., *Cyberprzestępczość – kradzież informacji. Zagadnienia kryminologiczne i kryminalistyczne*, „Zeszyty Naukowe WSIZiA w Warszawie", Nr 4(29)2014.

Wójcik J.W., *Cyberprzestępczość a prawo*, „Problemy Prawa i Administracji", Nr 1/2011.

Wójcik J.W., *Cyberprzestrzeń – kryminologiczne i kryminalistyczne zagadnienia śladu transakcyjnego i elektronicznego*, w: E. Gruza, M. Goc, T. Tomaszewski (red.), C*o nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2010,

Wójcik J.W., *Kryminologia. Współczesne aspekty*, Warszawa 2014,

Wójcik J.W., *Kryminologiczna ocena transakcji w procesie prania pieniędzy*, Warszawa 2001,

Wójcik J.W., *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego* w: R. Borowiecki , M. Romanowska (red.), *System informacji strategicznej… Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001,

Wójcik J.W., *Przestępstwa w biznesie*, Warszawa 1998,

Wójcik J.W., *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008.

Wójcik J.W., *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa 2002.

Wójcik J.W., *Przeciwdziałanie finansowaniu terroryzmu*, Warszawa 2007.

Wójcik J.W., *Przeciwdziałanie praniu pieniędzy*, Kraków 2004,

Wójcik J.W., *Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne*, Warszawa 2011,

Wójcik J.W., *Wywiad gospodarczy a prawna ochrona informacji*, Warszawa 2000,

Wójcik J.W., *Wywiad gospodarczy. Wybrane problemy kryminologiczne i kryminalistyczne* w: *Wywiad gospodarczy. Teoria i praktyka*. Materiały z konferencji. Warszawa dnia 30 września 1999 r.,

Wójcik J.W., *Z problematyki ochrony informacji w cyberprzestrzeni nie tylko w sytuacjach kryzysowych* w: R. Częścik i inni: *Zarządzanie kryzysowe w administracji*, Warszawa-Dęblin 2014,

Wójcik J.W., *Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne* [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, red. T. Jemioło, J. Kisielnicki, K. Rajchel, Warszawa 2009,

Wróbel W., *Kodeks karny. Część. szczególna. Komentarz*, t. II, Warszawa 2008,

Wróbel W., *Niektóre problemy ochrony tajemnicy w projekcie kodeksu karnego*, „Przegląd Prawa Karnego" 1996, nr 14, 15.

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

Wysocki M., *Wykorzystanie otwartych źródeł informacji przez instytucje finansowe* w: W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012,

Zawadka G., *Mistrzyni wyłudzeń i kamuflażu*, „Rzeczpospolita" z 24-25 maja 2014 r.

Żebrowski A., *Wywiad i kontrwywiad XXI wieku*, Lublin 2010,

Żebrowski A., *Zakłócanie informacyjne elementem rozwoju organizacji gospodarczej* w: J. Kaczmarek, M. Kwieciński, *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010,

Żurak-Owczarek C., *Business Intelligence – nowoczesna koncepcja zarządzania informacjami w przedsiębiorstwie* w: J. Kaczmarek, M. Kwieciński (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010,

## AKTY PRAWA KRAJOWEGO

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. nr 78, poz. 483 ze zm.)

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 2000, Nr 98, poz. 1071 ze zm.).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (tj. Dz. U. 2014, poz. 121).

Ustawa z dnia 17 listopada 1964 r. kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 ze zm.).

Ustawa z dnia z dnia 26 czerwca 1974 r. kodeks pracy (tj. Dz.U. 2014 poz. 1502).

Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (tj. Dz. U. z 2014 r. poz. 637 ze zm.).

Ustawa z 26 maja 1982 r. – Prawo o adwokaturze (tj. Dz. U. z 2014 poz. 637).

Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24 ze zm.).

Ustawa z dnia 20 czerwca 1985 r. o prokuraturze (tj. Dz. U. z 2011 r. Nr 270, poz. 1599).

Ustawa z dnia 29 września 1986 r. – Prawo o aktach stanu cywilnego (Dz. U. z 2004 r. Nr 161, poz. 1688 ze zm.).

Ustawa z dnia 23 grudnia 1988 r. o działalności gospodarczej (Dz. U. *1988* nr 41 poz. 324).

Ustawa z dnia 7 kwietnia 1989 r. – Prawo o stowarzyszeniach (Dz. U. z 2001 r. Nr 79, poz. 855 ze zm.).

Ustawa z dnia 6 kwietnia 1990 roku o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, ze zm.).

Ustawa z dnia 14 lutego 1991 r. – Prawo o notariacie (tj. Dz. U. z 2014 r., poz. 164).

Ustawa z dnia 28 września 1991 r. o kontroli skarbowej (Tekst jedn.: Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.).

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz. U Nr 153, poz. 1503).

Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (tj. Dz. U. z 2011 r. Nr 231, poz. 1375 ze zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych ( tj. Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.).

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 1995 r. Nr 88, poz. 439 ze zm.).

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (tj. Dz. U. z 2011 r. Nr 277, poz. 1634 ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. 2002 r., Nr 72, poz. 665 ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. z 2005 r. Nr 1, poz. 2, z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (tj. Dz. U. z 2011 r. Nr 231, poz. 1376 ze zm.).

Ustawa z dnia 22 sierpnia 1997 roku *o ochronie osób i mienia (*tj. z 2005 roku Nr 145, poz. 1221, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. nr 89, poz. 555 ze zm.).

Ustawa z dnia 21 sierpnia 1997 r. – Prawo o publicznym obrocie papierami wartościowymi (Dz. U. z 2005 r. Nr 111, poz. 937 ze zm.).

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tj. Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.).

Ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów (Dz. U. Nr 73, poz. 763 ze zm.).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2001 r, nr 128, poz.1402).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t j. Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204, z 2004 r. Nr 96, poz. 959, Nr 173, poz. 1808, z 2007 r. Nr 50, poz. 331).

Ustawa z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. Nr 124, poz. 1154 ze zm.).

Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2010 r. nr 113, poz. 759).

Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. 2004 Nr 64 poz. 593).

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. Nr 183, poz. 1538 ze zm.).

## NETOGRAFIA

Agencja Ochrony Wena file:///C:/Users/jwwojcik/Documents/PRAWO/Ba%C5%82tyk%20--%20Agencja%20Ochrony%20WENA%20Sp%C3%B3%C5%82ka%20z%20o.o.. html(17.01.2015).

Ciecierski M., *Szpiegostwo przemysłowe opanowało cyberprzestrzeń* http://biznes.pl/wiadomosci/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen,5402264,news-detal. html(28.11.2014).

Chmielarz W. http://niwserwis.pl/artykuly/szpiegostwo-przemyslowe-duzy-zysk-niskie-kary. html(14.11.2013).

Duszczyk M., *Wyciekają firmowe tajemnice* http://www.ekonomia.rp.pl/artykul/1143012. html(22-09-2014).

Dziekański P*., Informacja jako dobro ekonomiczne będące źródłem przewagi konkurencyjnej* www.ur.edu.pl/file/16795/28.pdf(2.06.2014).

Kopańko K., *Zamiast wykorzystywać luki w systemach bezpieczeństwa dla własnych korzyści, ostrzegają przed nimi świat* http://tech.pb.pl/3816189,69255,hakerzy-w-bialych-kapeluszach(22.12.2014).

*Mail Abuse Prevention System*, http://www.mail-abuse.com/spam_def.html(12.07.2014).

Moryś A., *Geneza i ewolucja wywiadu gospodarczego*. Część pierwsza http://www.ujk.edu.pl/infotezy/ojs/index.php/infotezy/article/view/15/33(25.03.2015).

Niemczyk P., *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"* file: ///C:/Users/jwwojcik/Downloads/Piotr%20Niemczyk.pdf(10.08.2015).

Profesjonalny Wywiad Gospodarczy Skarbiec https://www.wywiad-gospodarczy.pl/kontr-wywiad-gospodarczy.html(30.XI.2017).

Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r. Warszawa 2015,

file:///C:/Users/jwwojcik/Downloads/raport_2015i%20(1).pdf(12.06.2015) http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_factorfantasy.html;(22.07.2011).

https://www.google.pl/search?dcr=0&source=hp&ei=Jed-WtK3JtCckwXIz53gCA&q=sprawozdanie+z+ogólnopolskiej+konferencji+naukowej+wywiad+i+kontrwywiad+w+teorii+i+praktyce+biznesu(dostęp 10.02.2018).

Turaliński K. https://www.e-bookowo.pl/publicystyka/wywiad-gospodarczy-i-polityczny.html(18.08.2015).

http://sjp.pwn.pl/szukaj/wizerunek(15.02.2015).