

MORAVSKÁ VYSOKÁ ŠKOLA OLMOUC  
Ústav managementu a marketingu

MYSLIKOVJAN VIKTOR

PODNIKOVÁ ŠPIONÁŽ ANEB JAK CIZÍ INFORMACE  
ZÍSKAT A O VLASTNÍ NEPŘIJÍT

CORPORATE ESPIONAGE-HOW STRANGE  
INFORMATIONS GET AND DON'T LOST OWN  
INFORMATIONS

Bakalářská práce

RNDr. Ing. Miroslav Rössler, CSc., MBA

Olomouc 2011

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a použil jen uvedené informační zdroje.

Olomouc 31. března 2011

## **Poděkování**

Rád bych poděkoval panu RNDr. Ing. Miroslavu Rösslerovi, CSc., MBA za cenné připomínky a odborné rady, kterými přispěl k vypracování této bakalářské práce. Dále bych rád poděkoval Mgr. Antonínu Novákovi, že mi poskytnul rozhovor na téma týkající se této problematiky a poskytnul mi cenné informace z oblasti práva.

# OBSAH

Úvod.....	6
1. Historie průmyslové špionáže.....	7
2. Definice základních pojmů a rozdělení.....	8
2.1 Definice základních pojmů.....	8
2.2 Hlavní důvody podnikové špionáže.....	9
2.3 Rozdělení podnikové špionáže.....	9
2.3.1 Podle typu hrozby.....	9
2.3.2 Podle typu útočníka.....	10
3. Podniková špionáž z úhlu ekonomického.....	11
3.1 Zdroje v podniku a tržní hodnota podniku.....	11
3.1.1 Práce s lidským kapitálem.....	12
3.2 Pravděpodobnost vyzrazení informací.....	14
3.3 Získávání informací.....	17
3.3.1 Dělení informací podle dostupnosti.....	17
3.3.2 Sběr a vyhodnocování informací.....	18
3.3.3 Způsoby monitorování konkurence.....	19
4. Podniková špionáž z úhlu právní.....	21
4.1 Rozhovor s Mgr. Antonínem Novákem.....	21
4.2 Obchodní tajemství.....	26
4.3 Druhy ohrožení obchodního tajemství.....	28
4.3.1 Krádež informací.....	28
4.3.2 Odposlechy.....	31
4.3.3 Podplacení/Přetažení zaměstnanců.....	32
4.4 Desatero ochrany obchodního tajemství.....	33
4.5 Soudní statistika.....	34
5. Podniková špionáž z úhlu etického.....	37
5.1 Válka vs. konkurenční boj.....	37
5.2 Význam etického kodexu.....	39
5.3 Society of Competitive Intelligence Professional (SCIP).....	40
5.3.1 SCIP Etický kodex pro Profesionály v oblasti CI.....	40

Závěr.....	41
Anotace.....	42
Literatura a prameny.....	43
Seznam obrázků.....	45
Seznam tabulek.....	46

# ÚVOD

Tématem mé bakalářské práce je „Podniková špionáž aneb jak cizí informace získat a o vlastní nepřijít“. Toto téma jsem si vybral z toho důvodu, že se jedná o oblast nanejvýš aktuální a výsostně důležitou pro řízení podniku, neboť informace jsou jednou z nejcennějších komodit podniku, ne-li tou nejcennější, vzhledem k tomu, že tomuto tématu není dosud věnovaná dostatečná pozornost a publicita. Rozhodl jsem se zpracovat danou tematiku tak, abych poskytl základní přehled přístupů k podnikové, nebo také průmyslové špionáži.

Cíl mé práce je poskytnout dostatečný přehled informací, které budou moci sloužit menším a středním firmám jako základní kámen pro tvorbu firemní strategie v této oblasti. Jako metody pro dosažení tohoto cíle jsem se rozhodl použít rozbor odborných textů a interview.

Tuto práci jsem se rozhodl rozdělit do čtyř základních částí. V první úvodní se budu zabývat definicemi pojmů a druhy rozdělení podnikové špionáže. Následovat bude ekonomická část, kde se budu dívat na celou problematiku z úhlu podniku. V právní části se budu zabývat ochranou informací popřípadě právními dopady při úniku, specifikací různých druhů úniku informací a statistickými údaji soudů. V poslední části se budu zabývat etickým hlediskem celé problematiky.

V celé práci se budu snažit provazovat teoretickou a praktickou stránku dané problematiky tak, aby docházelo k vyvození praktických závěrů použitelných v praxi.

V bakalářské práci budu čerpat především z odborných tištěných článků, internetových médií jak domácích tak i zahraničních, odborných publikací zabývajících se touto problematikou, dále budu čerpat z právních norem a zákonů České republiky, zejména však z obchodního zákoníku, který se danou tematikou do značné míry zabývá.

Věřím, že zde publikované poznatky budou přínosem pro všechny čtenáře a to i ty, kteří se nezabývají ochranou informací v podnikové sféře, na které je tato práce přednostně zaměřena, neboť praktiky zde popsané v praxi nemají za cíl zjistit informace pouze o určitém podniku, ale mnohdy i o jeho konečných zákaznících, tedy o každém z nás.

# 1. HISTORIE PRŮMYSLOVÉ ŠPIONÁŽE

„To, co nazýváme špionáží, existuje již několik tisíciletí. Tato činnost, často označovaná jako druhé nejstarší řemeslo, je pravděpodobně ještě starší než činnost úsměvně označovaná za nejstarší a mimo jiné často využívaná pro účely špionáže.“<sup>1</sup>

Lidé od pradávna prahli po informacích a co se týče špionáže, tak hlavním předmětem byly informace těch druhých, o které se nechtěli dělit. Již v pravěku například dovednost rozdělat oheň byla otázkou života a smrti. Pokud tedy nějaká skupina o svůj oheň přišla, vyslali zvěda, který oheň ukradl jiné skupině, aby zajistil přežití svého kmene. Jakmile lidé přišli na to jak oheň rozdělat, bylo zcizení tohoto postupu pravděpodobně první krádeží technického postupu.

Celá historie lidstva je ovšem propředena podobnými případy a to od prolomení tajemství výroby hedvábí, na které měla Čína kdysi monopol, přes postup výroby benátského skla až po krádeže plánů atomové bomby.

Ať se nám to líbí nebo ne, je průmyslová špionáž součástí podnikání a společně s rozvojem techniky se také stejnou rychlostí rozvíjí metody podnikové špionáže, stejně tak i obranné přístupy. Narozdíl od pravěku nastává jediná změna, nejde již o přežití kmene, ale o přežití podniku a udržení jeho pozice na trhu.

---

<sup>1</sup> J. PIEKALKIEWICZ, *Historie světové špionáže*, s. 11

## 2. DEFINICE ZÁKLADNÍCH POJMŮ A ROZDĚLENÍ

### 2.1 Definice základních pojmů

Pro celkové snazší pochopení celé problematiky jsem se rozhodl uvést hned v úvodu mé práce definice základních pojmů, se kterými budu v textu dále pracovat, aby nedošlo k mylnému výkladu. V průběhu textu budou pro větší přehlednost uvedeny další definice, které budou tematicky souviset s danou kapitolou.

#### **Špionáž**

„Označení činnosti spojené s cílem získat utajeným způsobem tajné, obvykle jiným způsobem nezjistitelné informace.“<sup>2</sup>

#### **Průmyslová špionáž**

„Průmyslová špionáž se zabývá sledováním firem nebo organizací, aby zjistila jaké inovace a plány mají ve své činnosti, aby ilegálně získala tajemství o nových výrobcích, technologiích, vzorcích nebo výrobních procesech.“<sup>3</sup>

Vzhledem k tomu, že právní řád České republiky řadí podnikovou špionáž do nekalé soutěže, uvádím zde i její zákonnou definici. Obchodnímu tajemství, které je povětšinou hlavním předmětem podnikové špionáže, je věnovaná samostatná podkapitola kapitola a jeho definici naleznete v ní společně s jejím rozbořením.

#### **Nekalá soutěž**

„Nekalou soutěží je jednání v hospodářské soutěži nebo v hospodářském styku, které je v rozporu s dobrými mravy soutěže a je způsobilé přivodit újmu jiným soutěžitelům, spotřebitelům nebo dalším zákazníkům. Nekalá soutěž se zakazuje.“<sup>4</sup>

---

<sup>2</sup> M. PEČENKA, J. BAŠTA a kol., *Encyklopedie špionáže* s. 319

<sup>3</sup> C. GIFFORD, *Svět špionáže*, s.18

<sup>4</sup> OBCHODNÍ ZÁKONÍK č. 513/1991 Sb., §43 od.1



## **2.2 Hlavní důvody podnikové špionáže:**

### **Efektivnost**

nespornou výhodou podnikové špionáže je efektivnost, neboť informace získané touto cestou jsou nesrovnatelně levnější než informace získané například vlastním výzkumem, a to jak po stránce finanční, tak i časové.

### **Tržní výhoda**

informace získané z podnikové špionáže jsou prostředek, který poskytuje jeho vlastníkům značnou výhodu na trhu. Ve vysoce konkurenčním prostředí může znalost jinou cestou nedostupných informací znamenat rozhodující konkurenční výhodu, která může ostatní účastníky na trhu uvést do tak nevýhodné pozice, že může skončit i jejich krachem.

### **Ochrana vlastních informací**

podniková špionáž může mít za účel i zjistit, zda sami nejsme sledováni, popřípadě zjistit, jaké informace má o nás naše konkurence k dispozici a na základě toho vytvořit obrannou strategii.

## **2.3 Rozdělení podnikové špionáže**

Na podnikovou špionáž se dá pohlížet z mnoha různých úhlů. Níže jsem vybral dvě nejpodstatnější rozdělení, první podle toho odkud může útok přijít a druhé podle typu útočníka.

### **2.3.1. Podle typu hrozby:**

#### **Vnitřní:**

Mezi vnitřní hrozby patří především zaměstnanci podniku, kteří se mohou buď dobrovolně nebo nedobrovolně (např. vydírání) rozhodnout poskytovat utajené informace konkurenci.

### **Vnější:**

Mezi vnější hrozby patří především konkurenční podniky, které se mohou rozhodnout porušit zákonné a etické hranice a snaží se všemi dostupnými prostředky získat tajné informace, nebo destabilizovat podnik například softwarovou sabotáží.

### **2.3.2 Podle typu útočníka:**

#### **Jednotlivce**

do této skupiny spadají například hackeři pracující na vlastní pěst, kteří se snaží nabourávat do cizích informačních systémů a následně se z nich snaží informace prodat konkurentům na trhu. Dále sem řadíme vlastní zaměstnance, kteří nás zradí.

#### **Firmy**

většinou se jedná o konkurenční firmu, která se snaží zjistit údaje o svém konkurentovi a využívá k tomu všech dostupných metod.

#### **Státy**

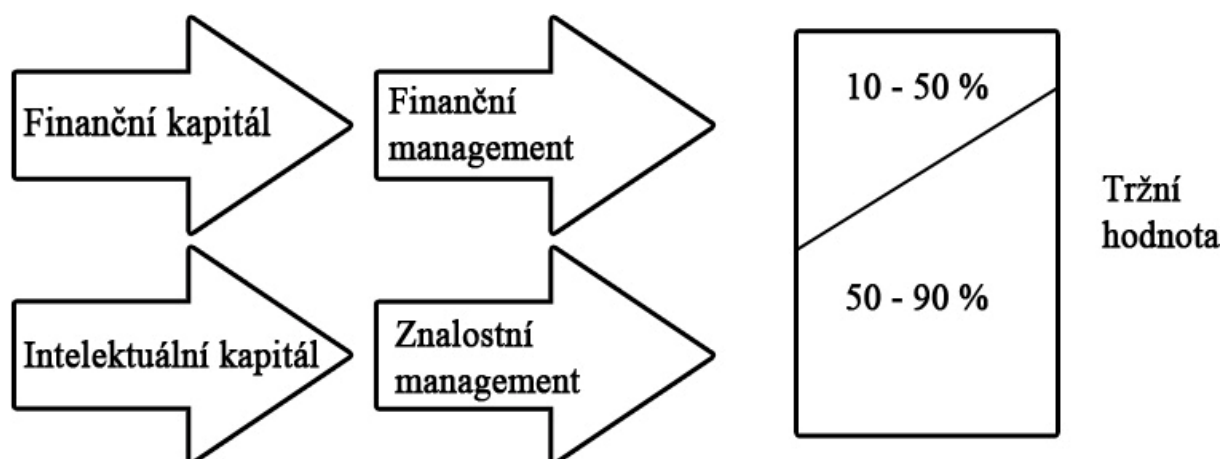
u význačných projektů se nedá vyloučit, že o informace, které spadají do firemního tajemství, projeví zájem i tajné služby cizích států. Problém je v tom, že tito agenti jsou perfektně školeni a disponují v podstatě neomezeným množstvím prostředků a špičkové techniky pro splnění úkolů.

### 3. PODNIKOVÁ ŠPIONÁŽ Z ÚHLU EKONOMICKÉHO

Informace a znalosti mají pro podnikání naprosto zásadní význam. Dá se v podstatě říci, že jejich znalost či neznalost rozhoduje o úspěchu. Z tohoto důvodu se v této části budu nejdříve zabývat tím, jaký je jejich vliv na tržní hodnotu podniku. Dále se zaměřím na pravděpodobnost, že se podaří udržení informace v tajnosti. Získávání informací bude dalším tématem, neboť pro podnik není podstatné pouze chránit své informace, ale pokud možno i získat co nejvíce informací o své konkurenci.

#### 3.1 Zdroje v podniku a tržní hodnota podniku

Hodnota podniku je pojem, který se velmi těžko specifikuje. Velmi zjednodušeně se dá říci, že hodnotu podniku odráží jeho zdroje a jejich využití. Zdroje podniku můžeme rozdělit na hmotné a nehmotné, finanční a intelektuální atd. Existuje mnoho pohledů na tuto problematiku. Pojďme se nyní podívat na to, jakou mohou mít hodnotu informace v rámci tržní hodnoty celého podniku.



Obr. 1 Tržní hodnota podniku<sup>5</sup>

Z výše uvedeného schématu je vidět, že informace vlastněné podnikem se do jeho tržní hodnoty promítají v 50% až 90%, zatímco finanční zdroje se do tržní

<sup>5</sup> V. BUREŠ, *Znalostní management a proces jeho zavádění*, s. 32

hodnoty podniku promítají v 10 až 50% jeho hodnoty. Samozřejmostí je, že tento podíl se mění v závislosti na tom, v jakém oboru daná společnost podniká. Neboť know-how, které vlastní například McDonald's, je sice velmi cenné, ovšem i v případě jeho zcizení má firma zázemí ve své značce a v množství poboček. Zatímco pro firmy, zabývající se například spekulativním investováním do pozemků, může být odhalení jejich investičních záměrů osudové. Není proto potřeba říkat, že investice do ochrany informací by měly odpovídat hodnotě, kterou pro nás tyto informace představují.



Obr. 2 Model tržní hodnoty společnosti podle společnosti <sup>6</sup>

Podíváme-li se blíže na strukturu intelektuálního kapitálu, tak jak ji popisuje Bureš ve své knize, dostaneme přehled základních oblastí, které se nejčastěji stávají předmětem podnikové špionáže. Každá z těchto oblastí potřebuje při své ochraně svůj specifický přístup, který budu dále rozebírat v kapitole „4.3 Druhy ohrožení obchodního tajemství 28 s.“. Pouze oblast týkající se lidského kapitálu jsem se rozhodl zařadit také do této části, neboť k ní tematicky náleží.

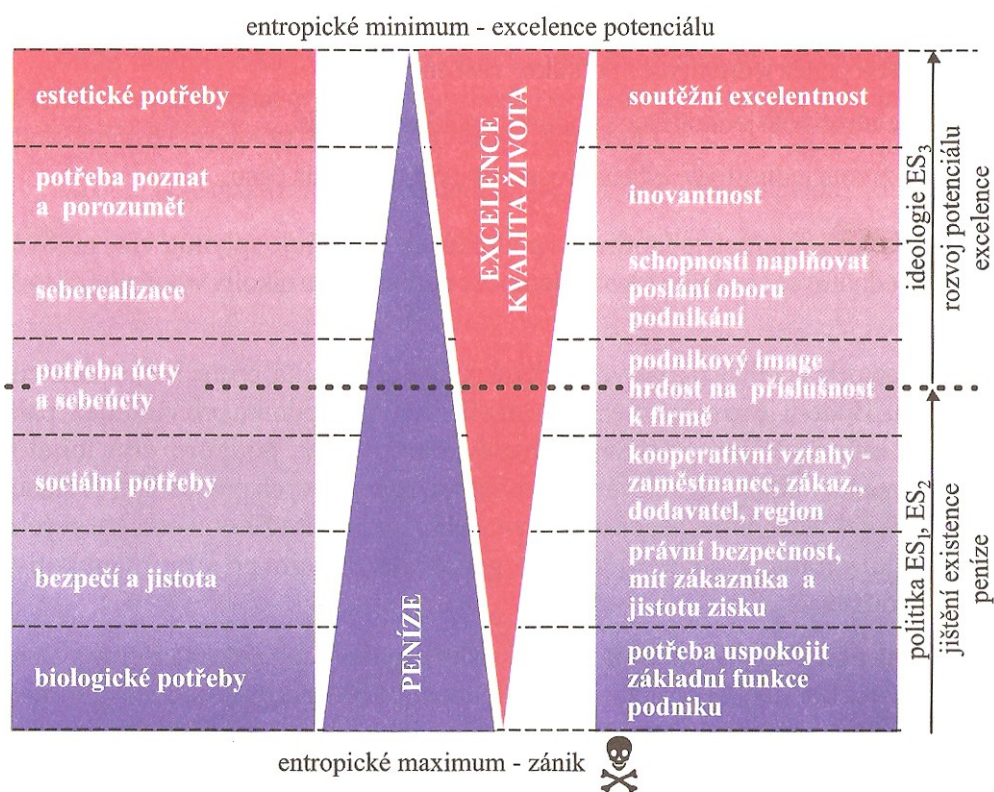
### 3.1.1 Práce s lidským kapitálem

Vzhledem k tomu, že určitá část zaměstnanců společnosti přichází přímo do styku s utajovanými nebo minimálně neveřejně dostupnými informacemi, je potřeba zajistit opravdu kvalitní výběr těchto zaměstnanců, předtím než dostanou přístup k

<sup>6</sup> V. BUREŠ, *Znalostní management a proces jeho zavádění*, s. 32

informacím a to tak, abychom minimalizovali riziko například nespolehlivosti ze strany zaměstnance apod.

Ovšem i sebelépe vybraný zaměstnanec může podlehnout pokušení a rozhodnout se předat utajované informace konkurenci, pokud nejsou v podniku uspokojovány jeho základní potřeby. Z toho důvodu je nutné, aby management nezapomínal na potřeby svých zaměstnanců a harmonizoval je spotřebami podniku. Tímto totiž můžeme minimalizovat pravděpodobnost, že se daný zaměstnanec rozhodne prodat tajné informace konkurenci.



Obr. 3 Pyramida potřeb, člověka i podniku<sup>7</sup>

Z výše uvedeného schématu je jasné, že pro člověka je hlavní prioritou uspokojení jeho biologických potřeb. Pokud dochází k jejich uspokojení, snaží se zaměstnanec uspokojit své další potřeby, jako je používání patřičné úcty a seberealizace. Pokud není ze strany podniku potřebám zaměstnance věnovaná dostatečná pozornost, stanou se příčinou nespokojenosti, která může vyústit v ohrožení utajovaných informací. Zaměstnanci provozují podnikovou špionáž z dvou hlavních důvodů:

<sup>7</sup> A. KOPČAJ, *Řízení proudu změn*, s. 131

## 1) Peníze

Finanční ohodnocení je jedním z hlavních motivů, proč se zaměstnanci rozhodnou zradit svou stávající společnost a prodat její obchodní tajemství konkurenci. Pokud lidé, kteří se podílejí na tvorbě obchodního tajemství, popřípadě s ním přicházejí přímo do styku, nejsou patřičně dle své důležitosti ohodnoceni, vznikne u nich pocit, že je firma vykořisťuje a rozhodnou se jí to „oplatit stejnou mincí“.

## 2) Nedostatek uznání

Touha po společenském uznání je mnohdy mnohem silnější než touha po finančním ohodnocení. Tento fakt je potřeba nepodceňovat, neboť zaměstnanec, který nebude cítit dostatek uznání ve společnosti, může začít být frustrovaný a bude více svolný při poskytnutí interních údajů konkurenci, když uvidí, že za ně obdrží obdiv a uznání, které se mu v jeho stávající práci nedostává.

## 3.2 Pravděpodobnost vyzrazení informací:

Existuje mnoho faktorů, které ovlivňují pravděpodobnost, že daná informace zůstane utajena. Ovšem nezávisle na tom o jakou informaci se jedná, zde existují vždy dva faktory, které ovlivňují pravděpodobnost, že daná informace bude zcizena. Je to spolehlivost nositele informací a počet nositelů informací. Nejlépe tuto pravděpodobnost popisuje vzorec:

$$P = s^n$$

Kde:

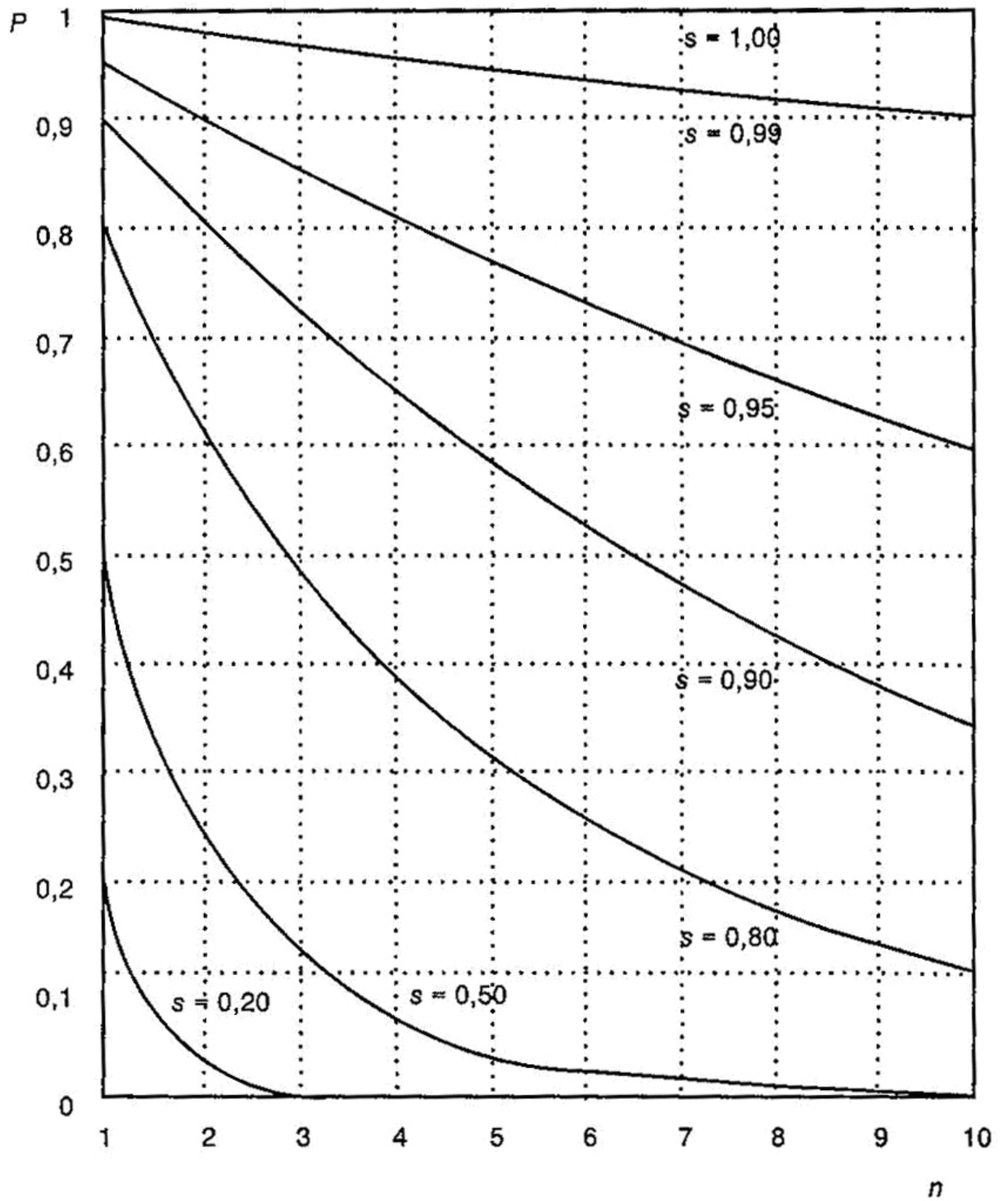
P – je pravděpodobnost, že dané informace nebo jejich soubor zůstanou utajeny

s – je spolehlivost daného nositele informací

n – je počet nositelů dané informace<sup>8</sup>

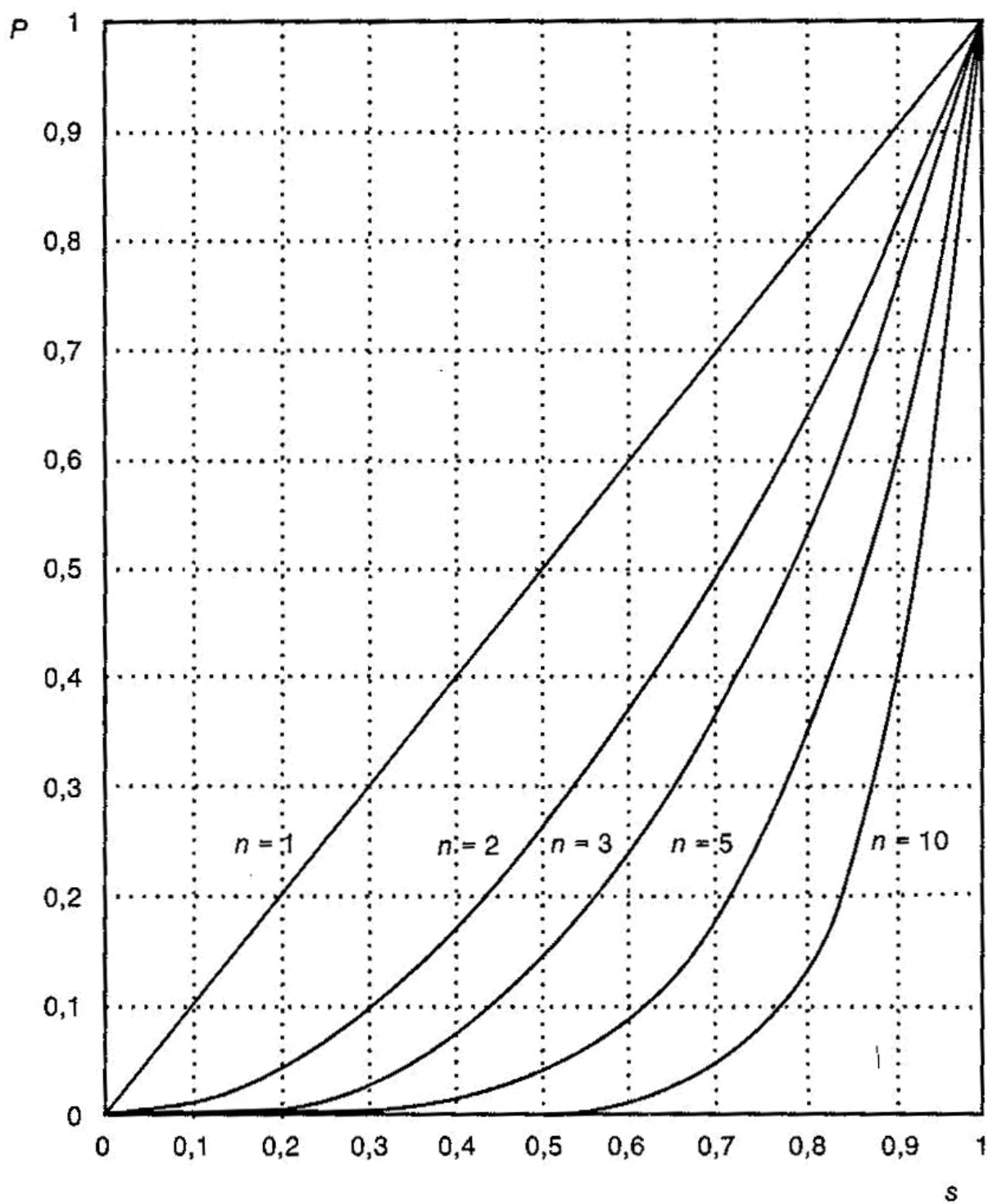
---

<sup>8</sup> F. BARTES, *Konkurenční strategie firmy*, s. 39



Obr. 4 Grafické znázornění pravděpodobnosti utajení informace k počtu nosičů<sup>9</sup>

<sup>9</sup> F. BARTES, *Konkurenční strategie firmy*, s. 40



Obr. 5 Grafické znázornění pravděpodobnosti utajení informace ke spolehlivosti nosiče informace<sup>10</sup>

<sup>10</sup> F. BARTES, *Konkurenční strategie firmy*, s. 40



Z grafického znázornění vztahu  $P = s^n$  jasně vyplývá, že čím více je nositelů dané informace, tím větší je pravděpodobnost jejího následného vyzrazení.<sup>11</sup>

Co se týká ochrany informací, je tedy nejdůležitější uchovávat tyto informace pouze po nezbytnou dobu, a to v co nejmenším počtu kopií tak, aby k nim měli přístup pouze lidé, kteří dané informace potřebují nezbytně k výkonu své práce.

### **3.3 Získávání informací**

To, že společnost monitoruje aktivity svého konkurenta ještě neznamená, že se jedná o neetické nebo dokonce nezákonné jednání. Naopak se jedná o korektní prostředek používaný v rámci konkurenčního boje, pokud se tedy nepřekračují meze stanovené zákonem.

#### **3.3.1 Dělení informací podle dostupnosti:**

##### **1) Informace volně dostupné**

Tento typ informací je běžně dostupný. Patří sem tisková prohlášení, výsledky společnosti, ceníky, které společnost sama zveřejňuje a informace, které jsou volně k dispozici například v obchodním rejstříku apod.

##### **2) Informace spadající do obchodního tajemství**

Tyto informace jsou přesně definovány zákonem a podrobněji o nich bude pojednáno v samostatné kapitole.

Vzhledem k tomu, že druhý typ informací je chráněn zákonem, budu se zde zabývat pouze získáváním informací volně dostupných.

#### **3.3.2 Sběr a vyhodnocování informací**

Tato činnost má mnoho společného s podnikovou špionáží. Jejím cílem je totiž také zjistit pokud možno co nejvíce o konkurenci na trhu a to pokud možno utajeným způsobem, neboť vzbudit pozornost v tomto ohledu není logicky žádoucí, nikoliv

---

<sup>11</sup> Srov. F. BARTES, *Konkurenční strategie firmy*, s. 40-41

z důvodu obavy trestního postihu, ale ze ztráty konkurenční výhody. Celý proces získávání informací má několik etap.

### **Aktivní soutěživé zpravodajství**



Obr. 6 Schéma činností při získávání informací <sup>12</sup>

Z tohoto schématu jasně vyplývá, že podnik nejprve monitoruje činnost konkurence a následně se snaží získat co nejvíce informací o jednotlivých činnostech. Dále proběhne ověření, zda dané údaje získané při sběru informací jsou skutečně věrohodné. Po důkladné analýze těchto údajů pak dojde k přijetí rozhodnutí, jak bude podnik dále postupovat.

---

<sup>12</sup> V. BUREŠ, *Znalostní management a proces jeho zavádění*, s. 118

### 3.3.3 Způsoby monitorování konkurence

#### 1) Samostatný monitoring

Společnost sama provádí celý proces sběru a vyhodnocování informací o konkurenci.

##### **Výhody:**

Pokud společnost tuto činnost provádí sama, má mnohem větší pravděpodobnost, že takto získané informace se nedostanou do nepravých rukou. Neboť jak z výše uvedené pravděpodobnosti vyzrazení informace vyplývá, čím méně subjektů o dané informaci vědí, tím větší je pravděpodobnost, že zůstane utajena. Druhou výhodou je, že takto získané informace jsou mnohem levnější než při využití speciálních agentur, které se touto činností zabývají.

##### **Nevýhody:**

Sběr a vyhodnocování informací o konkurenci je velmi sofistikovaná záležitost a často je velký problém sehnat dostatečně kvalifikované zaměstnance, kteří mají s touto činností patřičné zkušenosti.

#### 2) Využitím profesionální agentury

Jedná se o společnost, která za vás zjistí požadované informace a případně zpracuje profil vaší konkurenci. Pokud chcete mít jistotu, že daná společnost operuje v mezích zákona, můžete si zjistit, zda je tato společnost členem organizace SCIPs (The Society of Competitive Intelligence Professional), což můžeme volně přeložit jako Sdružení profesionálů konkurenčního zpravodajství. V tomto sdružení se členové zavazují dodržovat nejen právní, ale i etické postupy při získávání informací.<sup>13</sup>

---

<sup>13</sup> Srov. NICK WALKER, *Marketing: Know your enemy*, dostupné na <<http://www.independent.co.uk/life-style/marketing-know-your-enemy-1526528.html>>

**Výhody:**

Dané společnosti většinou disponují dostatečným množstvím kvalifikovaného personálu a mají vyvinuty své ověřené interní postupy pro co nejefektivnější a nejrychlejší získávání informací. Další výhodou je, že dané výstupy jsou již profesionálně zpracovány a vyhodnoceny, takže zadávající společnost může pouze přijmout opatření na základě informací, které obdrží.

**Nevýhody:**

Ne každá společnost musí nezbytně poskytnout skutečně hodnotné informace, či postupovat naprosto legitimní cestou. Jak už je výše zmíněno, nejlepší je spolupracovat se společnostmi, které mají dobré reference a jsou členy SCIPs. Ovšem ani to nemůže být stoprocentní zárukou. Další nevýhodou je, že nemůžeme vědět, zda daná společnost informace, které zpracovala pro nás, ještě neposkytuje také třetí straně, která například podniká ve stejném odvětví. V nejhorším případě se může i stát, že daná společnost nám může poskytovat cílené desinformace, popřípadě informace získávat od nás pro konkurenci. Kromě toho zde opět platí pravidlo, že čím více nositelů informací existuje, tím větší je pravděpodobnost, že dojde k jejich prozrazení.

V této kapitole jsem se zabýval hlavně důležitostí informací pro podnik, konkrétně jak se promítají do jeho tržní hodnoty. Rozborem intelektuálního kapitálu jsme získali možné oblasti, na které se podniková špionáž zaměřuje, jejichž ochranou se budu zabývat dále. Na základě vzorce o pravděpodobnosti utajení dané informace jsem stanovil daná opatření, jak maximálně eliminovat riziko prozrazení tajných informací a v poslední části jsem se zabýval procesem sběru informací o konkurenci. Oba uvedené postupy mají svoje pozitiva a negativa a záleží na každé společnosti jaký způsob zvolí.

## **4. PODNIKOVÁ ŠPIONÁŽ Z ÚHLU PRÁVNÍ**

### **4.1 Rozhovor s Mgr. Antonínem Novákem**

Tématem tohoto rozhovoru bude obchodním tajemství, trestní odpovědnosti právnických osob, konkurenční doložka a doložka o mlčenlivosti. Neboť se jedná o důležité právní oblasti vztahující se přímo či nepřímo k podnikové špionáži a ochraně obchodního tajemství.

Mgr. Antonín Novák absolvoval v roce 2002 Právnickou fakultu MU. Ve stejném roce začal také právní praxi. Od roku 2006 má svojí vlastní praxi jako samostatný advokát.

**Myslíte si, že v České republice je dostatečné právní zázemí pro ochranu obchodního tajemství a hospodářské soutěže?**

Ano, právní úprava v této oblasti je srovnatelná řekněme s právními úpravami v jiných členských zemích EU. Právní úprava hospodářské soutěže i její dílčí suboblasti nekalé soutěže je ovlivněna předpisy Evropských společenství a v širším kontextu i mezinárodními závazky České republiky.

**Takže to právo na ochranu hospodářské soutěže je více méně po celé EU unifikováno?**

Právo na ochranu hospodářské soutěže je do značné míry unifikováno, vychází v zásadě z evropských směrnic. To se týká zejména antimonopolního práva, ale ve značné míře i práva na ochranu před nekalou soutěží. Na vysvětlenou je třeba dodat, že právo na ochranu hospodářské soutěže můžeme velmi zhruba rozčlenit na dvě velké oblasti. A to na právo na ochranu hospodářské soutěže v užším smyslu (antimonopolní), které náleží do oblasti veřejného práva, a které se zabývá např.

kartelovými dohodami apod. a právem na ochranu před nekalou soutěží, které řadíme do oblasti soukromého práva, a které je upraveno především v ust. § 44 a násl. obchodního zákoníku.

### **Jaké právní normy upravují „ochranu před podnikovou špionáží“?**

Záleží na tom jak pojem „ochrana před podnikovou špionáží“ definujete. Pokud za podnikovou špionáž považujete snahy o neoprávněné získání údajů, které jde definovat jako obchodní tajemství podle §17 Obchodního zákoníku, je možno použít vůči pachateli širokou paletu právních prostředků, jejichž použití je ovšem odvislé od okolností jednotlivého případu. Pokud hovoříme o právních sankcích, jejich použití závisí na mnoha různých faktorech- na postavení tzv. pachatele, který informace tvořící obchodní tajemství získá, či se je snaží získat. Tedy zda jde o zaměstnance, obchodního konkurenta či jinou osobu, způsob provedení „útoků“ - vloupáním, popř. hackerským útokem, dále jak „daleko“ se pachatel ve své snaze získat a nekalým způsobem využít informace tvořící obchodní tajemství dostal a popř. jak vysokou způsobil škodu apod.

V úvahu připadají samozřejmě nejen sankce, které plynou z porušení práv na ochranu před nekalou soutěží, které najdete v obchodním zákoníku, ale dle okolností případu i např. sankce pro zaměstnance dle zákoníku práce, popř. trestní postih.

### **Jaké jsou právní prostředky pro ochranu „obchodního tajemství“?**

K problematice jsem se již vyjádřil v předchozí otázce, jedná se o obecné právní prostředky ochrany práva na ochranu před nekalou soutěží uvedené v ust. § 53 obchodního zákoníku a dále dle okolností případu i jiné prostředky právní ochrany – jako příklad možno uvést např. postižení pachatele, který se vloupal do areálu závodu likérky, kde po vylomení dveří odcizil recepturu – návod na výrobu likéru. Pachatel by se dopustil trestného činu krádeže, pokud by obchodní tajemství využil a způsobil likérce újmu nebo získal prospěch ve větším rozsahu. Svým jednáním by naplnil i skutkovou podstatu trestného činu, čin dle ust. § 248 trestního zákoníku – porušení předpisů o pravidlech hospodářské soutěže.

## **Jak moc podle vás ovlivní nově schválená trestní odpovědnost právnických osob v České republice podnikovou špionáž ?**

Jestli dovolíte, na tuto otázku odpovím poněkud obecně. Co se týče odpovědnosti právnické osoby, je třeba rozlišovat tzv. pravou trestní odpovědnost, která je odpovědností za trestný čin, tj. za soudně trestní delikt podle trestního zákoníku nyní platného a mezi jinými formami odpovědnosti právnické osoby za protiprávní jednání, např. odpovědnost za spáchaný správní delikt, popřípadě civilně právní odpovědnost např. způsobenou škodu.

Práva a trestní odpovědnost právnických osob za trestně spáchané činy je značně problematická, protože z povahy věci platí, že trestné činy páchají fyzické osoby. Žádnou účelovou argumentací nemůžete zastíit fakt, že zaviněné protiprávní skutky, které nesou znaky trestného činu, mohou páchat pouze jen fyzické osoby – živí lidé. Zkušenosti z blízkých zemí (např. z Polska) ukazují, že i v praxi je uplatňování tohoto typu odpovědnosti velmi problematické.

## **Mohu se zeptat které země EU již mají zavedenou trestní odpovědnost právnických osob?**

Například Polsko, Velká Británie a Francie.

## **Proč si myslíte, že byla schválena trestní odpovědnost právnických osob v České republice, když se v zahraničí příliš neosvědčila?**

Formální argument byl ten, že tuto legislativu již všechny ostatní státy Unie zavedly a již nebylo zmíněno, že se nejedná o povinnost ve smyslu zavedení tzv. pravé trestní odpovědnosti právnické osoby, o které jsem již hovořil. Kromě toho například v Německu si vystačí s odpovědností za správní delikt, která plní v podstatě stejnou funkci.

## **Jaký je váš názor na trestní odpovědnost právnických osob? Má podle vás význam?**

Dle mého názoru bude mít právní odpovědnost firem značně negativní vliv na vlastníky podniků, kdy se jejich zaměstnanci dopustí trestné činnosti jménem společnosti, formálně „ve prospěch společnosti“, ale fakticky ve svůj prospěch, neboť pachatelé hospodářské trestné činnosti páchají tuto trestnou činnost typicky ve svůj prospěch.

Například pokud akciová společnost ABC nedovoleným způsobem vykáčí velkou část lesa, což může být trestným činem, konkrétní viník (člen představenstva) bude potrestán třeba odnětím svobody a kromě toho bude společností státním orgánem na ochranu lesa udělena značná pokuta. Teď si představte situaci, že viník byl odvolán z funkce, škoda i pokuta byla akciovou společností uhrazena a společnost je obžalována z trestného činu a musí čelit hrozbě dalších duplicitních sankcí, včetně i hrozby zrušení společnosti.

## **Konkurenční doložka**

**Dále bych se rád zeptal jaké právní normy upravují konkurenční doložku, popřípadě zda se dá použít při ochraně obchodního tajemství?**

Konkurenční doložka je upravena § 310 Zákoníku práce. Její podstata spočívá v tom, že se zaměstnanec zaváže zdržet po určitou dobu výdělečné činnosti ve stejném oboru činnosti jako zaměstnavatel, popř. činnosti, která má ve vztahu k poslední zmíněné soutěžní povahu. K tomu vám mohu říci, že ve většině případů není hospodářský důvod pro to, proč by zaměstnanec měl být takto omezován. Kromě toho je zaměstnavatel povinen po dobu, kdy takto zaměstnance omezuje – a délka tohoto omezení nesmí přesáhnout jeden rok - vyplácet peněžité vyrovnání, nejméně však ve výši průměrného měsíčního výdělku. V praxi jsem se s uplatněním konkurenční doložky neseťkal.



## **Do jaké míry si myslíte, že je vymahatelná konkurenční doložka?**

Vymahatelnost konkurenční doložky může být značně problematická, neboť zaměstnanec může vyvíjet výtěžnou činnost, která má soutěžní povahu ve vztahu k činnosti, kterou vykonával v pracovním poměru např. prostřednictvím nastrčené osoby, což se reálně velmi těžko dokazuje. Z tohoto důvodu to moc praktické není.

## **Já osobně jsem se setkal s omezením činnosti i po ukončení pracovního poměru a to po dobu 5 let od ukončení pracovního poměru a bez proti plnění. Mám tomu rozumět, že takto formulovaná konkurenční doložka je neplatná?**

Ano, takto formulovaná doložka je neplatná pro rozpor se zákonem, neboť zde není stanoveno odškodné pro zaměstnance splňující zákonné podmínky. Kromě toho omezení zaměstnance ve smyslu nevykonávat po ukončení pracovního poměru činnost, která má soutěžní povahu s předmětem činnosti zaměstnavatele, nesmí trvat déle než 1 rok. Delší omezení zaměstnance v tomto směru zákon neumožňuje.

## **Jde konkurenční doložku použít u všech zaměstnání nebo existují některé výjimky?**

Konkurenční doložku lze použít u všech zaměstnání, jedinou výjimkou jsou činnosti uvedené v ust. § 311 Zákoníku práce.

## **Mlčenlivost**

### **Jak moc je podle vás častá doložka o mlčenlivosti v pracovních smlouvách v České republice?**

Doložka o mlčenlivosti se v pracovních smlouvách objevuje poměrně často. V zásadě sankce za porušení mlčenlivosti jsou stanoveny jako u porušení povinnosti z pracovního poměru. Je možno vymáhat škodu, pokud byla způsobena, jedná - li se o pracovní smlouvy zakládající pracovní poměr, ale ve většině případů se porušení

mlčenlivosti velice těžko prokazuje a ani se v praxi moc často neobjevuje, že by byla smluvní povinnost mlčenlivosti, ke které se zaměstnanec zavázal v pracovní smlouvě ze strany zaměstnavatele nějak vymáhána, resp. sankcionována.

Podle zákoníku práce je povinnost mlčenlivosti uložena určitým kategoriím státních zaměstnanců – viz. ust. § 303 odst. 1 a 2 písm. b) cit. Předpisu. Povinnost mlčenlivosti ukládají i jiné obecně závazné předpisy, např. existuje povinnost mlčenlivosti zdravotnických pracovníků apod.

### **Na co vše se může „smluvní“ mlčenlivost zaměstnanců vztahovat?**

Povinnost mlčenlivosti nutno definovat tak, aby tzv. kryla skutečnosti, které nejsou obecně známé, a které je třeba v rámci oprávněného hospodářského zájmu zaměstnavatele nesdělovat třetím subjektům. Domnívám se, že povinnost mlčenlivosti se nemusí striktně vztahovat pouze na obchodní tajemství. V zásadě by se povinnost mlčenlivosti neměla vztahovat na obecně známé skutečnosti, obvyklé technické postupy, s čímž se lze v praxi občas setkat.

## **4.2. Obchodní tajemství**

„Předmětem práv náležejících k podniku je i obchodní tajemství. Obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje.“<sup>14</sup>

Co musí obchodní tajemství splňovat, aby bylo jeho případné zcizení vymahatelné u soudu a co se skrývá pod jednotlivými pojmy:

---

<sup>14</sup> Obchodní zákoník, č. 513/1991 Sb., §17  
<<http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx>>

### **Skutečnosti povahy obchodní, výrobní či technické**

Do této oblasti patří zejména seznamy zákazníků, dodavatelů či odběratelů, ceníky, výkazy obrátů a výkonnosti středisek, výběrová kritéria, marketingové strategie, technické dokumentace, postupy, plány výroby, výsledky pokusů či výzkumů, dosud nechráněné postupy a mnoho dalších.

### **Skutečnost souvisí s podnikem**

Souvislost s podnikem, tedy dané informace jsou nezbytné například pro řízení podniku například (nákupní kritéria), nebo budou v budoucnu podniku sloužit, například (strategické plány pro expanzi)

### **Skutečnosti, které mají skutečnou, nebo alespoň potenciální materiální nebo nemateriální hodnotu**

Zde se hlavně posuzuje, zda má daná informace vyjádřitelnou hodnotu v penězích. Například hodnota databáze klientů podniku se dá odvodit podle toho, jaký přínos by pro společnost daní klienti měli, pokud by o ně společnost nepřišla.

### **Daná skutečnost není v příslušných obchodních kruzích běžně dostupná**

Jedná se tedy o informaci, kterou si nemohou ostatní konkurenti podniku běžně jinde obstarat a jejím zcizením vlastník přichází oproti konkurenci o svou výhodu.

### **Podnikatel má vůli k utajení skutečnosti**

Obchodní tajemství má nárok na ochranu ze strany zákona, pokud má podnikatel vůli obchodní tajemství tajit. Sám tedy jedná podle toho, že daná informace má značnou hodnotu a není běžně dostupná ostatním konkurentům na trhu. Tím se rozumí, že podniká i kroky k ochraně daného tajemství. Vzhledem k tomu, že zákon přesně nestanoví, jak má projev dané vůle vypadat, lze jen doporučit provést ho formou písemnou, kde specifikuje daný podnikatel charakter informací, které považuje za podnikové tajemství. Tím se vyhne zbytečným potížím při soudním vymáhání.

### **Podnikatel odpovídajícím způsobem zajistí utajení skutečnosti**

Jak má podnikatel zajistit dané informace zákon nestanoví. Nejlépe je zajistit zabezpečení daných informací dle jejich povahy, utajované soubory mít za heslované

na oddělených discích, prototypy a výsledky výzkumu v zabezpečených prostorách apod. Není nutné psát, že podcenění ochrany může mít pro podnik fatální následky, neb únik informací nejvyšší důležitosti může nenávratně poškodit postavení podniku a ani 10 vyhraných soudních při už to nedokáže napravit.

Pokud obchodní tajemství nespĺňuje byt' jedinou podmínku ze zákonné definice, nejedná se podle zákona o obchodní tajemství a nebude tak zcizení daných informací posuzováno u soudu.

### **4.3. Druhy ohrožení obchodního tajemství:**

Zde se pokusím specifikovat nejčastější druhy útoků vedených při podnikové špionáži. Každé ohrožení bude nejprve stručně specifikováno, následně zde nastíním možnosti prevence a případný postup jak jednat pokud již došlo k narušení bezpečnosti v podniku a informace byly zcizeny.

#### **4.3.1 Krádež informací**

Krádež informací může mít 3 základní podoby:

##### **Vloupání**

##### **Popis:**

Zloděj fyzicky vnikne do prostor společnosti a odcizí dokumenty, které jsou součástí obchodního tajemství.

##### **Prevence:**

Na trhu existuje mnoho bezpečnostních systémů pro zabezpečení firemních prostor, včetně alarmů a kamerových systémů apod. Kromě toho se na českém trhu vyskytuje bezpočet bezpečnostních agentur, které nabízí zabezpečení daných objektů a v případě vniknutí do objektu ihned vyšlou své zaměstnance, aby celou situaci zkontrolovali.

**Narušení:**

Pokud dojde ke krádeži obchodního tajemství, většinou jedinou možností je kontaktovat policii a doufat, že pachatele zadrží dříve, než stihne dané informace zneužít a spáchá tak pro podnik nenahraditelné škody. Bohužel ke spoustě případů policie zavolána není, neboť vedení společnosti mívá takový strach ze zveřejnění skutečnosti, že jejich obchodní tajemství bylo zcizeno, že se radši rozhodne kontaktovat soukromé detektivní společnosti, aby dopadly pachatele.

**Vynesení informací zevnitř společnosti****Popis:**

V tomto případě se většinou zaměstnanci nebo i někteří ze společníků rozhodnou prodat obchodní tajemství konkurenci. Narozdíl od vloupání je mnohem těžší specifikovat, kdy k odcizení informací došlo, popřípadě osoba, která krade informace, nemusí být nikdy odhalena.

**Prevence:**

Část preventivních opatření je zmíněna v kapitole“3.1.1 Práce s lidskými kapitálem s. 12“, která se zabývá motivací a ohodnocení zaměstnanců.

Další možností prevence je striktní specifikace, která pozice má přístup k danému typu informací a to tak, aby byl měl každý zaměstnanec informace, které potřebuje k výkonu své činnosti, ale již neměl přístup k ostatním utajovaným informacím. S tím souvisí oprávnění vstupu do určitých částí podniku.

Do této části patří i prověrky zaměstnanců a jejich kontrola při styku s citlivými údaji. Není až tak nezvyklé, že zaměstnanci, pracující na strategických projektech, podléhají striktním osobním prohlídkám a pracují pod kamerovým dohledem.

Další způsob ochrany je instalace speciálního softwaru, který zaznamenává, se kterými dokumenty daný zaměstnanec pracoval, popřípadě které dokumenty a kam odesílal či kopíroval. Tyto prostředky značně ulehčí, v případě narušení bezpečnosti, specifikovat rozsah způsobených škod. Mimoto daný software může upozornit na nepovolené kopírování či neoprávněné odesílání dokumentů ze společnosti a pomoci chytit viníka při činu.

**Narušení:**

Vzhledem k tomu, že dopadení interního viníka bývá často velmi komplikovaná záležitost a ne vždy se podaří pachatele dopadnout, většina firem v tomto ohledu vůči svým zaměstnancům postupuje naprosto nekompromisně a skoro vždy tyto případy končí u soudu.

**„Nabourání“ systému informačního systému****Popis:**

Do informačního systému společnosti se nabourá „škůdce“, který zde vyhledává a stahuje tajné informace. Existuje mnoho forem - počítačových útoků přes různé viry, červy a trojské koně.

**Prevence:**

K prevenci patří řádné zabezpečení podnikové sítě, včetně antivirů a firewallů. Na trhu je pro firmy bezpočet softwarových řešení, které slibují nejrůznější stupně ochrany. Neméně důležité je také poučit zaměstnance, aby nestahovali přílohy a soubory z neznámých stránek a e-mailů, neboť tím mohou nevědomky narušit bezpečnost celé sítě. Další možností je používání různého šifrování. Existuje mnoho dalších metod jak zajistit zabezpečení firemní sítě.

**Narušení:**

Vzhledem k tomu, že tyto útoky jsou koncipovány tak, aby poškozený pokud možno neměl ani zdání o tom, že byl o nějaké údaje připraven, bývá škůdce většinou neodhalen. Proto je potřeba o to více věnovat pozornost prevenci. V těchto málo případech, kdy dojde k tomu, že poškozený přijde na to, že bylo vniknuto do jeho systému, nezbyvá než posílit obranná opatření, neboť většina těchto útoků bývá vedena ze zahraničních serverů, kdy reálné dopadení viníka je mizivé.

### 4.3.2 Odposlechy:

#### Mobilního telefonu

##### Popis:

Odposlech mobilního telefonu je v dnešní době velmi populární. Jeden z nejefektivnějších způsobů je úprava mobilního telefonu, kdy útočník vám zcizí na chvíli mobilní telefon a nechá jej upravit. Má pak přehled o tom komu voláte, nebo může využívat mikrofon telefonu jako štěnici.<sup>15</sup>

##### Prevence:

Je potřeba nenechávat firemní a osobní mobilní telefony bez dozoru. Například nenechat ležet telefon v restauraci na stole, zatímco si odskočíte na toaletu. Dále řešit věci týkající se obchodního tajemství nejlépe pouze osobně. Další možností jsou preventivní kontroly mobilních telefonů, které jsou ovšem velmi nákladné.

##### Narušení:

Pokud máte pocit, že je váš telefon odposloucháván, můžete si jej nechat překontrolovat zvláštními agenturami, které mají vybavení, aby tento druh infiltrace odhalily. Nicméně pravděpodobnost dopadení viníka je minimální až nulová. Pokud ho nechytnete přímo při činu.

#### Štěnice

##### Popis:

Útočník buďto pronese do společnosti Mirko zařízení, které zaznamenává zvuk, nebo do počítače nainstaluje software<sup>16</sup>, který využívá mikrofonu pro odposlech, zatímco jeho majitel o tom nemá nejmenšího tušení. Tyto zařízení mohou mít nejrůznější podobu jako například při slavné aféře Watergate.

---

<sup>15</sup> Srov. TANGO spol. s r.o., *Odposlech mobilního telefonu S-GSM* <<http://www.odposlechy.com/odposlech-mobilniho-telefonu/>>

<sup>16</sup> Srov. GOLDSILVER, s.r.o., *Odposlech počítače, SKYPE, ICQ, monitoring provozu PC*, dostupné na: <<http://www.goldsilver.cz/odposlech-pocitace-skype-icq-monitoring-provozu-pc/>>

**Prevence:**

Dávat pozor především na návštěvníky ve společnosti, kteří se dostaví na pohovor, nebo například na instalatéry apod. Je třeba nenechávat tyto osoby o samotě. Pokud možno zamezit těmto lidem vstup do místností, kde probíhají strategické porady apod. Stejně tak u počítačů provádět striktní kontroly, zda nedošlo k bezděčné infiltraci.

**Narušení:**

Pokud máte pocit, že došlo k narušení, je nejlépe vyhledat pomoc specializovaných agentur, jež se zabývají vyhledáváním podobných zařízení a softwaru. I v tomto případě je však možnost chycení pachatele minimální.

**4.3.3. Podplacení/Přetažení zaměstnanců****Popis:**

Zaměstnanec podává úmyslně strategické informace vašemu konkurentovi.

**Prevence:**

Je nutné dbát na to, aby zaměstnanci, kteří přicházejí do styku s informacemi strategického charakteru, nebo dokonce týkající se obchodního tajemství, byli patřičně zaplacení a sdíleli podnikovou kulturu.

**Narušení:**

Při narušení je potřeba zjistit typ informací, které byly zcizeny a následně podniknout patřičná opatření. Podle typu úniku lze zaměstnance stíhat buď za porušení obchodního tajemství podle obchodního zákoníku, nebo krádež dle trestního zákoníku.

Tento výčet popisuje nejčastější způsoby, jakých podniková špionáž využívá při získávání utajovaných informací. Rozhodně se nejedná o vyčerpávající výčet, neboť s vývojem nových technologií se objevují stále sofistikovanější metody, jak informace získávat bez vědomí jejich majitelů. Proto je třeba věnovat značnou pozornost preventivním opatřením a nepodceňovat okolní rizika. Většinu rizik se dá



předejít, pokud firma bude dodržovat toto desatero týkající se práce s utajovanými materiály.

#### **4.4. Desatero ochrany obchodního tajemství**

**1) Udržení v tajnosti, že vlastníme informace v utajení.**

Pokud se podniku povede uchovat v tajnosti, že má tajné informace, s velkou pravděpodobností se tak vyhne útokům ze strany konkurence.

**2) Separování tajných informací od ostatních.**

Je potřeba tajné informace jednoznačně oddělit od ostatních informací v podniku, aby nedošlo k jejich bezděčnému zveřejnění.

**3) Omezit přístup k tajnými informacím na nezbytné minimum.**

Zde je nejlepší dodržování takzvané zásady „Need to know“ kdy zaměstnanci mají přístup k tajným informacím podniku pouze ve chvíli, pokud to jejich pozice nezbytně vyžaduje a to v nezbytném rozsahu.

**4) Zajištění odpovídající ochrany dat na základě jejich typu.**

Zde je potřeba, aby utajované informace byly dle své důležitosti náležitě chráněny. Samozřejmě každá ochrana komplikuje následnou práci s danými informacemi, proto je nejlepší rozdělit dané informace dle stupně důležitosti a následně dle toho zajistit jejich ochranu.

**5) Znemožnění reprodukce tajných dokumentů.**

**6) Zajistit informace o přesném pohybu tajných dokumentů.**

Je nutné vést evidenci, komu byly tajné dokumenty poskytnuty a kde se právě nachází, abychom měli nad tajnými dokumenty maximální kontrolu.

**7) Vést seznam zaměstnanců, kteří mají přístup k utajovaným informacím.**

Tento seznam nám může značně pomoci při hledání viníka, pokud dojde k narušení bezpečnosti.

**8) Důsledné dodržování práce s tajnými dokumenty.**

Je potřeba všechny tyto kroky bez výjimek dodržovat.

**9) Znemožnit volný pohyb cizím osobám v podniku.**

Jak již bylo výše zmíněno i osoby, které nebudí na první dojem podezření, jako opraváři, nebo uchazeči o zaměstnání, mohou být zrovna tak najati konkurencí, aby zcizili tajné dokumenty či nainstalovali třeba štěnice.

10) **Dostatečně platit zaměstnance**, kteří mají přístup k utajovaným informacím. Jeden z hlavních motivů bývá pro zaměstnance nedostatečné finanční ohodnocení.<sup>17</sup>

Pokud podnik bude dodržovat výše uvedená pravidla, s velkou pravděpodobností se vyhne úniku informací, nebo alespoň minimalizuje všechna rizika.

#### 4.5. Soudní statistika:

Níže jsou v tabulce zpracovány údaje ze soudních statistik z období od roku 2003 až 2009, týkající se porušení hospodářské soutěže a obchodního tajemství. Bohužel ve statistice za rok 2007 byl uveden pouze celkový počet za celou Českou republiku.<sup>18</sup>

Přehled o pravomocných rozhodnutích soudu ve sporech ohledně ohrožení/porušení hospodářské soutěže a obchodního tajemství									
Rok/Kraj	Praha	Středočeský	Jihočeský	Západočeský	Severočeský	Východočeský	Jihomoravský	Severomoravský	ČR
2009	158	3	2	8	9	5	38	17	240
2008	88	5	6	5	4	5	26	11	150
2007	x	x	x	x	x	x	x	x	147
2006	42	8	14	15	4	8	24	21	136
2005	83	10	14	10	8	12	24	35	196
2004	77	4	4	8	4	16	32	18	163
2003	55	2	10	6	1	18	14	11	117

Tab. 1 Přehled pravomocných rozhodnutí soudu ve sporech ohledně ohrožení/porušení hospodářské soutěže a obchodního tajemství

V roce 2009 bylo v České republice registrováno 2 570 611 ekonomických subjektů. Soudních případů týkajících se porušení hospodářské soutěže a obchodního tajemství bylo ovšem pouze 240. Toto číslo zahrnuje pouze přečiny, které je možné

<sup>17</sup> Srov. F. BARTES, *Konkurenční strategie firmy*, s. 42

<sup>18</sup> Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2003*, s. 22

Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2004*, s. 44

Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2005*, s. 44

Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2006*, s. 48

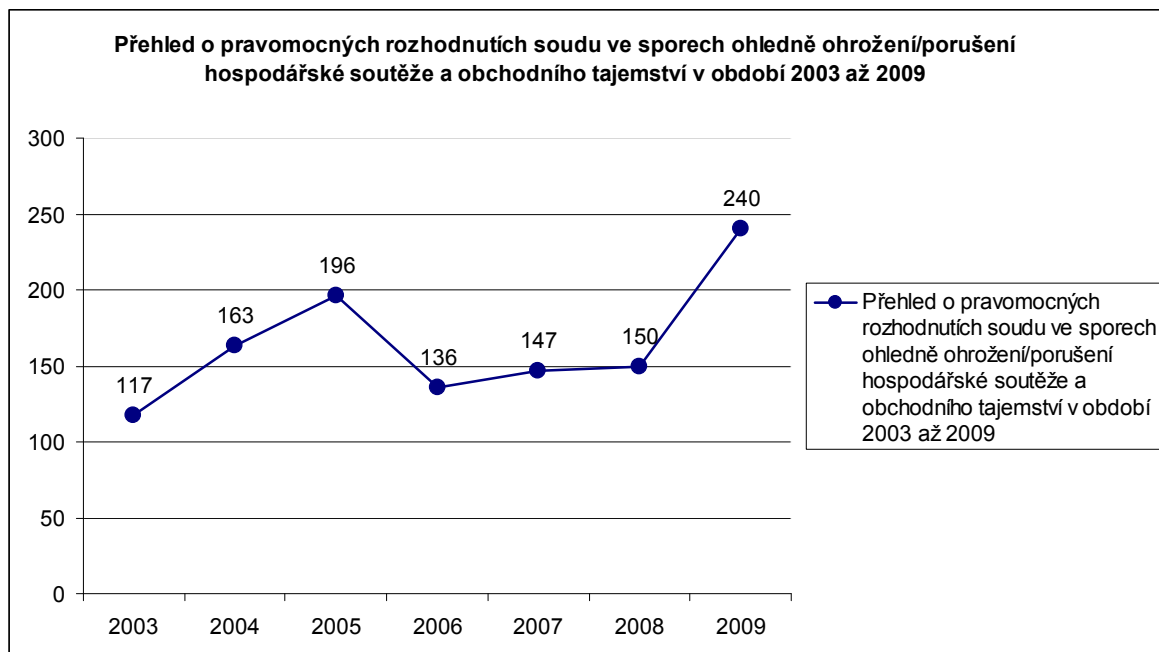
Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2007*, s. 55

Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2008*, s. 53

Srov. MINISTERSTVO SPRÁVEDLNOSTI, *Statistická ročenka soudní agenda II – 2009*, s. 8, dostupné na:

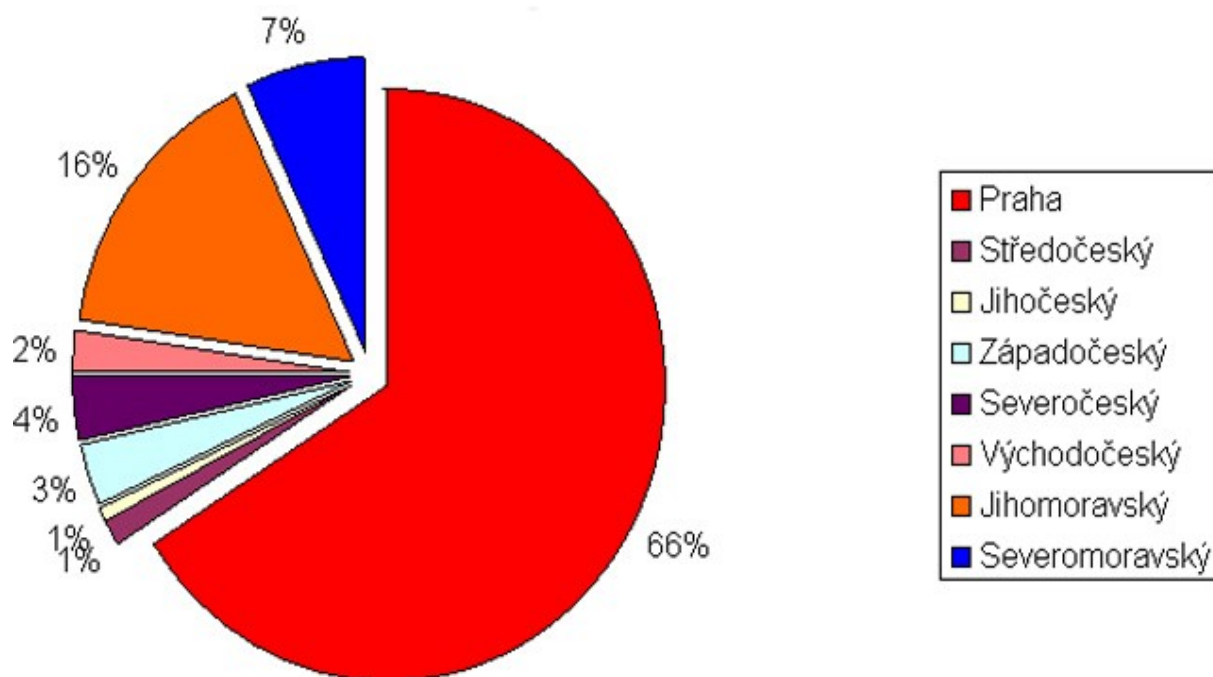
< [http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>

potrestat podle obchodního zákoníku. Nejsou zde tedy zahrnuty další „špionážní aktivity“, které například spadají do trestního práva nebo jiného práva.



Obr. 7 Vývoj počtu pravomocných rozhodnutí soudu ve sporech ohledně ohrožení/porušení hospodářské soutěže a obchodního tajemství v období 2003 až 2009

Jak je vidět z výše uvedeného grafu, je zde růstová tendence v počtu ohrožení hospodářské soutěže a obchodního tajemství, když není příliš vysoká.



Obr. 8 Podíl jednotlivých krajů v % za r. 2009 na pravomocných rozhodnutích v oblasti porušení hospodářské soutěže a obchodního tajemství.

Z výše uvedeného schématu jednoznačně vyplývá, že nejvíce se s porušováním hospodářské soutěže a obchodního tajemství potýká hlavní město Praha. Je to víceméně logické, protože je zde registrováno celých 19% ekonomických subjektů z celé České republiky.<sup>19</sup>

<sup>19</sup> ČESKÝ STATISTICKÝ ÚŘAD, *Počty jednotek v registru ekonomických subjektů podle územního členění a vybraných právních forem*, dostupné na: [http://www.czso.cz/csu/2009edicniplan.nsf/t/AC0046D0AD/\\$File/borgs2\\_1209.pdf](http://www.czso.cz/csu/2009edicniplan.nsf/t/AC0046D0AD/$File/borgs2_1209.pdf)

## 5. PODNIKOVÁ ŠPIONÁŽ Z ÚHLU ETICKÉHO

Etiku můžeme definovat jako systém mravních norem a společenských obyčejů. Zabývá se podstatou morálního vědomí a jednání. Etika se snaží vytvořit žádoucí stav. Určuje tedy normy správného a dobrého chování, které se ovšem v čase vyvíjejí.<sup>20</sup>

V této části se budu zabývat etickými faktory při získávání informací. Nejprve se podíváme na vnímání špionáže z etického úhlu a to na úrovni státu a podniku. Následně zde nastíním význam etického kodexu pro podnik.

### 5.1 Válka vs. konkurenční boj

Již od nepaměti se setkáváme s tím, že ekonomická sféra přebírá metody užívané při vojenských operacích a to včetně terminologie. Podniky vedou konkurenční boje, cenové války, sestavují strategické plány atd. Analogie mezi válkami států a jednotlivých firem je naprosto zřejmá. V obou případech se jak státy, tak firmy snaží získat výhodu nad svým nepřítelem za pomoci špionáže. Přesto se nazírání na užití špionáže v podnikové sféře značně liší oproti užití stejných prostředků ve válce. V roce 1874 na bruselské konferenci států byla špionáž schválena jako povolený válečný prostředek,<sup>21</sup> zatímco podniková špionáž je postavena mimo zákon.

I přesto, že postavení státu a podniku je velmi podobné. Státy i podniky musí čelit značným tlakům ze strany konkurence a z toho důvodu se uchylují ke špionáži, aby si zajistily své přežití.

„Každá vláda je povinna chránit svůj národ a svoji zemi. Nejčastěji se toho dosahuje budováním mocných ozbrojených sil a zároveň snahou získat zpravodajské informace o ozbrojených složkách jiných zemí.“<sup>22</sup>

---

<sup>20</sup> Srov. I. ŠRONĚK, *Etiketa a etika v podnikání*, s. 19

<sup>21</sup> Srov. J. PIEKALKIEWICZ, *Historie světové špionáže*, s. 11

<sup>22</sup> C. GIFFORD, *Svět špionáže*, s. 8

Bezpochyby každý bude souhlasit s tím, že vláda má za povinnost udělat maximum pro to, aby zajistila bezpečí a ochranu svých obyvatel, stejně tak a zajistila celkovou prosperitu státu.

### **Nedělá snad vedení podniku v podstatě to samé na hospodářské úrovni?**

Vedení podniku má za povinnost vést podnik tak, aby prosperoval a upevňoval svoji pozici na trhu a to nejen z důvodu zisku, ale i s ohledem na své zaměstnance, vlastníky a další subjekty, které jsou na daném podniku ekonomicky závislé. Čím je podnik větší, tím více roste jeho společenská odpovědnost. Zvláště v případě nadnárodních společností, které zaměstnávají desetitisíce zaměstnanců, disponují s majetky v hodně několika set miliard dolarů a závisí na nich stovky někdy i tisíce dodavatelských a odběratelských firem.

Skvělým příkladem je Coca-Cola. Kdyby byl totiž ukraden postup na výrobu tohoto nealkoholického nápoje, pravděpodobně by firma ztratila svoji konkurenční výhodu na trhu, což by mělo vliv na marketing, produkci a v neposlední řadě hlavně tržby. Coca-Cola jistě čelí mnoha pokusům o zcizení jejího výrobního tajemství ze strany své konkurence. Proč by tedy neměla mít například Coca-Cola právo provádět kontrašpionáž, aby své tajemství ochránila?

### **Pokud by byla podniková špionáž legalizována, přispělo by to k rozvoji hospodářské soutěže na trhu.**

Není pochyb o tom, že by tento návrh někteří hráči na trhu jistě nadšeně uvítali. Proč by zde neměla platit stejná pravidla jako ve válce mezi státy. Jde přeci o konkurenční boj a to je tvrdá hra, ve které jde o miliony. Kromě toho je na každém, jak bude svá tajemství dobře chránit. Stát tu není od toho, aby nám dělal „chůvu“.

Informace získané podnikovou špionáží, by mohly firmám poskytnout informace nezbytné k udržení se na trhu a jejich rychlejšímu rozvoji, pomoci jim se připravit se na kroky jejich konkurentů a mnoho dalších výhod.

Přesto se pohled společnosti na tuto problematiku značně liší a ve všech vyspělých státech je způsob získávání informací tímto způsobem postaven striktně mimo zákon.

Důvody pro to jsou jednoznačné. Kdyby byla podniková špionáž legalizována, vedlo by to k celkové nestabilitě v tržním prostředí. Podniky by si navzájem kradly výsledky svých výzkumů, postupy a technické vzory. Tato nestabilita v ekonomice by se následně negativně promítla do celé produktivity státu. Také by se tím značně snížila motivace firem investovat do vědy a výzkumu. Nemluvě o tom, že by mnohonásobně vzrostly náklady na ochranu informací a z firemního prostředí by se naprosto vytratil prvek důvěry, který je pro kvalitní spolupráci mezi podniky nezbytný.

## 5.2 Význam etického kodexu

Etický kodex je dokument, který stanoví a upravuje pravidla u organizací nebo jednotlivců tam, kde zákonná úprava není nezbytná. Přijetí etického kodexu může být dobrovolné nebo povinné. Pokud má mít ovšem nějaký význam, tak jeho dodržování musí být vymahatelné.<sup>23</sup>

Přestože etický kodex je většinou dobrovolný, hraje velmi významnou roli v přístupu zaměstnanců k podniku.

Dan Ariely ve své knize publikuje výsledky svého výzkumu, kdy testoval sklon lidské osobnosti k podvádění, pokud jsou pro něj vytvořeny podmínky.

Vytvořil tři testovací skupiny, jedné nedal žádnou možnost k podvádění. Všechny tři skupiny dělaly jednoduchý test. V druhé skupině dal při plnění úkolu možnost podvádět s tím, že před splněním úkolu měla vypsát 10 světových děl. Třetí skupina měla stejné podmínky jako druhá, jen měla za úkol vypsát 10 božích přikázání. Zatímco skupina číslo dvě měla o jednu třetinu lepší výsledky než kontrolní skupina, tak skupina číslo dvě měla naprosto shodný výsledek jako skupina testovací.<sup>24</sup>

Ariely dále ve své knize píše: „Velký dojem na mě udělala skutečnost, že i studenti, kteří si vzpomněli jen na jedno či dvě přikázání, se jimi nechali ovlivnit zrovna tak jako studenti, kteří jich měli namemorováno všech deset. To dokazuje, že

---

<sup>23</sup> Srov. I. ŠRONĚK, *Etiketa a etika v podnikání*, s. 194

<sup>24</sup> Srov. D. ARIELY, *Jak drahé je zdarma*, s. 167

poctivější chování nevyvolalo samo desatero, ale pouhá vzpomínka na nějaký morální standard.<sup>25</sup>

Z těchto poznatků jasně vyplývá, že etický kodex může mít a měl by mít právě funkci onoho morálního standardu. Etický kodex by měl poskytovat zdravý základ pro podnikovou kulturu, aby se zaměstnanci mohli s podnikem lépe identifikovat. To bude mít za následek nejen větší věrnost zaměstnanců vůči podniku, snížení drobných krádeží v podniku (jako jsou například kancelářské potřeby), ale i snížení rizika poskytnutí tajných firemních informací třetí osobě, přičemž se nemusí jednat jen o obchodní tajemství.

### **5.3 Society of Competitive Intelligence Professional (SCIP)**

O SCIP jsem již psal v kapitole „3.3.2 Sběr a vyhodnocování informací, s.16“. SCIP byla založena v roce 1986. Jedná se o nadnárodní neziskovou organizaci pro všechny, kdo se zabývají konkurenčním zpravodajstvím. Jejich cílem je zvýšit úspěšnost svých členů v této oblasti za pomoci vzdělávání a další podpory.<sup>26</sup> Tato společnost má pro všechny své členy závazný etický kodex.

#### **5.3.1 SCIP Etický kodex pro Profesionály v oblasti CI**

##### **Členové se zavazují:**

Neustále usilovat o zvýšení uznání a respektu v této profesi.

Jednat v souladu se všemi platnými zákony, vnitrostátními i mezinárodními.

Poskytnout všechny relevantní informace včetně vlastní identity a organizace, pro kterou pracují a to před všemi rozhovory, aby se předešlo střetu zájmů.

Poskytnout věrné a realistické závěry při plnění svých povinností.

Dodržovat etický kodex ve své společnosti s obchodními partnery a v rámci celé profese.

Zůstat věrný politice společnosti a jejím cílům a pravidlům.

---

<sup>25</sup> D. ARIELY, *Jak drahé je zdarma*, s. 168

<sup>26</sup> Srov. STRATEGIC AND COMPETITIVE INTELLIGENCE PROFESSIONAL, *SCIP Code of Ethics for CI Professional*, dostupné na <<http://www.scip.org/content.cfm?itemnumber=2214&navItemNumber=492>>



## ZÁVĚR PRÁCE

V úvodu své práce jsem uvedl stručnou historii podnikové špionáže. Následně jsem se zabýval definicí základních pojmů a uvedl jsem důvody pro podnikovou špionáž ze strany podniku. Posléze jsem se zabýval rozdělením podnikové špionáže podle toho, odkud může přijít hrozba a následně i od koho.

Po této úvodní části jsem se zaměřil na ekonomické aspekty podnikové špionáže. Zejména pak na to jaký mají vliv informační zdroje podniku na tržní hodnotu podniku. Rozborem intelektuálního kapitálu jsem stanovil základní oblasti, které mohou být předmětem podnikové špionáže. Následně jsem se zabýval péčí o zaměstnance a jejich hlavními motivy pro páchání špionážní činnosti. Na základě jejich specifikace jsem uvedl i opatření, jak se dané situaci nejlépe vyhnout. V závěru této části jsem se zabýval konkurenčním zpravodajstvím a možnými přístupy k němu, včetně popisu základní činnosti se získáváním informací spjatých.

Hned v úvodu právní části uvádím rozhovor s Mgr. Antonínem Novákem, který odpovídá na právní otázky týkající se podnikové špionáže a témat přidružených, včetně právních následků spojených s jednotlivými přečiny. Dále se zde zabývám konkrétním způsoby narušení bezpečnosti společnosti, popisují jejich řešení, a také navrhuji preventivní opatření, aby k těmto skutečnostem nejlépe vůbec nedocházelo. Uvádím zde i účinné desatero preventivních opatření, které mají za účel zabránit jakékoliv infiltraci do společnosti. Na závěr této části uvádím statický počet případů porušení hospodářské soutěže a narušení obchodního tajemství.

V etické části práce se zabývám postavením podnikové špionáže oproti špionáži na úrovni států a pohledu na celou tuto problematiku. Následně se zabývám významem etického kodexu ve společnosti. Na úplný závěr uvádím etický kodex Society of Competitive Intelligence Professional, která sdružuje společnosti zabývající se konkurenčním zpravodajstvím.

V celé práci jsem se snažil provazovat teorii s praxí a v průběhu jsem navrhl mnoho opatření, rad a návodů jak postupovat, aby společnost uchránila svoje obchodní tajemství a tím i svoje místo na trhu. Takže cíl mé práce byl splněn.

## ANOTACE

<b>Příjemní a jméno autora:</b>	Viktor Myslikovjan
<b>Instituce:</b>	Moravská vysoká škola Olomouc
<b>Název práce v českém jazyce:</b>	Podniková špionáž aneb jak vlastní informace získat a o vlastní nepřijít
<b>Název práce v anglickém jazyce:</b>	Corporate espionage – how strange informations get and don't lost own informations
<b>Vedoucí práce:</b>	RNDr. Ing. Miroslav Rössler, CSc., MBA
<b>Počet stran:</b>	46
<b>Počet příloh:</b>	0
<b>Rok obhajoby:</b>	2011
<b>Klíčová slova v českém jazyce:</b>	špionáž, podniková špionáž, hospodářská špionáž, obchodní tajemství, hospodářská soutěž, informace
<b>Klíčová slova v anglickém jazyce:</b>	espionage, corporate espionage, economic espionage, trade secrets, competition, information

Celá práce se zabývá úvodem do problematiky a definicí základních pojmů, včetně stručného historického přehledu. Následně je práce zaměřena na rozdělení podnikové špionáže, její důvody a kontrašpionáží. Zejména jsou zde zpracovány přístupy týkající se ochrany a získávání informací z hlediska ekonomického, právního a etického, a to z hlediska jak teoretického, tak i praktického.

The work concerns with introduction to problems and definition of basic notions including brief historical overview. I also focus on types of industry espionage, its reasons and counterespionage. The thesis focuses on approaches regarding protection and gathering of information. Both theoretical and practical aspects are considered, as well as economical, legal and ethical issues.

## LITERATURA A PRAMENY:

- ARIELY, Dan. *Jak drahé je zdarma*, 1. vyd. Český Těšín, Práh, 2009. 215 s. ISBN 978-80-7252-239-2
- BARTES, František. *Konkurenční strategie firmy*, 1. vyd. Praha, Management Press, 1997. 124 s. ISBN 80-85943-41-7
- BUREŠ, Vladimír. *Znalostní management a proces jeho zavádění*, 1. vyd. Praha, Grada, 2007. 211 s. ISBN978-80-247-1978-8
- ČESKÝ STATISTICKÝ ÚŘAD, *Počty jednotek v registru ekonomických subjektů podle územního členění a vybraných právních forem*, [online]. [cit. 10. března 2011] Dostupné na WWW  
<[http://www.czso.cz/csu/2009edicniplan.nsf/t/AC0046D0AD/\\$File/borgs2\\_1209.pdf](http://www.czso.cz/csu/2009edicniplan.nsf/t/AC0046D0AD/$File/borgs2_1209.pdf)>
- GOLDSILVER, s.r.o., *Odposlech počítače, SKYPE, ICQ, monitoring provozu PC*, [online]. [cit. 1. března 2011] Dostupné na WWW  
<<http://www.goldsilver.cz/odposlech-pocitace-skype-icq-monitoring-provozu-pc/>>
- GIFFORD, Clive. *Svět Špionáže*. 1. vyd. London: Kingfisher Publications, 2004. 64 s. ISBN 0 7534 0963 1
- KOPČAJ, Andrej. *Řízení proudu změn: Všedním způsobem nevšední rozvoj firmy, zákonitosti a metody řízení proudu změn*, 1.vyd. Ostrava, Kopčaj-Silma, 1999. 300s. ISBN 80-902358-1-6
- MINISTERSTVO SPRAVEDLNOSTI,. *Statistická ročenka soudní agenda II – 2003*, s. 118 [online]. [cit. 15. března 2011] Dostupné na WWW  
<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>
- MINISTERSTVO SPRAVEDLNOSTI,. *Statistická ročenka soudní agenda II – 2004*, s.118 [online]. [cit. 15. března 2011] Dostupné na WWW<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>
- MINISTERSTVO SPRAVEDLNOSTI,. *Statistická ročenka soudní agenda II – 2005*, s.118 [online]. [cit. 15. března 2011] Dostupné na WWW<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>
- MINISTERSTVO SPRAVEDLNOSTI,. *Statistická ročenka soudní agenda II – 2006*, s.118 [online]. [cit. 15. března 2011] Dostupné na WWW<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>
- MINISTERSTVO SPRAVEDLNOSTI,. *Statistická ročenka soudní agenda II – 2007*, s.118

- [online]. [cit. 15. března 2011] Dostupné na WWW<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>  
MINISTERSTVO SPRAVEDLNOSTI, *Statistická ročenka soudní agenda II – 2008*, s.118  
[online]. [cit. 15. března 2011] Dostupné na WWW<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>  
MINISTERSTVO SPRAVEDLNOSTI, *Statistická ročenka soudní agenda II – 2009*, s. 118  
[online]. [cit. 15. března 2011] Dostupné na WWW<[http://cslav.justice.cz/portal/page/portal/cslav\\_public/cslav\\_public\\_rocenky](http://cslav.justice.cz/portal/page/portal/cslav_public/cslav_public_rocenky)>  
Obchodní zákoník č. 513/1991, v platném znění [online]. [cit. 15. března 2011] Dostupné na WWW  
<<http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx>>  
PEČENKA, Marek. a Bašta Jaroslav a spol. *Encyklopedie Špionáže*, 1.vyd. Praha, Libry, 1993. 430 s. ISBN 80-901579-1-2  
PIEKALKIEWICZ, Janusz. *Historie světové špionáže*. 1. vyd. München, Südwest Verlag GmbH & Co.KG, 2004. 565 s. ISBN 80-206-0738-2  
STRATEGIC AND COMPETITIVE INTELLIGENCE PROFESSIONAL, *About SCIP* [online]. [cit. 15. března 2011] Dostupné na WWW  
<<http://www.scip.org/content.cfm?itemnumber=2214&navItemNumber=492>>  
ŠRONEK, Ivan. *Etiketa a etika v podnikání*, 1. vyd. Praha, Managament Press, 1996. 212 s. ISBN 80-85603-94-2  
TANGO, SPOL. S R. O. , *Odposlech mobilního telefonu S-GSM*, [online]. [cit. 10. března 2011] Dostupné na WWW < <http://www.odposlechy.com/odposlech-mobilniho-telefonu/>>  
WALKER, Nick. *Marketing: Know your enemy*, [online]. [cit. 10. března 2011] Dostupné na WWW <<http://www.independent.co.uk/life-style/marketing-know-your-enemy-1526528.html>>

## SEZNAM OBRÁZKŮ

Obr. 1 – Tržní hodnota podniku.....	10
Obr. 2 – Model tržní hodnoty společnosti podle společnosti .....	11
Obr. 3 – Pyramida potřeb, člověka i podniku.....	12
Obr. 4 – Grafické znázornění pravděpodobnosti utajení informace k počtu nosičů .....	14
Obr. 5 – Grafické znázornění pravděpodobnosti utajení informace ke spolehlivosti nosiče informace .....	15
Obr. 6 – Schéma činností při získávání informací .....	17
Obr. 7 – Vývoj počtu pravomocných rozhodnutí soudu ve sporech ohledně ohrožení/porušení hospodářské soutěže a obchodního tajemství v období 2003 až 2009 .....	34
Obr. 8 – Podíl jednotlivých krajů v % za r. 2009 na pravomocných rozhodnutích v oblasti porušení hospodářské soutěže a obchodního tajemství .....	35

## SEZNAM TABULEK

Tab. 1 - Přehled pravomocných rozhodnutí soudu ve sporech ohledně ohrožení/porušení hospodářské soutěže a obchodního tajemství .....	34
--	----