Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví
Studijní obor: informační studia a knihovnictví

Jan Kolátor

Příčiny a důsledky softwarového pirátství

Diplomová práce

Praha 2007

Vedoucí diplomové práce: **Peter Pálka**

Oponent diplomové práce:

Datum obhajoby:

Hodnocení:

[Vzor: Vložený list (dvě strany) „Zadání diplomové práce“]

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze, 10. srpna 2007

……..
podpis diplomanta

Identifikační záznam

KOLÁTOR, Jan. *Příčiny a důsledky softwarového pirátství. [Reasons and Results of Software Piracy].* Praha, 2007. 115 s., 5 s. příl. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2007. Vedoucí diplomové práce Peter Pálka.

Abstrakt

Práce je věnována příčinám a důsledkům softwarového pirátství. Podává přehled definic a typologie softwarového pirátství, přehled historie vývoje sledované problematiky i důvodů a podmínek vzniku softwarového pirátství. Rozebírá vztah softwarového pirátství k informačnímu průmyslu. Prezentuje vybrané mezinárodní a státními organizace, které se touto problematikou zabývají. Analyzuje otázky související s legalitou softwarových prostředků. Popisuje jednotlivé druhy metod a postupů softwarového pirátství. Ve svém závěru hodnotí druhy nákladů na ochranu dat a vliv těchto nákladů na výsledné ceny softwaru.

Klíčová slova

softwarové pirátství, nelegální software, hacking, internetová kriminalita

Obsah

Předmluva

Tématem diplomové práce jsou příčiny a důsledky softwarového pirátství. Cílem práce je analyzování problematiky legality používaných informací a softwarových prostředků, které s informacemi pracují. Východiskem bude přehled definic a typologie softwarového pirátství, stručný nástin historie vývoje problematiky bude zpracován jako úvod k přehledu důvodů a podmínek vzniku sledované problematiky. Dále bude práce seznamovat čtenáře se vztahem softwarového pirátství k informačnímu průmyslu, s vybranými mezinárodními a státními organizací, které se softwarovým pirátstvím zabývají, právní problematikou a jednotlivými druhy metod a postupů softwarového pirátství. Ve svém závěru pak s hodnocením několika druhů nákladů na ochranu dat a vlivem těchto nákladů na výsledné ceny softwaru.
Snaha podat vyčerpávající obraz problematiky nelegálního softwaru a nelegálních postupů při práci s informacemi přesahuje možnosti diplomové práce. Úsilí je vedeno spíše k podání přehledu významných shrnutí a závěrů prací, které již byly na toto téma napsány.

Důvodem pro výběr tohoto tématu bylo dlouhodobé setkávání se s uvedenou problematikou během studia, při práci v knihovně, stejně jako při snaze o získání přesných informací o možnostech sdílení a dostupnosti dat. Hlavním zájmem bylo zmapovat problematiku jak ze strany oficiálních institucí, tak z pohledu uživatelů informačních technologií, kteří se dopouštějí softwarového pirátství.

Ke zpracování tématu byla provedena rešerše z dostupných databází a na internetu s cílem vyhledat relevantní zdroje. Prohledány byly mimo jiné seznamy zdrojů na webovských sídlech mezinárodních organizací a národních orgánů vybraných států, které se zabývají ochranou duševního vlastnictví, dále pak webovské stránky a prezentace významných softwarových firem.

Diplomová práce je rozdělena do sedmi kapitol. Rozsah práce je celkem 115 stran. Text byl doplněn přehledem použitých informačních pramenů, které byly citovány podle norem ISO 690 a ISO 690-2.

Vzhledem k obvyklé praxi institucí, které se zaměřují na na ochranu duševního vlastnictví, nevyjadřovat se mimo oficiální tisková prohlášení, jsem velmi ocenil spolupráci Oddělení pro styk s veřejností české pobočky Business Software Alliance.

Na závěr bych chtěl poděkovat za konzultace, připomínky a cenné rady vedoucímu diplomové práce, Petru Pálkovi a za připomínky k legislativním otázkám JUDr. Pavle Kremerové.

Úvod

Problematika softwarového pirátství se s rozvojem informační společnosti stává stále aktuálnější. S přibývajícím počtem lidí pracujících s digitálními informacemi a programy stoupá důležitost odborně zkoumat danou problematiku a to z ekonomických, ze společenských i z bezpečnostních důvodů. Sledováním konkrétních postupů a metod v softwarovém pirátství se začaly zabývat vývojové a distributorské firmy z oblasti informačních technologií. V zemích nejvíce postihovaných softwarovým pirátstvím vznikaly a stále vznikají instituce zabývající se zkoumáním a vyhodnocováním procesů, postupů a dopadů používání nelegálních prostředků při práci s informacemi.

První pokusy o zmapování problémů spojených s legálním a nelegálním softwarem byly provedeny hromadnými sdělovacími prostředky. Na tyto pokusy navazují první odborné studie z akademické oblasti.

1. Definice pojmu softwarové pirátství

Teoretické vymezení problematiky softwarového pirátství jako jevu vzniklého relativně nedávno není ustáleno a je zásadně ovlivněno názory a konkrétními zájmy osoby či instituce, která se uvedeným tématem zabývá. Velký vliv má také ekonomická, politická a sociální situace, za níž teoretická úvaha vzniká, a právní rámec konkrétního státu.

1.1 Pojem softwarové pirátství

V prostředí, které se zabývá problematikou softwarového pirátství, je významná Business Software Aliance (BSA) sdružující přední světové výrobce softwaru, o níž bude podrobněji pojednáno ve čtvrté kapitole. BSA definuje softwarové pirátství velmi jasně a poměrně rozsáhle, přesto však můžeme konstatovat, že jde o jednostranný pohled, který nepodchycuje zdaleka všechny aspekty tohoto problému: „Softwarové pirátství je neautorizované kopírování nebo distribuce softwaru chráněného copyrightem.[1] To může být uskutečňováno kopírováním, stahováním, sdílením, prodejem nebo instalováním vícenásobných kopií na osobní nebo pracovní počítač. Řada lidí si neuvědomuje, že, pokud si koupí software, kupují si ve skutečnosti licenci na jeho používání, ale nikoliv vlastní software. Tato licence říká, kolikrát můžete software instalovat, proto je důležité si ji přečíst. Pokud uděláte více kopií softwaru, než licence dovoluje, dopouštíte se pirátství“ [Business Software Alliance, 2000].[2]

[1] Autorské právo (anglicky označováno jako copyright) je odvětví práva, které popisuje nároky tvůrců tzv. „autorských děl“, tzn. spisovatele, hudebníky, filmaře, programátory apod. na ochranu před nespravedlivým využíváním jejich tvorby.

[2] „Software piracy is the unauthorized copying or distribution of copyrighted software. This can be done by copying, downloading, sharing, selling, or installing multiple copies onto personal or work computers. What a lot of people don't realize or don't think about is that when you purchase software, you are actually purchasing a license to use it, not the actual software. That license is what tells you how many times you can install the software, so it's important to read it. If you make more copies of the software than the license permits, you are pirating.“

Jednotlivé počítačové firmy často definují softwarové pirátství na svých stránkách v rámci protipirátských iniciativ. Příkladem může být definice firmy Adobe: „Softwarové pirátství je nelegální distribuce, anebo reprodukce softwarových aplikací firmy Adobe pro obchodní, nebo osobní použití. Nezáleží na tom, zda je softwarové“ [*Adobe…*].[3] pirátství úmyslné nebo neúmyslné, vždy se jedná o nelegální čin postihnutelný podle zákona. Definice tohoto typu nejsou formulovány obecně, ale většinou se zaměřením na konkrétní zájmy firem.

Kromě počítačových firem se jako jedny z prvních začaly definováním počítačového a softwarového pirátství zabývat masmédia. Definice softwarového pirátství, kterou uvádí **British Broadcasting Corporation (BBC)** v Glosáři na svých webových stránkách, je velmi stručná a také nepostihuje všechny aspekty tohoto jevu: „Produkce nelegálních kopií softwaru“ [British Broadcasting Corporation, 2001].[4] Podobně krátkou definici nalezneme na výukových stránkách Essential Concepts: Apendix A: „Softwarové pirátství je nelegální kopírování nebo používání programů“ [Essential, 2007].[5]

Další definice sledovaného jevu můžeme nalézt ve slovnících a encyklopediích na internetu. Definice, kterou uvádí heslář z oblasti informačních technologií populárního internetového vyhledávače a katalogu **Yahoo!**: „Software piracy: unauthorised duplication of computer software“, je velice stručná a svým obsahem se od předcházející neliší. [Glossary of IT Terms, 2000]. Také definice specializované encyklopedie z oblasti informačních technologií **What IS.com** zdaleka nepostihuje ani neobjasňuje celou šíři problému: „Softwarové pirátství je nelegální kopírování, distribuce nebo používání softwaru“ [WhatIs.com, c2007].[6]

Anglická verze velmi populárního on-line encyklopedie Wikipedia používá pojem softwarové pirátství pouze jako nedeskriptor termínu „copyright infringement“, který

[3] „Software piracy is the illegal distribution and/or reproduction of Adobe software applications or fonts for business or personal use, whether software piracy is deliberate or not, it is still illegal and punishable by law“.
[4] „The production of illegal copies of software“.
[5] „Software piracy is the illegal copying or use of programs“.
[6] „Software piracy is the illegal copying, distribution, or use of software“.

definuje jako: „Porušení copyrightu softwaru, které je také nazýváno softwarovým pirátstvím, se vztahuje k několika postupům při nichž dochází bez povolení vlastníka copyrightu k vytváření kopií a jejich prodeji. Tato činnost je většinou lidí označována jako softwarové pirátství. Ve většině zemí jde o porušení copyrightu a nevhodné chování, jelikož znehodnocuje jinak komerčně dostupnou práci“ [Copyright, 2007].[7]

Pohled z druhé strany spektra přináší definice publikované na internetových stránkách hackerských skupin a skupin P2P. Zde většinou nenalezneme přímo definici softwarového pirátství jako takového, ale jsou zde často probírány jednotlivé činnosti a postupy těchto pirátů, jako jsou cracking, hacking, sdílení dat, sledování dat a jiné. Pro potřeby této práce byly vybrány definice několika častěji používaných výrazů, aby s nimi bylo možno dále pracovat. Nepůjde o úplný a podrobný výklad všech termínů, jelikož postupů, procesů a zájmů hackerských skupin je velké množství a díky prudkému vývoji v oblasti informačních technologií se stále rozšiřují a vyvíjejí:

- **Hacking** – Hacking je neautorizované použití počítače a počítačové sítě. (Termín „***hacker***“ původně označoval velmi nadaného programátora. Postupně nabývá toto slovo pejorativního významu.)[8]

- **Cracking** – Cracking označuje metodu, při které jsou při nelegálním kopírování překonávány kopírovací ochrany a registrační techniky. Crackeři jsou méně schopnou skupinou hackerů a jsou odpovědní za miliónové ztráty softwarových společností.[9]

[7] „The copyright infringement of software, also called software piracy, refers to several practices when done without the permission of the copyright holder: Creating a copy and selling it. This is the act most people refer to as software piracy. This is copyright infringement in most countries and is unlikely to be fair use or fair dealing if the work remains commercially available“.

[8] Hacking is unauthorized use of computer and network resources. (The term „hacker“ originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications) [www.tecrime.com/0gloss.htm].

[9] To copy commercial software illegally by breaking (cracking) the various copy-protection and registration techniques are being used. Crackers are looked down upon by real hackers and they are the ones seen on the news for causing billions of dollars in damages [www.tecrime.com/0gloss.htm].

- **P2P (Peer to Peer)** – Technologie P2P využívá místo jednoho počítače spojenou sílu počítačové sítě s tisíci zapojenými počítači k jedinému účelu, urychlení zpracovávané procedury. Napster byl první P2P program, který sloužil ke sdílení hudby mezi milióny uživatelů počítačů po celé světě. Program SETI@home využívající technologie P2P k simulaci složitých jevů a za 3 roky práce od roku 1999 do roku 2002 čtyři milióny počítačů dosáhly pokroku, jakého by dosáhl jeden počítač po 1,248 letech práce.[10]

- **Seed/Peer** – P2P technologie umožňuje sdílení souborů a jejich stahování po částech. Linky k těmto souborům se nazývají „***torrenty*“**, stažením tohoto torrentu získá uživatel lokaci cílového souboru a seznam ostatních uživatelů (***peerů***) participující na sdílení cílového souboru. Peerové, kteří již vystavují soubor jako celek, se nazývají „***seedeři*“**. Ten kdo soubor vystavil jako první se nazývá původní seeder.[11]

- **Warez -** Je termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem. Slovo bylo vytvořeno z anglického slova ***wares*** (zboží, zřejmě v souvislosti se slovem softwares) způsobem tzv. leetspeeku. Podle druhu bývá někdy warez rozdělován na ***gamez*** (počítačové hry), ***appz*** (aplikace), ***crackz*** (cracky)

---

[10] Instead of one single computer, P2P utilizes the computing power of thousands of computers together to do one thing, speeding up the time required to perform the job. Napster was the originator of P2P for sharing music files between millions of computer users worldwide. SETI@home uses P2P with just under 4 million computers and has, since it started in July 1999 (to August 2002) done 1,009,000 hrs of computation time, or the equivalent of 1,248 years work on one computer!... [www.techdirectcomputers.com/Encyclopedia.htm].

[11] The client connects to the tracker(s) specified in the torrent file, from which it receives a list of peers currently transferring pieces of the file(s) specified in the torrent. The client connects to those peers to obtain the various pieces. Peers that provide a complete file are called seeders, and the peer providing the initial copy is called the initial seeder [http://en.wikipedia.org/wiki/BitTorrent].

a také ***moviez*** (filmy). Nejčastějším způsobem šíření warezu je dnes hlavně internet [http://cs.wikipedia.org/wiki/Warez].

1.2 Typologie softwarového pirátství

Podobně jako definice pojmu softwarového pirátství je i typologie tohoto jevu nejednotná. Můžeme však říci, že s pokusy vymezit podle společných znaků jednotlivé druhy softwarového pirátství se v poslední době setkáváme častěji. V zahraničních zdrojích je nejčastěji uváděno rozdělení na pět hlavních typů:

1. **Porušování patentových a autorských práv** (Publisher patent and copyright infringement).
2. **Průmyslové pirátství** (Industrial piracy).
3. **Pirátství podniků** (Corporate piracy).
4. **Pirátství prodejců** (Reseller piracy).
5. **Domácí pirátství** (Home piracy).

V prostředí českého internetu je poměrně známá a citovaná typologie Pavly Kramerové [KRAMEROVÁ, 1998], podle niž existují následující typy softwarového pirátství:

1. **Pirátství koncových uživatelů** (End User Piracy) - používání několikanásobné kopie jednoho softwarového balíku na několika počítačích nebo nepovolené rozšiřování kopií licencovaného softwaru dalším osobám.
2. **Domácí pirátství** (Home Piracy) - zahrnuje různé činnosti od soukromého vyměňování disket a CD s přáteli až po provozování nevýdělečného **nástěnkového systému (Bulletin Board System - BBS)**, který bude podrobněji popsán v šesté kapitole, pro nelegální distribuci softwaru.

3. **Pirátství prodejců** (Reseller Piracy) - prodej počítačů s předem nainstalovanými nelegálními kopiemi některých programů, instalace softwaru do počítačů bez toho, aby byly uživatelům poskytnuty originální diskety a manuály, prodej softwaru již staženého

   z distribuce. Pro tento druh pirátství je typické velké množství uživatelů, kteří mají nainstalován program se stejným sériovým číslem, se zcela chybějící či nekompletní dokumentací k programu nebo dokumentací, která neodpovídá nainstalované verzi programu.
4. **Pirátství probíhající na BBS nebo na internetu** (BBS/Internet Piracy) - elektronický přesun legálního programového vybavení, kdy systémový operátor nebo uživatelé nahrávají na BBS či internet nebo z nich stahují legální software a materiály, aby mohli zhotovit a používat kopie bez zaplacení odpovídající licence.
5. **Pirátství podniků** (Corporate Piracy) - k jedné legálně instalované kopii určitého programu na lokální síti (Local Area Network - LAN) firmy nebo podniku má nelicencovaný přístup potenciálně i několik set zaměstnanců.
6. **Poškození nebo narušení obchodního jména nebo obchodní známky** - jednotlivec nebo firma v rozporu se skutečností prohlásí, že provozuje autorizovaný servis nebo poskytuje autorizovanou podporu určitého systému či programu, stejného prohřešku se dopouští i ten prodejce, který neoprávněně používá cizí obchodní značku nebo cizí obchodní jméno.
7. **Porušení patentových a autorských práv** - jeden výrobce okopíruje za účelem dosažení zisku materiál nebo proces od jiného výrobce a v nezměněné podobě ho implementuje

   do vlastního produktu.

8. **Průmyslové pirátství** (Industrial Piracy) - jednotlivec nebo skupina jednotlivců za účelem získání značného majetkového prospěchu ve velkém měřítku kopíruje a distribuuje programové vybavení.

Tomáš Chudíček na svých internetových stránkách rozlišuje následující typy softwarového pirátství [CHUDÍČEK, 2007]:

1. Nelegální zásahy do počítačových programů.
2. Nelegální výroba počítačových programů.
3. Nelegální šíření počítačových programů.
4. Nelegální využívání počítačových programů.

Nyní se na jednotlivé typy podíváme podrobněji:

1. **Nelegální zásahy do počítačových programů.**

   Typické způsoby zásahů jsou:

   • **Plagiátorství** - úprava původního díla bez souhlasu autora a vydávání takto pozměněného díla za vlastní.

   • **Tvorba národních verzí programů** - překlad a šíření původního programového díla bez svolení autora.

2. **Nelegální výroba softwaru**

   Kam je zařazena:

   • **Nelegální průmyslová výroba softwaru** - v podniku, který průmyslově vyrábí CD-ROM, je zadána legální zakázka na základě neplatné/padělané licence pro výrobu standardního softwaru.

   • **Domácí výroba/kopírování softwaru bez odpovídající licence** - soukromá osoba pro vlastní obohacení kopíruje a prodává programy a dokumentace k nim.

3. **Nelegální šíření počítačových programů.**

   Může probíhat jako:

   • **Pašování nelegálního softwaru a jeho prodej na našem trhu** - nelegální dovoz padělaných programů, které byly vyrobeny v zahraničí, jejich distribuci a prodej zajišťuje většinou organizovaná skupina pachatelů.

   • **Prodej softwaru bez svolení autora** - pachatel získává nelegálně kopírovaný software nebo software sám nelegálně kopíruje.

   • **Půjčování/pronájem softwaru bez svolení autora** - půjčování nosičů nebo výpočetní techniky s nainstalovaným softwarem.

4. **Nelegální šíření softwaru na internetu** - vystavování počítačových programů pro potřeby dalších uživatelů na volně dostupných stránkách nebo na stránkách přístupných na základě hesla.

5. **Nelegální užívání počítačových programů**

   Zahrnuje dva typické příklady:

   • **Užívání legálně získaného softwaru v rozporu s licenčními podmínkami** - např. užívání programů na více počítačích, instalace her s licencí pro jeden počítač na server apod.

   • **Užívání nelegálně získaného softwaru** [CRAIG, 2005].

2. Historický vývoj softwarového pirátství

Pokud budeme mapovat historii softwarového pirátství, nutně musíme porovnávat jeho vývoj s vývojem internetu a kriminality na něm. Důvodem je propojenost obou problémů, kdy internet se postupně stal zdrojem či nositelem většinového podílu veškerého nelegálního softwaru. Při sledování historického vývoje můžeme využít dva možné úhly pohledu. Informace o hackerských útocích, nelegálních programech, neautorizovaných informacích a

jiných nelegálních aktivitách můžeme získávat z oficiálních sdělovacích prostředků, publikací, ze stránek organizací zabývajících se mapováním a potíráním těchto aktivit nebo ze zdrojů provozovaných samotnými hackery. Při podrobnějším studiu těchto zdrojů dojdeme k závěru, že oba dva druhy často nejsou objektivní a jejich informace bývají podávány tendenčně

a u oficiálních institucí jsou navíc poskytované informace obvykle cenzurovány. Pokud chceme tedy získat pravdivý obraz problematiky, musíme extrahovat informace z obou zdrojů a jejich porovnáváním se pokusit dojít k nezkresleným závěrům.

2.1 Jednotlivé historické etapy vývoje

2.1.1 Phreackingové období

Za první tzv. „protohackery“ jsou undergroundovou IT komunitou a literaturou např. Brucem Sterlingem v jeho díle *„The Hacker Crackdown“* [STERLING, 1992] považováni bezejmenní pracovníci Bellovy telefonní společnosti (Bell Telephone Company), kteří byli propuštěni v roce 1878. Ale teprve od roku 1960 se ve Spojených státech amerických, kde začaly být telefonní ústředny řízeny počítači, začal rozvíjet tzv. phreacking, tj. překonávání telefonních systémů s cílem získat informace o telefonních společnostech a zajistit si volání zdarma [GREGURAS, 1998], [SHIMEALL, 1999, s. 58], [*History of software piracy*, 2004].

Jeden z prvních pokusů o prehacking provedl v roce 1969 Joe Engressia (který používal přezdívky jako The Whistler, High Rise Joe a nyní je známý jako Joybubbles). Ačkoliv byl slepý, byl studentem Univerzity jižní Floridy (University of South Florida - USF) a v době svého studia zjistil předčíslí a kód, po jehož navolení bylo možné volat z telefonních automatů zdarma do zahraničí. Dva roky poté student jménem John Draper, jenž vystupoval pod přezdívkami Captain Crunch nebo Crunchman, sestrojil zřízení „blue box“, které

emitovalo telefonní servisní tóny a s jehož pomocí se z jakéhokoliv telefonu dalo volat zdarma [SHIMEALL, 1999, s. 58], [*History of software piracy*, 2004].

Teprve v roce 1972 (za přispění telefonních společností) nalezly americké soudy prostředky a zákony, podle nichž mohly preackery obžalovat. První z obžalovaných a odsouzených byl právě John Draper, který byl v Kalifornii podmínečně odsouzen k trestu odnětí svobody na pět let[12] [SHIMEALL, 1999, s. 58], [*History of software piracy, 2004*].

2.1.2 Hackerské období

Hackeři v původním slova smyslu, kteří se považují za svobodomyslné počítačové nadšence nepřekračující zákon, označují za své duchovní předchůdce zpravidla studenty prestižních amerických technických univerzit, především **Massachusettského technologického institutu (Massachusetts Institute of Technology – MIT)** a **Stanfordské univerzity (Stanford University)** ze 60. letech 20. století.

Pokud bychom však hledali mírně zromantizované kořeny moderního hackerského undergroundu, lze je sledovat nejspíše k dnes už dávno zapomenutému anarchistickému proudu hippies, zvanému Yippies. Jeho členové, kteří vytvořili své jméno z názvu „Youth International Party“, uskutečňovali radikální program sabotáží a politických provokací. K jejich metodám patřilo otevřené odmítání vlády a zákonů stejně jako manipulace s médii. Jedním z hlavních představitelů byl radikální aktivista Abbie Hoffman, který se věnoval manipulaci televizních společností a jiných medií pomocí fám, záměn identit a lží. Jeho nejslavnější prací byla kniha
s názvem „Ukradni tuto knihu“, která už svým názvem nabádala k porušování běžné distribuce
a práva.

[12] Nejznámějším se však stal **Kevin Mitnick** díky vydávání popularizačních knih a článků o problematice hackingu [http://en.wikipedia.org/wiki/Kevin_Mitnick].

Mnozí hackeři a lidé sdílející a poskytující jiným nelegální software či data, pokládají za předchůdce současného softwarového pirátství takzvané „**neviditelné univerzity**“ **(invisible college)**. Pokud by tento fenomén vznikl v současné době, s velkou pravděpodobností by se hovořilo o virtuálních univerzitách, stejně jako se dnes v souvislosti s internetovým přístupem
do katalogů knihoven a k plnotextovým knihám i časopisům běžně hovoří o virtuálních knihovnách.

Neviditelnou univerzitu představuje skupina odborníků, vědců nebo jiných duševních pracovníků, jež spojuje společný odborný nebo profesionální zájem. Tato univerzita je „neviditelná” v tom smyslu, že ve skutečnosti není ohraničena žádnou zdí a umožňuje vstup každému, kdo má o spolupráci zájem a to bez ohledu na místo, kde dotyčný žije. Pro některé badatele je důvodem ke vstupu do neviditelné univerzity i možnost vzájemné komunikace a sdílení informací [DIADOTO, 1994]. Stejně tak pro mnohé softwarové piráty je dnes jednou z hlavních motivací touha po příslušnosti ke konkrétní pirátské skupině, účast na její komunikaci, možnost sdílet a vyměňovat si poznatky týkající se konkrétního softwaru anebo programování.

Neviditelné univerzity měly a mají jednoznačně pozitivní vliv na zvýšení **informační gramotnosti**[13] celé společnosti. Pomáhají vytvářet tvůrčí prostředí, formulovat problémy a nacházet na ně řešení. Dalším společným znakem je neformální komunikace mezi členy neviditelných univerzit. Současní softwaroví piráti poukazují na podobnost s komunikací v pirátských skupinách. “Neviditelnost” této komunikace, může být sledována a popsána pracovníky z oblasti **bibliometrie**[14] (dnes i **kybermetrie**), odborné komunikace a

[13] Informační gramotnost je schopnost jednotlivce prostřednictvím dostupných informačních metod a technologií vyhledávat, zpracovávat, vyhodnocovat a využívat informace [TDKIV, *Informační gramotnost*].
[14] Vědní obor zabývající se kvantitativní analýzou dokumentů vznikajících v rámci vědecké komunikace, který vychází z předpokladu, že zkoumané dokumenty jsou odrazem stavu vědeckého poznání. Bibliometrické výzkumy směřují k formulaci kvantitativních zákonitostí souvisejících s formální a sémantickou strukturou dokumentů (např. Bradfordův zákon, Lotkův zákon, Zipfův zákon atd.). Bibliometrie se chápe jako součást

scientometrie[15]. Tuto neformální komunikaci představují např. citace, elektronická pošta, telefonní rozhovory, stejně jako i přednášky nebo diskuse na různých setkáních, které nebyly publikovány. Komunikace probíhá neformálními kanály. Jejím charakteristickým rysem je, že je mnohem více interaktivní než jakákoliv komunikace formální a bývá obvykle orálního či krátkodobě uchovávaného verbálního charakteru [LANCASTER, 1978]. Znázornění komunikace je možné pomocí sociogramů, tedy diagramů znázorňujících, kdo s kým komunikuje. Někdy tyto diagramy mohou zachycovat i častost komunikace.

Již v roce 1965 spoluzakladatel společnosti Intel Gordon Moore předpověděl, že každé dva roky dojde ke zdvojnásobení počtu tranzistorů, jež lze integrovat na mikročip. Úvaha, která je známá jako **Mooreův zákon**, platila a ovlivňovala informační průmysl více než třicet let. Gordon Moore ve svých článcích často polemizoval s informační politikou USA a nadnárodních telefonních společností a podporoval hackerská undergroundová hnutí [SHIMEALL, 1999, s. 58], [*History of software piracy*, 2004].

Slovo **hacker** jako označení typu lidí zabývajících se určitou nelegální činností vzniklo již v roce 1969. Jeho původ můžeme hledat v amerických skupinách modelářů, kteří předělávali vláčky k vyššímu výkonu. Po nástupu prvních sálových počítačů se někteří z těchto hackerů začali učit jejich ovládání a programování. Stali se zaměstnanci firem pracujících se sálovými počítači, studovali na vysokých školách technického směru a nebo se dopouštěli prvních trestných činů, kradli tzv. „strojový čas“[16] počítačů a ověřovali na nich své dovednosti [SHIMEALL, 1999, s. 58], [*History of software piracy*, 2004].

Důležitou vlastností hackerů je, jak již bylo uvedeno, jejich sdružování do skupin. Jednou z prvních významných skupin byla v roce 1969 skupina MIT, další pak v roce 1980

---

informetrie anebo scientometrie, prakticky se však s těmito disciplínami výrazně překrývá [TDKIV, *Bibliometrie*].

[15] Metody matematické a statistické analýzy vědeckého výzkumu, především v přírodních vědách [TDKIV, *Scientometrie*].

[16] Jde o čas rezervovaný na práci se sálovými počítači, využívaný k výpočtům předem připravených algoritmů.

Legie Prokletých (Legion of the Doom), která se věnovala nabourávání do sítí, preakingu, kopírování interních informací firem a jejich zveřejňování na internetu [SHIMEALL, 1999, s. 58], [*History of software piracy*, 2004].

V roce 1986 německá hackerská skupina **Chaos Computer Club** získala z vládní sítě informace o německém atomovém programu a v době černobylské havárie je zveřejnila [CASIRAYA, 2002, s. 1], [*History of software piracy*, 2004].

V roce 1989 se šestnáctiletý chlapec z Eimwoodu v New Orleans naboural do hlavního počítače firmy McDonald‘s a podařilo se mu přepojit linky tak, aby všechny hovory byly volány přes New York. Eimwoodské pobočce firmy McDonald‘s tak vzrostly roční náklady na telefon
o 17 000 dolarů. Za necelý rok byl zatčen a odsouzen na 400 hodin veřejně prospěšných prací a na 44 podmínek [*History of software piracy*, 2004].

V roce 1990 zorganizovala Americká tajná služba (**United States Secret Service - USSS**) a Arizonská policejní pobočka (**Arizona Policy Department - APD**) pro organizovaný zločin rozsáhlou mezinárodní akci proti hackerům. Cílem akce bylo zamezení nelegálnímu kopírování softwaru na území Arizony a okolních států a jako pronikání do soukromých bází dat a zveřejňování interních informací [CASIRAYA, 2002, s. 1], [*History of software piracy*, 2004].

Hackerům z Nizozemí se podařilo během dvou měsíců proniknout do 34 stránek Ministerstva obrany USA (**US Department of Defense - DoD**) a získat odtud informace vojenského, logistického i osobního charakteru. Tyto informace sice nebyly označeny jako tajné, ale jejich zveřejnění značně poškodilo prestiž Department of Defense. Ve zprávě vydané Tiskovou kanceláří vlády Spojených států (**Office of Press Relations - U.S. Department of State**) se uvádí, že z mnoha pokusů o průnik do bází dat Department of Defense jich bylo 65% úspěšných [*History of software piracy, 2004*].

V roce 1995 byla vydána příručka pro správce sítí pod názvem Bezpečnostní nástroj administrátora pro analyzování sítě (*Security Administrator Tool for Analyzing Network - SATAN*) o správě sítí a zabezpečení informací na nich. Příručka se stala velmi čtenou a využívanou mezi hackerskou veřejností [*Software piracy and the Law,* 2002].

V roce 1998 byla v Alabamě poprvé použita takzvaná e-mailová bomba. Hackeři rozeslali soubor 14 000 mailů na náhodně vybrané komerční adresy. Ve stejném roce byl vytvořen virus jménem Melissa. Tento virus napadl 100 000 uživatelů e-mailu a za jeden rok způsobil škody v hodnotě 80 milionů dolarů [*History of software piracy,* 2004].

Potřeba řešit problematiku nelegálního softwaru vedla v roce 1998 k založení organizace BSA, která se stala mluvčím předních světových výrobců softwaru. Od tohoto roku organizuje akce a vzdělávací programy zaměřené na autorskoprávní problematiku. Hlavním cílem BSA je ochrana autorských práv členů aliance, ať už prostřednictvím trestních řízení či prevencí formou osvěty. Činnost této organizace je podrobně popsána ve čtvrté kapitole.

V roce 2000 devatenáctiletá Raphella Gray ukradla přes 23 000 čísel kreditních karet z osmi společností s využitím děr v zabezpečení ochrany internetu. Poslala pak Billu Gatesovi dárek objednaný a zaplacený jeho vlastní kreditní kartou [CASIRAYA, 2002, s. 1].

2.1.3 Stav nelegálního softwaru po roce 2000

Charakteristickým rysem začátku tohoto období byl přechod od akcí individuálních hackerů, nebo hackerských skupin ke korporativnímu a všeobecnému softwarovému pirátství. Je třeba zdůraznit, že softwarovým pirátem se dnes stává (ať již vědomě, či nevědomě) v podstatě téměř každý uživatel počítače.

Toto období přineslo také výrazný kvantitativní posun v počtu nových hrozeb a incidentů.

Z analýzy Computer Industry Almanac vyplývá, že ač počet uživatelů internetu roste zhruba

lineárně,[17] počet incidentů se v roce 2001 oproti roku 2000 více než zdvojnásobil, viz následující tabulka.

Rok	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**
Počet incidentů	cca 2 000	cca 2 500	cca 4 500	cca 10 000	cca 21 000	cca 43 000

Tabulka č. 1 – Počet incidentů sledovaný v analýze Computer Industry Almanac. Zdroj: [http://www.cert.org].

Příčin tohoto prudkého nárůstu je několik, mezi hlavní patří stále razantnější pronikání počítačových technologií do všech oblastí lidské činnosti, nedostatečné všeobecné povědomí o počítačové bezpečnosti a také principální neschopnost právního řádu pružně reagovat na nové výzvy. Zde nemluvíme pouze o nedostatcích v zákonech, ale také o neschopnosti represivních složek využívat možnosti, které stávající právní úpravy nabízejí [*Sedmá výroční zpráva BSA*

o softwarovém pirátství ve světě, 2003], [HUNDLEY, 2002].

V letech 2002 až 2005 bylo ročně nahlášeno cca 150 000 incidentů [HUNT, 2004, s.1-3], [*Sedmá výroční zpráva BSA o softwarovém pirátství ve světě,* 2003], [HUNDLEY, 2002]. To naznačuje stabilizaci předchozího překotného vývoje.

Povaha internetu jako hlavního prostředí působení nelegálního softwaru stále značně snižuje šance na vystopování a dopadení pachatele. Nových systémů, aplikací a jejich nových verzí každý rok přibývá a s nimi roste i počet bezpečnostních chyb. Zprávy o nových chybách v systémech už dávno nepůsobí senzačně, proto je sleduje pouze úzce specializovaná skupina odborníků. V tom je právě ten problém - přes 95 % všech úspěšných útoků využívá známou

[17] Pro srovnání počet připojených uživatelů v roce 1996 činil cca 50 milionů a v roce 2002 cca 600 milionů. Zdroj: http://www.cert.org/

bezpečnostní slabinu, která byla detailně popsána, a na kterou existuje oprava [*Sedmá výroční zpráva BSA o softwarovém pirátství ve světě,* 2003], [HUNDLEY, 2002].

V lednu 2002 vydal časopis *Computer Economics* studii s analýzou finančních dopadů bezpečnostních incidentů. Jejich celosvětové finanční dopady byly odhadnuty v roce 2001 na téměř 25 miliard dolarů. V České republice se tato částka pohybovala kolem 18 milionů eur [HUNT, 2004, s. 1-3], [*Sedmá výroční zpráva BSA o softwarovém pirátství ve světě, 2003*]. Tradičně největší ztráty mají na svědomí autoři počítačových virů. Již ve svém původním pojetí byl každý virus prostředkem porušujícím práva napadeného.

Podle týdeníku pro informační profesionály *Computer World* se léto 2002 stalo zlatou sezonou hackerů. Stále blíže realitě je od té doby i vazba kybernetických útočníků na jednotlivá politická seskupení. Tedy to, o čem se zatím psalo pouze ve sci-fi literatuře. K hlavním skulinám, kterými se hackeři dostávali během léta roku 2002 do systémů, patřily bezpečností díry

v OpenSSH, webovém serveru Apache a klientských programech společnosti Microsoft, především v programech Microsoft Internet Explorer a Microsoft Outlook. Softwarové firmy reagovaly na novou situaci zvýšenou mírou investic do zabezpečení a ochrany, a to nejenom samotných programů a dat, ale také systémů a médií jako jsou např. CD-ROM a formát DVD.

Prognózy z uvedeného roku poukazovaly na nový typ útoků a postupů, který měl výrazně destabilizovat informační toky a poškodit celý internet. K tomu měl přispět nový typ nebezpečných počítačových červů, schopných infikovat webové servery, prohlížeče a další prvky na internetu tak rychle, že zamoření celého internetu by bylo záležitostí několika minut. Autoři výzkumného dokumentu s názvem *„How to 0wn the Internet in Your Spare Time“* [STANIFORD, 2002] publikovaného v roce 2002 předpokládají budoucnost, v niž viry používají „**hit list“** k lokalizaci napadnutelných systémů místo toho, aby bez cíle skenovaly

okolí, jak to již předvedly Nimda nebo Code Red[18]. Prognózovaná generace červů měla také obsahovat kód umožňující automatizovaný útok a destrukci souborů či ovládnutí systému prostřednictvím vzdálené kontroly Denial of Service (DoS). Z takto ovládnutého systému může útočník získávat jakákoliv data, a to i taková, na která by se jinak vztahovaly zpřísněné režimy práce s informacemi.

Výrazný zlom v boji proti softwarovému pirátství představoval rok 2004, kdy organizace Americká asociace nahrávacího průmyslu **(Recording Industry Association of America - RIAA)** v rámci snahy o ochranu autorských práv přichystala druhou vlnu žalob na uživatele sítě P2P, zaměřenou na ty, kteří nabízeli ke stažení velké objemy hudebních nahrávek chráněných autorskými právy[19]. Tato vlna žalob byla lépe připravena než předchozí. RIAA zvolila jiný postup. Dopředu totiž obeslala více než 204 uživatelů, kteří měli údajně porušovat autorská práva hudebních umělců a nahrávacích společností. Ti byli seznámeni s žalobou a měli možnost celou situaci vyřešit mimosoudně. Část z nich této možnosti využila a zbytek čekal soudní spory. Sto dvacet čtyři oslovených uživatelů sítě Kazaa se s RIAA dohodlo na mimosoudním vyrovnání, zbylých osmdesát zvolilo soudní spory. Tímto útokem se RIAA také na určitou dobu podařilo snížit počet aktivních uživatelů P2P sítí v USA [*RIAA opět...*].

2.2 Důvody a podmínky vzniku a vzestupu softwarového pirátství

V celé řadě případů nelze motivy pirátů zcela jednoznačně identifikovat. Pro jejich činy je často možné kombinovat několik motivací. Příkladem může být útok hackera, který používá přezdívku Gabriel, na síť vydavatelství Bloomsbury Publishing Plc. se sídlem

[18] Oba tyto červy se projevují stejnou funkcionalitou. Po spuštění se červ automaticky kopíruje po lokální síti a snaží se napadat nezabezpečené webové servery. Právě automatické kopírování červa působí, že je méně ničivý ,ale obtížně se odstraňuje. Po té, co z vlastního počítače odstraníte spoustu červem vytvořených souborů, přikopíruje se tam z jiného počítače.

[19] První vlna žalob z předchozího roku skončila neúspěchem, všichni obvinění museli být propuštěni a RIAA své činy musela vysvětlovat i senátorovi, který si představitele této společnosti předvolal.

v Londýně. Jediným účelem získání rukopisů knihy *Harry Potter a smrtelní svatí* (Harry Potter and the Deathly Hallows) od J. K. Rowlingové dříve, než bude uvedena do celosvětové produkce.

O tomto činu informoval 25. 6. 2007 sám Gabriel na uznávaných internetových stránkách InSecure.org [FYODOR. 2007], které se zabývají bezpečnostní problematikou. Informaci přejaly okamžitě světová média, např. Reuters. [REUTERS, 2007], a to bez ohledu na to, že autority, jako třeba David Perry, který je mluvčím softwarové bezpečnostní agentury, okamžitě označily zprávu za hoax [Hoax, 2007].

Motivem hackera zde zcela jistě nebyla snaha o osobní finanční obohacení, jelikož „rukopis“ umístil na internet, spíše zde může jít o snahu o zvýšení osobní prestiže v konkrétní sociální skupině a o touhu po znalosti informací, které jsou široké veřejnosti nepřístupné. Obdobně jako u předchozího dílu této série, který byl ukraden v průběhu přípravy do tisku [*JK Thieef..., 2007*], je i v tomto případě velmi důležitým faktorem celosvětová poptávka po daném díle. Poptávka je tak silná, že ani médii proklamovaných 15 miliónů dolarů na ochranu není dostačujících. Lze předpokládat, že v budoucnu bude tlak na získání originálů dále stoupat. Síla celosvětové poptávky na jedné straně a uměle vytvořeného nedostatku, ať již zapříčiněného tempem uvedení produktu do prodeje, umělým vytvářením bariér volného šíření díla či dalšími faktory, na straně druhé, motivuje ke snaze získat tyto informace jakýmikoliv prostředky. Stejný princip lze vysledovat také u nově vydávaného softwaru. Pokud je očekávání produktu velké, dochází často k pirátským útokům na samotného producenta softwaru se snahou produkt odcizit, ať již jde o ještě nepublikované verze nebo jen části zdrojového kódu, které jsou následně publikovány na diskusních serverech, jako je kupříkladu slovenský http://blackhole.sk/, kde se scházejí hackeři a softwaroví piráti. Úspěšně publikované „úlovky“ slouží, jak již bylo řečeno, nejen k získání informací či dat samotných, ale také ke zvýšení osobní prestiže jedince.

Softwarové pirátství je celosvětový fenomén. V roce 2001 Business Software Alliance konstatovala, že není žádný národ s nižší než 20 % mírou pirátství a že ze sledovaných národů jsou dva, které přesahují 90% [*Třetí výroční zpráva BSA a IDC,* 2006]. Míru softwarového pirátství v letech 1999 až 2003 dokládají údaje v tabulce č. 2.

Země / Rok	1999	2000	2001	2002	2003	Průměr
Vietnam	98%	97%	94%	95%	92%	95,2%
Čína	91%	94%	92%	92%	92%	92,2%
Ukrajina	90%	89%	87%	89%	91%	89,2%
Rusko	89%	88%	87%	89%	87%	88,0%
Indonésie	85%	89%	88%	89%	88%	87,8%
Pákistán	83%	83%	83%	80%	83%	82,4%
Libanon	88%	83%	79%	74%	74%	79,2%
Bolívie	85%	81%	77%	74%	78%	79,0%
Nigérie	68%	67%	79%	69%	84%	73,4%
Zimbabwe	63%	59%	68%	70%	87%	69,4%

Tabulka č. 2 - Míra softwarového pirátství ve vybraných zemích v letech 1999 – 2003. Zdroj : [*Sedmá výroční zpráva BSA o softwarovém pirátství ve světě, 2004*].

Odhaduje se, že v roce 2001 výrobci softwaru ztratili asi 10,97 miliónů dolarů jako důsledek působení softwarových pirátů [*Třetí výroční zpráva BSA a IDC,* 2006]. Navíc, ve většině regionů ve světě se zvýšil podíl o 37 % v roce 2000, a o 40 % v roce 2001. Tento trend se nezměnil a přes mediální tlak a snahy soukromého i státního sektoru se zdá, že softwarové pirátství je od svého vzniku až do současnosti stále na vzestupu.

Odborná literatura nabízí některá vysvětlení pro vzestup softwarového pirátství a jeho stoupající hrozbu celosvětovému informačnímu průmyslu. Zatímco aktualizované studie

Software Publisher´s Association (SPA) [*Třetí výroční zpráva BSA a IDC*, 2006] stále tvrdí, že příjem na osobu není spojen s podmínkami existence a vzestupem softwarového pirátství, Shin

a kol. [SHIN, 2004] dokazují zjevnost faktu, že vysoká cena softwaru je tažnou silou softwarového pirátství ve státech s nízkou mírou hrubého domácího produktu (HDP).[20] Dále tvrdí, že zvýšení HDP na osobu je zjevně spojeno se snížením úrovně pirátství v daném státě. Zmiňovány jsou i další faktory, zejména dostupnost pirátského softwaru, méně tvrdé zavádění a prosazování autorského práva [MORES, 2000], morální problémy s prosazováním autorského práva, s úrovní infrastruktury informačních technologií a s úrovní přístupnosti internetu [*Forum section...*, 2000]. Jsou zde i další faktory (jenž budou popsány dále), které mohou vysvětlit vzestup softwarového pirátství v posledních letech.

Pokud si položíme základní otázku, proč se vlastně liší úroveň softwarového pirátství v jednotlivých regionech či dokonce státech, můžeme běžně předkládané důvody rozdělit do čtyř kategorií:

1. **Ekonomické faktory -** mnozí výzkumní a odborní pracovníci publikující na toto téma, již dlouho poukazují na to, jak je důležitá cena softwaru s ohledem na úroveň pirátství. Shin

   a kol. [SHIN, 2004] naznačují, že HDP na obyvatele je nepřímo úměrný základní úrovni softwarového pirátství (zámožnější národy mají nižší potřebu nelegálního softwaru). Avšak může být pravdou, že současný pokles ceny softwaru vede k nižší závislosti úrovně softwarového pirátství na HDP, než tomu bylo v minulých letech.

   V současné době je uváděno, že samotné ekonomické faktory mohou vysvětlit pouze asi 62 %-63 % softwarového pirátství, a jak již bylo řečeno, při klesajících cenách softwaru

[20] Kde si obyvatelé vysoké ceny softwaru nemohou dovolit.

a nárůstu alternativních řešení v podobě freewaru[21] bude mít tento vliv stále klesající tendenci.

2. **Technické faktory** - z průzkumů a statistik, které předkládá v každé výroční zprávě BSA vyplývá fakt, že softwarové pirátství je běžnější ve státech s nižší infrastrukturou informačních technologií, kde kvalita (starší verze, nižší množství vylepšení) dostupného
a používaného softwaru je nižší. Proto lidé často kopírují pirátský software a pracují s ním.

   Potřeba uživatelů pracovat s nejnovějšími verzemi a využívat poslední novinky je důležitá pouze v okamžiku, kdy jsou tyto verze dostupné [MORES, 2000]. Někteří odborníci se také domnívají, že softwarové pirátství rozkvetlo se vzestupem internetu, kde mnohé webové stránky poskytují software zdarma či za nižší ceny, než jsou ceny poskytované výrobcem a dodavatelem [SHIN, 2004]. Dle jiných, ke kterým se přiklání i autor této práce, je distribuce za pomoci internetu pouze novou distribuční cestou ať již dodavatelského/komerčního či volně šiřitelného softwaru (zejména freewaru a sharewaru).

   Od roku 2004, kdy byla studie [SHIN, 2004] uveřejněna, se vývoj v oblasti distribuce softwaru, informací a dalších komodit informačního průmyslu přesouvá jednoznačně k internetové distribuci, tudíž rozvoj internetu v dané zemi napomáhá snížení míry potřeby softwarového pirátství.

3. **Regulační faktory** - nastavením vyšší daně a poplatků obecně vybíraných pro vládu z prodeje softwaru zapříčiňuje vláda vzestup cen softwaru a tím může neúmyslně přispívat k povzbuzení činnosti pirátů. Rozvojové státy velmi často uvalují vysoká cla na počítačové produkty a také úroveň softwarového pirátství je v těchto státech vysoká.

[21] Bude blíže vysvětleno v páté kapitole.

Obecně se předpokládá, že nízká cenzura zabraňující nákupu a vysoká dostupnost tohoto nelegálního softwaru jsou také důvody k vzrůstu úrovně softwarového pirátství v těchto zemích [MORES, 2000]. Pravidla copyrightu jsou často považována za převzatá ze zahraničí a neodpovídající místní tradici, jsou také složitá na pochopení a ještě složitější na vymáhání výkonnou mocí. Meso a spol. [MESO, 2005] identifikují vymahatelnost copyrightu jako význačný bod v budování národní informační politiky. Pokud vláda neimplementuje konzistentně tato pravidla, částečně kvůli laxnosti přístupu výkonné státní moci a kvůli jejich tíhnutí k ignorování korupce a částečně kvůli složitosti a celistvosti těchto pravidel dochází ke skulinám a vytváření prostoru, který mohou využívat softwaroví piráti. Takže, i když vymáhání intelektuálního vlastnictví a správná osvěta a vzdělávání zmenšuje tento problém, ve skutečnosti je jen velmi málo jedinců porušujících copyright přistiženo a potrestáno.

Občasné útoky výkonné moci a společností zaměřujících se na vymáhání dodržování copyrightu jsou spíše symbolického charakteru a jen zřídka naruší volné šíření nelegálního softwaru. Státy, které povolují prodej nelegálního softwaru za nižší ceny, než jsou ceny, poskytované dodavatelem, napomáhají rozkvětu černého trhu. Jedinci a společnosti v těchto státech si nemusejí být ani vědomi toho, že kupují pirátský software, který má auru legitimity. Celkově má nízká úroveň povědomí o legálnosti softwaru a lehká dostupnost tohoto softwaru přímou úměru s indikátorem korupce v dané zemi.

Korupce může být definována jako: *„cena, již je potřeba vynaložit na získání takových privilegií, kterými normálně disponuje pouze stát, jako je možnost vybírání státních daní, poplatků, tarifů, obhospodařování státních zakázek a profitování z nich, získání nezasloužených výjimek oproti jiným a další…“* [HERITAGE, 2006].

4. **Sociální a kulturní faktory:** Tyto faktory vyjadřují převažující názory sociální struktury země a postoje, které sdílejí členové této společnosti. Jedním z měřítek sociální struktury je sociální vzdálenost mezi jedinci. Existují společnosti se slabšími sociálními vazbami, v nichž je kladen velký důraz na individualitu jedince a lidé se starají spíše o sebe, a pak kolektivní společnosti se silnými sociálními vazby mezi jedinci a velmi silným skupinovým cítěním.

Softwarové pirátství je populární ve státech s kolektivní společností, kde lidé tíhnou k vytváření pevných společenských vazeb, v nichž se vytváří jasné rozlišení toho, kdo je členem společnosti (in-group) a kdo jím není (out-group). Tyto rozdíly jsou velmi zřetelné. Loajalita a závazky členů k ostatním členům společnosti vyvolává na oplátku očekávání toho, že stejně budou chráněni i oni sami [HOFSTEDE, 2001, s. 4]. Na druhou stranu ti, kteří ke společnosti nenáležejí, nejsou pokládáni za hodnověrné a hodné respektu, dokud se jim nedostane toho privilegia stát se příslušníky takové skupiny. V těchto společnostech je software zakoupený jedincem pokládán za majetek všech členů společnosti a je jimi navzájem sdílen. Vzhledem k tomu, že nejvíce kolektivní společnosti náležejí k rozvojovým zemím a softwaroví producenti pocházejí většinou z vyspělých států, jsou předem odsouzeni k tomu být vnímáni negativně.

Pirátství může být také více akceptované ve státech s nízkou životní jistotou obyvatelstva.[22] Nízká životní jistota vede k nižší odolnosti vůči změnám a k porušování pravidel, pokud je to považováno za potřebné. V národech s vysokou mírou bezpečí a jistoty jedince ve společnosti dochází ke strachu a odmítání nejistoty, kterou používání nelegálního softwaru přináší. Lidé ve státech s nízkou mírou rizika ve společnosti mohou považovat za bezpečnější a pohodlnější získávání softwaru legální cestou.

Ve studii zahrnující padesát tři zemí (později rozšířené na šedesát devět zemí),

[22] Jsou to národy s obyvatelstvem donuceným podstupovat nějaké nadměrné riziko.

Hofstede [HOFSTEDE, 2001] vytvořil index pro měření úrovně **individualismu/kolektivismu (Individual/Collectivism - IC)** a v**yhýbání se nejistotě (Uncertainty Avoiding - UA).** Tento index zůstává tím nejčastěji využívaným indexem pro měření sociálního rozměru problematiky nelegálního softwaru. Například Japonsko dosahuje podle indexu hodnoty 92 (z maxima 100), Spojené státy americké 91, Velká Británie 89 a Nizozemsko 80. Jsou proto pokládány za velmi individualistické státy. Na druhé straně spektra se nacházejí státy jako Ekvádor s indexem 8, Pákistán s indexem 14, ale i Švédsko s indexem 29, které jsou pokládány za státy s kolektivní společností.

Obecný přístup ke kopírování ve společnosti hraje velkou roli v úrovni pirátství. Na rozdíl např. od USA, kde kopírování je běžně přirovnáváno k podvádění, existují státy, kde kopírování je často chápáno jako kulturní cvičení, ne jako nemorální čin. Například asijští studenti umění jsou vzděláváni tak, že kopírují díla svých mistrů a podobnost této kopie s originálem je měřítkem úspěchu studenta. Copyright nebývá v těchto společnostech správně chápán a často ani brán na zřetel. Uvedeným přístupem je, na rozdíl od historických dob, celosvětově proslulá hlavně Čína, zatímco Japonsko postupně přejalo evropské vnímání copyrightu [SWINIARD, 1990]. Výsledná cena CD se softwarem a s hudbou je proti pořizovací výrobní ceně velmi často označována za přemrštěnou. Jedinci ve státech s vysokou mírou nejistoty mohou přemrštěný nepoměr pokládat za ospravedlnitelný důvod k pirátství.

Ale i v některých západních státech se lidé domnívají, že krádež softwaru není špatná. Jako příklad může být uvedeno pirátství v hudebním průmyslu (podrobněji bude popsáno v šesté kapitole), které je celosvětově rozšířeno. Dokonce i ve Spojených státech amerických, kde si občané mohou hudbu bez jakýchkoliv omezení koupit v obchodech nebo na internetu, je hromadně pirátsky stahována. Kupříkladu dříve pomocí softwaru jako jsou Napster či Kazaa [*Forum section...*, 2000].

Metodologie a postupy použité při zjišťování úrovně a závislostí mezi různými faktory ovlivňujícími úroveň pirátství se liší podle jednotlivých kategorií. Závislost úrovně softwarového pirátství v jednotlivých zemích je vypočítávána BSA/SPA [*Třetí výroční zpráva BSA a IDC,* 2006] na základě poměru mezi poptávkou/požadavky po novém softwaru a skutečnou výší dodaných nových softwarových aplikací [BAGHRI, 2006]. Dodávky počítačů do nejdůležitějších států jsou odhadovány ze soukromých a utajovaných dat dodávaných společnostmi, které jsou členy BSA/SPA. Počet softwarových balíčků instalovaných na každém prodaném osobním počítači tvoří stranu **produktové poptávky**. Počet softwarových aplikací legálně dodaných uživateli tvoří **dodavatelskou část**. Rozdíl mezi těmito dvěma hodnotami tvoří odhad výše softwarového pirátství. Úroveň pirátství tedy definujeme jako poměr mezi množstvím pirátského softwaru a celkovým množstvím všeho nainstalovaného softwaru. Tato data jsou kombinována a upravována tak, aby vytvořila konzistentní výpočet [*Třetí výroční zpráva BSA a IDC,* 2006]. Pokud budeme sledovat každoročně vydávané statistiky BSA, zjistíme, že ve vyspělých státech dochází k dlouhodobému poklesu případů softwarového pirátství. Sledováno bylo 37 států od roku 1996 a statistiky lze dohledat až do současnosti. Data jsou získávána z přesně definovaných zdrojů a vytvářejí na sobě vzájemné vazby.

	Definice	**Zdroj dat**	**Očekávaná závislost**
Ekonomika	HDP na osobu	Světová banka	Nepřímo úměrné (-)
Technologické faktory **Informační infrastruktura** **Přístup k internetu**	Dostupnost IT Počet poskytovatelů	Světová banka	Nepřímo úměrné (-) Pozitivní (+)
Regulátory **Regulace obchodu** **Vymahatelnost/korupce** **Počítačové právo**	Index obchodní politiky Korupční index Vztah práva k IT	Nadace Heritage TI/GU index Světové ekonomické fórum	Pozitivní (+) Nepřímo úměrné (-) Nepřímo úměrné (-)

Sociálně/Kulturní **Sociální struktura** **Sociální konservatismus**	Individualismus/kolektivismus Odmítání rizika	Hofstedův index	Nepřímo úměrné (-) Nepřímo úměrné (-)

Tabulka č. 3 – Zdroje a závislosti jednotlivých faktorů.

U ekonomických faktorů softwarového pirátství je pro zjištění HDP (jako základního faktoru) jednotlivých států zdrojem **Světová banka (World Bank – WB**) (http://www.devdata.worldbank.com/). Uvedená data jsou převzata jako celá čísla a jejich podoba koreluje s nepřímou úměrou úrovně softwarového pirátství v daných státech [GOPAL, 1997], [SHIN, 2004], ačkoliv ostatní oficiální studie [*Třetí výroční zpráva BSA a IDC, 2006*] nenacházejí v těchto datech žádnou shodu, jsou i některé, které tvrdí, že HDP daného státu je
důležitý faktor ovlivňující vznik a vzestup softwarového pirátství, i když jeho význam klesá [BAGHRI, 2006, s. 72].

Výzkum z roku 1990 si dal za úkol zkoumat příčiny pirátského chování obyvatel v USA na vzorku studentů univerzit s technickým zaměřením [CHRISTENSEN, 1991]. Úzký výběr nejpodstatnějších zjištěných faktů je předkládán v příloze. Pokud shrneme závěry tohoto výzkumu, lze konstatovat, že demografický faktor nehrál v chování studentů žádnou roli. Nepodstatné bylo i to, kdo ze 139 zkoumaných studentů byl již výdělečně činný.

Zkoumané roky:	1996	2001	2003	Zjevnost závislost 1996	Zjevnost závislost 2001	Zjevnost závislost 2003	Shrnutí
HDP	-	-	-	Zjevné	NS	NS	Částečná závislost
IT infrastruktura	-	-	-	Zjevné	NS	NS	Částečná závislost
Použití internetu	-	-	-	NS	NS	Zjevné	NS
Obchodní regulace	-	-	-	Zjevné	NS	-	Částečná závislost
ITLAW	N/A	N/A	-	N/A	N/A	Zjevné	Částečná závislost
Korupce	-	-	-	Zjevné	Zjevné	Zjevné	Závislost
IC	-	-	-	Zjevné	Zjevné	Zjevné	Závislost
UA	-	-	-	NS	Zjevné	Zjevné	Částečná závislost

Tabulka č. 4 - Sledování závislosti vlivu faktorů na úroveň softwarového pirátství (NS – not significant (není zjevné; za zjevné je počítáno vše s hodnocením 0,10, a vyšším).

Nepotvrdila se ani hypotéza, že studenti, kteří jsou seznámeni s copyrightem, se budou méně častěji dopouštět softwarového pirátství. Autor studie hledá vysvětlení tohoto faktu v tom, že pouze 30 % studentů uvedlo, že plně porozumělo všem částem tohoto práva, zatímco ostatní nepovažují kopírování softwaru mezi přáteli stejně jako instalaci legálně zakoupeného softwaru na více počítačů za přestupek. Navíc jen méně než 6 % studentů vědělo, že copyright je a může být striktně vymáhat. Takže jediným faktorem, který se ukázal být skutečně rozhodujícím, bylo vlastnictví osobního počítače, tedy prostředku k páchání softwarového pirátství. Ze studentů vlastnících osobní počítač se k softwarovému pirátství přiznalo 73 % a z těch, kteří využívali ke své práci pouze firemní či univerzitní počítač přiznalo pirátství 28 %.

Velmi důležitou otázkou zůstává, k jakému posunu v chování studentů mohlo dojít do dnešní doby. Zda zvýšená publicita soudních sporů týkajících se softwarového pirátství, hromadné zavádění „univerzitních licencí“[23], zvýšení používání softwaru s otevřeným zdrojovým kódem (open-source alternative) a další faktory změnily procentuální zastoupení studentů dopouštějících se softwarového pirátství.

Ani přesné určení technologických faktorů ovlivňujících softwarové pirátství není zcela snadné. Úroveň informační infrastruktury určujeme na základě dostupnosti dvou informačních technologií: počítačů a kabelového či satelitního připojení (oba dva faktory však v poslední době nástupem nových technologií přestávají být prokazatelné, z důvodu využívání stále nových prostředků na připojení k síti internet i na páchání počítačové kriminality) [CHIN, 2000, s. 741]. Přístup k internetu je vypočítáván na základě počtu poskytovatelů internetového připojení (**Internet Service Providers - ISPs**). Bylo řečeno, že dostupnost softwaru přes internet může redukovat potřebu pirátství, může zároveň jít o to, že internet zjednodušuje možnost získat legitimní software a ještě často za sníženou cenu. Z tohoto faktu tedy nemohou být vyvozovány žádné závěry. Pravdou také zůstává, že ač je prodej nového softwaru a upgrade (aktualizace) stávajících balíčků přes internet automaticky pokládán za prodej legálního softwaru, často může být využito určité anonymity internetu a kupovaný softwaru může být pouhou nelegální kopií s kradenými aktivačními kódy či hesly.

Různé regulační faktory zachycuje několik indexů. Výše poplatků může být zachycena v indexu nazývaném Index obchodní politiky **(Trade Policy Index - TPI)**, který byl vyvinut nadací Heritage Foundation [HERITAGE, 2006]. Tento index je založen na průměrné výši poplatků jednotlivých států. Podle výsledků porovnání můžeme říci, že úroveň pirátství je přímo svázaná s TPI indexem. Čím vyšších hodnot indexu stát dosahuje, tím nižší je jeho

[23] Jde o velmi záslužný projekt některých softwarových společností jako kupříkladu Adobe, Sun a dalších. Tyto licence jsou buďto zcela zdarma, v rámci podpory vysokých škol, nebo za snížený poplatek. Jsou určeny pouze pro použití v akademickém prostředí a mají zajistit možnost seznámení studentů s jinak finančně nedostupným softwarem.

úroveň softwarového pirátství. Další index vytváří organizace **Transparency International** spolu s Univerzitou v Göttingenu **(Göttingen University)** Jedná se o Index výšky korupce (**Corruption Index)** [TRANSPARENCY, 2006]. Existuje také Index vnímání výšky korupce **(Corruption Perceptions Index - CPI),** který vyjadřuje vnímání korupce (jak jí vidí obchodníci, analýzy rizikovosti podnikání a široká veřejnost) v rozsahu hodnoty od 10 (vysoce nekorumpovatelné) po 0 (vysoce korupční prostředí). Index černého trhu **(Black Market Index)** [HERITAGE, 2006], který je založen na CPI, měří rozmach aktivit spojovaných s černým trhem. Jelikož je zde silná korelace mezi černým trhem a Indexem vnímání výšky korupce, bývá často Index černého trhu zcela nahrazován Indexem vnímání výšky korupce. Ačkoliv je index CPI pevně spojován s úrovní softwarového pirátství, na doplnění bývá ještě uváděn index **IT-LAW** [*World Economic*], který vychází v *Global Information Technology Report* a sleduje jiný pohled na aspekty regulačního práva.

Sociálně-kulturní aspekty jsou celkově pokryty Hofstedeho kulturními dimenzemi [HOFSTEDE, 2001], kde úroveň pirátství v jednotlivých zemí je negativně úměrná národní úrovni IC a úrovní UA (vysoká IC úroveň značí vysokou úroveň individualismu, vysoká úroveň UA značí vysokou míru odmítání nejistoty ve společnosti).

Otázka závislosti mezi HDP, infrastrukturou informačních technologií, používáním internetu, obchodní regulací, korupcí a jednotlivými indexy byla sledována v analýze situace ve 37 zemích. Pokud se podíváme na shrnující tabulku č. 4, můžeme konstatovat, že ač autoři studie

pokládají počet sledovaných údajů a časové období za dostatečné, sami přiznávají, že při zanesení dosud nesledovaných faktorů či trvání průzkumu po delší dobu, může dojít k nalezení nových zákonitostí, které zatím ze získaných dat nevyplynuly [BAGHRI, 2006, s. 72].

Z údajů shrnutých v tabulce také vyplývá, že vliv jednotlivých faktorů se může během let měnit, kupříkladu faktory regulující obchod měly jednoznačně negativní dopad na úroveň pirátství v roce 1996, ale ne již v letech 2001 až 2003. A pokud dohledáme data ve výročních zprávách[24], ani v následujících letech do roku 2006. Není lehké toto vysvětlit, může jít o samotnou změnu regulačních principů, nebo o zvýšenou dostupnost softwaru za sníženou cenu, což vede k nižší potřebě po regulačních opatřeních. Na druhou stranu faktor IT-LAW je stále výraznější, což může vést k závěru, že při snižování korupčnosti prostředí a zvyšování úspěšnosti prosazování zákonů klesá ve sledovaných státech úroveň softwarového pirátství [BAGHRI, 2006, s. 76].

[24] Např. na stránkách Trade Regulation Center: http://business-law.freeadvice.com/trade_regulation/.

3. Softwarové pirátství a informační průmysl[25]

Pro protipirátský postoj je mimořádně nosná tvůrčí strategická interakce mezi korporacemi,

jež berou v úvahu softwarové pirátství a mezi softwarovými koalicemi, které toto pirátství vyšetřují [MISHRA, 2005, 223-252]. Podniky působící v informačním průmyslu si stále více uvědomují fakt, že rychlý pokrok v technologii, s kterým často nedokážou držet krok ostatní složky společnosti, činí tyto společnosti softwarovými piráty snadněji zranitelné. Softwaroví piráti kradou nejčastěji výsledky kreativní práce zaměstnanců právě těchto firem. Informační průmysl investoval a stále investuje velké prostředky za účelem ochrany sebe a zákazníků, ačkoli stále většina společností tohoto průmyslu zastává názor, že striktní vymáhání autorského práva je hlavním prostředkem k potlačení softwarového pirátství.

Obchodní toky společností zapojených v informačním průmyslu se začaly postupně měni, z prostředí klient/server se vyvinuly v globální podnikové distribuované prostředí, ve kterém se internet stal integračním elementem. Podnětem pro tento přerod byl nejen prudký celosvětový vývoj komunikačních technologií a zvyklostí, ale také nutnost informačního průmyslu reagovat na vzrůstající tlak ze strany softwarových pirátů a vzrůstající podíl softwaru proudícího neoficiálními distribučními toky.

Ve stěžejní analýze trendů vývoje distribuce softwaru z roku 1998 definoval Fred M. Greguras nutné kroky, které budou muset distribuční společnosti zapojené do informačního průmyslu podniknout, pokud budou chtít omezit ztráty způsobené softwarovými piráty a vytlačit neoficiální distribuční toky [GREGURAS, 1998].

[25] V této diplomové práci je pojmem „informační průmysl“ vnímán poněkud šířeji, než je vnímán v kontextu oboru Informační studia a knihovnictví, do informační průmyslu jsou zde zahrnováni všichni tvůrci a distributoři komerčního charakteru, jejichž produktem jsou data, ať již v textové, video či audio podobě.

World Wide Web se podle Gregurase stává důležitějším obchodním prostředím a distribučním kanálem nejen softwaru, ale veškerých informačních produktů. Proto musí **„vendoři“**(dodavatelé) a distributoři pokrčovat v integraci internetu do svých obchodních modelů a spolupracovat na vytvoření široké varianty přístupových cest, které budou vyhovovat všem zákazníkům. Tyto silné metody přímé distribuce se mohou dostat do konfliktu s již existujícími metodami, ale jsou jedinou možnou cestou, kterou mohou softwarové společnosti konkurovat pirátské distribuci po ekonomické stránce. Podmínkou pro masové zavedení těchto **Obchodních modelů masového trhu (Mass Marked Business Models)** bylo dopracování softwarových licencí a právní ochrany takto distribuovaného softwaru.

Proces přidělování softwarové licence se postupně stal standardizovaným pro všechny velké informační distributory, v podobě **Uniform Commercial Code Article 2B „Licenses“,** což je konkrétní forma takzvané **Koncové uživatelské licenční smlouvy (End User License Agreement - EULA).** EULA je označení pro licenční ujednání (licenční smlouvu), které nákupem určitého počítačového programu (softwaru) uzavírá koncový uživatel s jeho tvůrcem, respektive výrobcem (podrobněji je o této problematice pojednáno v páté kapitole). Uvedené kroky přes stálou spornost vymahatelnosti těchto **Zastřešujících licencí (Shrink-wrap Licence)** značně urychlily proces smluvního jednání mezi zákazníkem a dodavatelem. Dále byl v obecné používání zaveden modul takzvané „podnikové multilicence“ a tím snížen výskyt porušování licenčního ujednání ze strany firem. Před jeho zavedením často docházelo ze strany firem k nepochopení nutnosti jiné smlouvy při instalaci softwaru na více počítačích jedné organizace.

Ve shodě s Greguresovou analýzou se email stal široce používaným komunikačním prostředkem v oblasti zákaznické podpory a komunikace s klienty. I velké informační koncerny začaly využívat webové stránky jinak, než jen jako místo umístění nabídky

produktů a reklamy, staly se plnohodnotným informačním centrem. Postupně se ukazuje, že zavedením sekcí jako jsou: Často kladené dotazy (**Frequently Asked Question(s) – FAQ**), Nápovědy a Manuály (**Helps and Manuals**) a dalších došlo nejen k uspokojení zákazníkovi potřeby po informacích, ale také k výraznému ušetření nákladů vynakládaných na zákaznickou podporu [KRUG, 2000, s. 150].

Pokud se s jistým nadhledem podíváme na směr, kterým se informační průmysl vydal a na prostředky, jež začal využívat, nabízí se myšlenka přejímání prostředků a postupů již vyzkoušených hackerskou komunitou a softwarovými piráty. Všechny níže jmenované prostředky, které dnes využívají velké i malé podniky informačního průmyslu pro svou rychlejší a snadnější práci, používali a používají i softwaroví piráti. Nejnovějším a podle názoru autora práce zcela zásadním příkladem je nasazení technologie P2P jako distribuční technologie velkými firmami hudebního průmyslu. Jde o nejnovější z řady technologií, která byla dříve považována prakticky za pirátský nástroj. První krok nastal, když nejvlivnější nahrávací společnosti Warner Bros., Disney a Atlantic Records koupily přímo monitorovací software pro P2P sítě od firmy BigChampagne. Právě tato firma monitoruje P2P síť Kazaa od roku 2000. Monitorovány jsou např. informace o tom, v jakém počtu jsou alba či písničky konkrétního interpreta sdílena, stahována a kolikrát je jeho jméno zadáno ve vyhledávací části programu. Jsou to velice cenné informace pro hudební vydavatelství, která se pak podle toho mohou řídit na trhu s klasickými CD nebo on-line prodejem, jež je dnes stále na vzestupu [RIAA opět...].

Nejen producenti softwaru, nahrávací společnosti, ale kupříkladu i webové rozhlasové stanice jsou ovlivňovány dopadem porušování autorského práva, přesněji regulačních opatření, která se o autorské právo opírají. Společnost Copyright Royalty Board ve Washingtonu vydala rozhodnutí o ztrojnásobení autorských poplatků ze své produkce. Internetová rádia by tedy měla platit o 300 - 1 200 % vyšší poplatky. Uvedené rozhodnutí

navíc počítá se zpětnou platností, což znamená platbu poplatků za již odvysílanou hudbu. Již dnes je zde patrný rozdíl mezi poplatky amerických internetových stanic a stanic vysílaných přes satelit. Nařízení mělo vejít v platnost 15. května 2007. Protikrokem ze strany internetových rádií bylo zřízení webové stránky www.savenetradio.org, která informuje o možných dopadech uvedeného nařízení. Jejím cílem je záchrana internetových rádií. Jedná se o modelovou situaci mnoha jiných pokusů o regulační proces, podložený autorským právem, využívající naladění informační společnosti na protipirátský boj a aplikovaný na volný trh a o regulaci spontánně vznikajících uskupení, která participují na informačním toku a podílí se na šíření informací [NÝVLT, 2007].

4. Mezinárodní a národní organizace zabývající se problematikou softwarového pirátství

4.1 Business Software Aliance

Organizace **BSA** (**Business Software Alliance)** je od roku 1988 mluvčím předních světových výrobců softwaru. Postupně se jí podařilo vydobýt přední postavení mezi organizacemi zabývajícími se problematikou softwarového pirátství a ochranou autorských práv. Její hlavní činností je organizace akcí a vzdělávacích programů zaměřených na autorskoprávní problematiku. Členy BSA aktivními v České republice jsou společnosti Adobe Systems Europe, Apple IMC, Autodesk, Bentley a Microsoft.

Hlavním cílem BSA je ochrana autorských práv členů aliance, ať už prostřednictvím trestních řízení či prevencí formou osvěty. Při své činnosti používá BSA jednak metody progresivní (semináře, přednášky, osvětovou činnost), jednak, a to především, metody represivní (ukládání a vybírání pokut, podávání trestních oznámení).

Velmi významným počinem BSA je vydávání každoroční zprávy nazvané *Podrobná studie BSA-IDC o globální míře softwarového pirátství* [Business Software Alliance, 2007]. Zpráva je vydávána ve spolupráci s organizací **International Data Corporation** (**IDC**), která je analytickou firmou specializující se na informační technologie, statistiky a konzumentskou technologii [Business Software Alliance, 2000].

Sesterskou organizací BSA je **Entertainment Software Association (ESA)**, jejímž cílem je ochrana počítačových her jako specializovaného softwaru. Vzhledem ke stoupající

produkci tohoto zábavního průmyslu a vysokému počtu nelegálního kopírování jeho produktů, důležitost této asociace stále roste.

4.2 Jiné organizace

Není podmínkou, aby firmy zainteresované v informačním průmyslu vytvářely vždy organizace s pevnou strukturou, další možností jejich sdružování jsou **iniciativy**. Obvykle jde o sdružení firem a jiných právních subjektů za předem definovaným účelem. Iniciativy často slouží k jednotnému postupu ve zvolené problematice a umožňují koordinované nasazování domluvených prostředků do praxe. Příkladem může být setkání zástupců firem Sony, Time-Warner, EMI, Universal Music Group a dalších v roce 1998. Tito zástupci se dohodli na nutnosti vyvinout model pro distribuování hudby přes digitální platformy, jako je kupříkladu internet. Cílem tohoto modelu bylo primárně vybírání zisků z této distribuce, ale také její zabezpečení.

Za podpory **Americké asociace nahrávacího průmyslu (Recording Industry Association of America - RIAA)** a také kupříkladu firem **America Online, Microsoft** či **RealNetworks** vznikla v roce 1998 **Iniciativa pro zbezpečení digitální hudby (Secure Digital Music Initiative - SDMI)**. Tato iniciativa si vytyčila za cíl za pomoci společností specializovaných na bezpečnostní technologie vyvinout standard SDMI, který by dokázal zabezpečit přehrávání, archivaci a distribuci digitální hudby. Standard byl vytvořen a v **Otevřeném dopise digitální komunitě (*Open Letter to the Digital Community)***, byla také vypsána **Výzva SDMI (SDMI Challange)**, ve které byli vyzváni všichni hackeři a odborníci z oblasti informačních technologií, aby se pokusili ochranu prolomit. Schéma bylo prolomeno skupinou, ve které byl i známý počítačový odborník Ed Felten, což vedlo k zániku iniciativy z důvodu nesplnění základního existenčního úkolu. Tento fakt popsal Eric Scheirer ve své

zprávě „*The end of SDMI*“. Pozitivním důsledkem vytvoření SDMI iniciativy bylo bezesporu globální rozšíření formátu MP3 jako univerzálního audioformátu [SCHEIRER, 1999].

Trvalejšího charakteru jsou **asociace** utvářené různými subjekty na spravování konkrétní problematiky. Jak již bylo zmíněno, mezi nejdůležitější asociace zabývající se bojem se softwarovým pirátstvím patří **Americká asociace pro nahrávací průmysl (Recording Industry Association of America - RIAA).** Jedná se o obchodní asociaci, která zastupuje nahrávací průmysl v USA. Asociace byl založena v roce 1952. V průběhu svého působení se podílela

na sestavování technického standardu pro frekvenci vinylových desek. Spolupracuje na udělování hudebních licencí a pravidelně uděluje ceny za hospodářskou úspěšnost prodaných skladeb. Jejím hlavním posláním v posledních letech však je boj proti pirátskému kopírování a sdílení hudby. RIAA je známa mnoha žalobami podávanými u amerických soudů všech úrovní a soudním bojem jak proti provozovatelům sítí P2P, tak proti jejich uživatelům.

V roce 2006 podala RIAA 2 500 žalob na 20 000 lidí v USA za porušování autorských práv [*RIAA opět...*]. Tato vysoká čísla zdůvodňuje finanční ztrátou firem hudebního průmyslu ve výši 4,2 miliard dolarů ročně. Vzhledem k nákladnosti těchto žalob a z důvodu neúspěchu hromadných žalob vůči provozovatelům a uživatelům sítí P2P v roce 2006 asociace RIAA zahájila **Výhodný prodej (Discount settlement)**. Jde o program, ve kterém nabízela poskytovatelům internetu, vzdělávacím institucím a koncovým uživatelům možnost přiznat se a zaplatiz autorské poplatky předtím, než zveřejní jejich identitu [*Who We Are*]. Za tímto účelem byl spuštěn nový web RIAA (http://www.p2plawsuits.com), kde je možné ve čtyřech krocích uzavřít a zaplatit „dohodu” s RIAA on-line.

Ve většině případů totiž nyní RIAA ještě před samotnou žalobou nabídne odhalenému pirátovi tzv. dohodu. Za určitou částku vypočtenou podle stažených dat (většinou jde o částku do 4 000 dolarů) stáhne RIAA žalobu.

Obrázek č. 1 - Odpověď vygenerovaná při zaplacení na stránce http://www.p2plawsuits.com.

Podobnou asociací jako RIAA, pouze s jiným zaměřením, je **Americká asociace filmového průmyslu (Motion Picture Association of America - MPAA),** přesněji Motion Picture Producers and Distributors Association of America. Tato nevýdělečná obchodní asociace se zaměřuje na americký film. Je tvořena šesti největšími americkými filmovými nahrávacími společnostmi a mezi její hlavní úkoly patří lobbing za zájmy těchto firem, ochrana jejich duševního vlastnictví a tvorba amerického ***hodnocení (ratingu)*** filmů. MPAA se podařilo pomocí žalob dosáhnout uzavření mnoha torrentů[26], tedy sítí na sdílení dat (např. LokiTorrent či EliteTorrents) a stránek (nař. *The Pirate Bay).* Pokračují ve vypouštění falešných „fake torrentů", prohledávání harddisků lidí stahujících hudbu a v podobných aktivitách, které slouží k boji proti pirátství. Pro svou kontroverzní politiku je stejně jako RIAA kritizována mnoha odpůrci z řad organizací zabývajícími se ochranou lidských práv a svobod. Tyto organizace dosáhly stažení produktu **MiiVi client**, který MPAA vyvíjela, a jenž měl sloužit k legálnímu stahování filmů, ale zároveň měl hledat nelegální produkty na harddiscích uživatelů [*Motion Picture* …].

[26] Jako torrent může být označován nejen soubor s lokací cílového dokumentu a seznamem seedů a peerů, ale také souhrnně celá síť. Která tuto technologii využívá.

Organizace, která úzce spolupracuje s MPAA a s RIAA při ochraně formátu DVD, se nazývá **Asociace pro kontrolu kopírování DVD (DVD Copy Control Association)**. Tato organizace vznikala v souvislosti s rozšířením formátu DVD nejen k jeho ochraně, ale také k jeho propagaci [DVD Copy Control Association, 2000]. V současné době patří mezi její aktivity prodej algoritmu CSS zabezpečovacího DVD formát. Kromě prodeje všem firmám, používajícím formát DVD k ukládání vlastních dat rozvíjí asociace nové formáty Blu-Ray a HD DVD, ve které byla vkládána stejná naděje jako do médií obsahujících prostředky zamezující kopírování. Dále se DVD Copy Control Association stále podílí na boji proti šíření kódu DeCSS[27] po internetu i mimo něj, a to v jakékoliv podobě. V boji proti šíření klíče obcházejícího ochranu AACS ho nahradila asociace **Licensing Administrator** (**AACS LA**) [HROUŽEK, 2007].

Asociací zabývající se přímo ochranou softwaru a spolupracující ve velké míře s BSA je **Software and Information Industry Association (SIIA)**. Tato organizace vznikla přerodem z **Software Publishers Association (SPA)** v roce 1999. SIIA se skládá z šesti divizí, kterými jsou: Veřejná politika (Public Policy), Protipirátská ochrana (Anti-piracy), Software (Software), Obsah (Kontent), Vzdělávání (Education) a Finanční a informační servis (Financial Information Services). Je také producentem periodika *Codie Awards*. Celkové zaměření SIIA není v takové míře orientováno na ochranu práva a boj proti softwarovým pirátům, ale spíše na propagaci softwaru, na hledání nových modelů (např. „**open source**“) a na výzkum celé problematiky.

Další známou organizací je **Mezinárodní federace producentů nahrávek hudby a videa (International Federation of Phonogram and Videogram Producers - IFPI),** jež se zabývá oblastí video a audio průmyslu a spolupracuje s RIAA a národními organizacemi.

[27] Technologie DeCSS byla vyvinuta na ochranu formátu DVD, jejím nástupcem pro nová média je technologie AACS.

Za nejdůležitější národní organizace jsou označovány: **British Phonographic Industry (BPI),** která se zabývá ochranou hudebních produktů a **Federation Against Copyright Theft (FACT),** instituce se zaměřením na ochranu copyrightu, jež působí ve Velké Británii. Dále **Canadian Recording Industry Association (CRIA),** nevýdělečná kanadská obchodní asociace sdružující všechny společnosti tvořící a prodávající hudební záznamy, **Australian Recording Industry Association (ARIA),** chránící sbírky a hudební licence v Austrálii, podobně jako asociace **Recording Industry Association of New Zealand (RIANZ)** na Novém Zélandu. Ve Španělsku působí **General Society of Authors and Publishers (SGAE)**, v Japonsku **Japanese Society for Rights of Authors, Composers and Publishers (JASRAC)** a **Recording industries Association of Japan (RIAJ),** v Rusku **Russian Organization on Collective Management of Rights of Authors and Other Rightholders in Multimedia** a **Digital Networks & Visual Arts (ROMS)**.

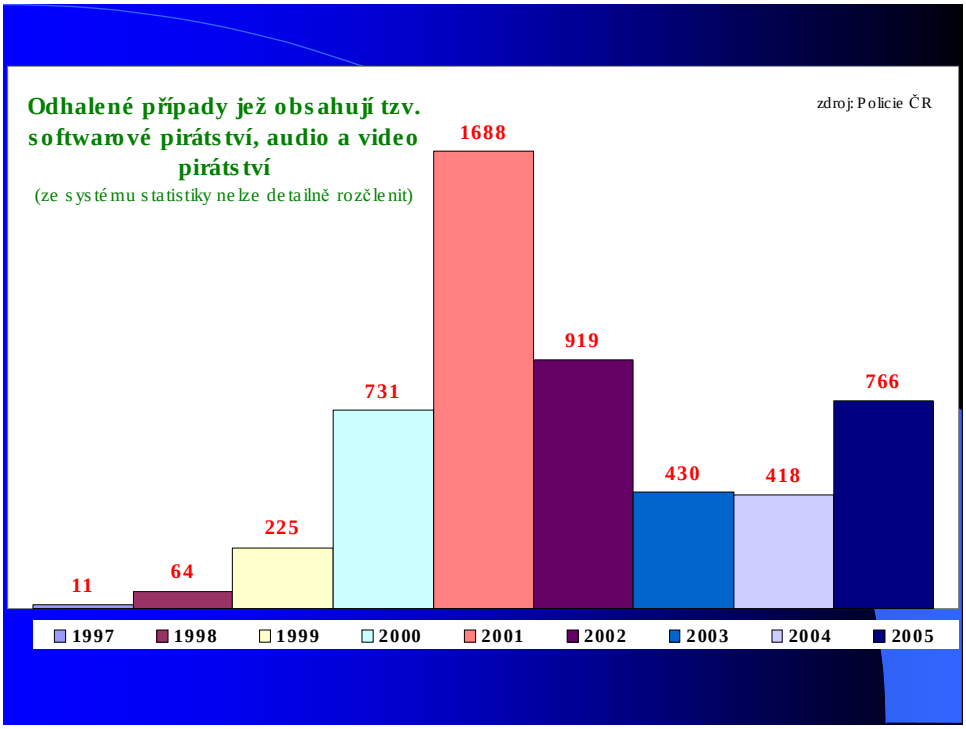
Také organizace, které se zabývají softwarovým pirátstvím pouze okrajově, často publikují velmi důležité dokumenty či přispívají k pokroku při návrzích zákonů sloužících k boji proti softwarovému pirátství. Příkladem může být iniciativa z roku1979, kdy byl pod záštitou **Světové organizace duševního vlastnictví (World Intellectual Property Organization (WIPO)** vydán typový zákon, který měl sloužit jako vzor pro zákony na ochranu počítačových programů. Tento zákon byl vytvořen jako vzor konkrétním zákonům, jež si měly jednotlivé státy vydat samostatně. Jde pouze o okrajový čin mezinárodní organizace WIPO, o které je v této diplomové práci pojednáno podrobně v druhé kapitole. Přesto však byl její návrh typového zákona významným krokem v boji proti softwarovému pirátství.

V České republice kromě BSA a státních orgánů (Policie ČR) existují také soukromé subjekty, je kupříkladu firma **Software Security (SWS**), jejíž ředitel Jiří Jakubka udává

činnost firmy jako „*monitorováním činnosti softwarových pirátů, objasňování případů porušování autorských práv a další formy neoprávněného užívání v oblasti herního softwaru pro PC a herní konzole (např. PlayStation od společnosti SONY)*“. Toho se dopouštějí zejména tzv. počítačoví piráti prodávající kopírovaný software a v neposlední řadě i provozovatelé nelegálních počítačových heren a heren s konzolemi PlayStation. Firma SWS vydává čtvrtletní zprávu o své činnosti.

Kromě BSA a SWS jsou v České republice i jiné soukromé firmy spolupracující s Policií ČR na vyhledávání softwarových pirátů a jedinců či firem porušujících autorské právo. Velmi známá jsou občanská sdružení **Dillia** a **Ochranný svaz autorský (OSA),** ale také kupříkladu **Agentura pro ochranu softwaru**, s jejímž návrhem na užší spolupráci v této oblasti s finančními orgány souhlasilo Ministerstvo financí ČR. První náměstek ministra financí ČR Miloslav Fiedler dokonce přímo prohlásil, že činnost těchto organizací je velmi záslužná. Ze spolupráce Agentury pro ochranu softwaru s Finančním ředitelstvím pro Středočeský kraj následně vznikl *Metodický pokyn pro finanční kontrolory*. Zákonným podkladem pro tento právní akt organizační povahy jsou ustanovení Zákona o územních finančních orgánech (zákon č. 531/1990 Sb. ve znění pozdějších změn a doplňků), Zákon o dani z přidané hodnoty (588/1992 Sb. ve znění pozdějších změn a doplňků), Zákon o daních z příjmů (586/1992 Sb. ve znění pozdějších změn a doplňků) a Zákon o účetnictví. Na základě tohoto metodického pokynu mohou finanční kontroloři podrobovat kontrole veškerý software užívaný organizacemi k jejich podnikatelské činnosti
a zjišťovat, zda nedochází k daňovému úniku nebo k porušování uvedených zákonů. Agentura pro ochranu softwaru na základě dvoustranných smluv provádí tzv. *softwarové audity*.
Ve smlouvě o provedení auditu se agentura zavazuje provést kontrolu veškerého softwaru používaného na všech počítačích provozovaných v příslušné organizaci. Po úspěšně skončeném auditu obdrží příslušná organizace tzv. *Deklaraci čistoty*. Ta je jakýmsi

potvrzením, že v kontrolovaném podniku není ani na jediném počítači jiný než legální software [KREMEROVÁ, 1998].



Obrázek č. 2 - Případy odhalené na základě spolupráce Policie ČR a externích firem.

Další velmi významnou agenturou v České republice je **Česká protipirátská unie (ČPU)**. Její aktivita je velmi výrazná zejména v poslední době, k jejímu mediálnímu zviditelnění přispěl podíl na soudních kauzách zahájených proti softwarovým pirátům v roce 2007.

Organizace zabývající se problematikou softwarového pirátství a ochrany autorských práv nezasahují pouze proti jedincům a malým firmám. Velmi často dochází také k zapojení těchto firem do autorskoprávních sporů velkých organizací či dokonce států. Příkladem může být postup Spojených států, které podaly 10. 4. 2007 u **Světové obchodní organizace (WTO)** dvě oficiální stížnosti na Čínskou lidovou republiku. Obě tyto žaloby se týkají pirátského nakládání s autorskými právy a nedostatečné ochrany duševního vlastnictví před nelegálním nakládáním a malého úsilí Číny v boji s nelegálně kopírovaným softwarem, knihami, filmy a

s hudebními nahrávkami americké provenience na čínském trhu. V USA dohlíží na tuto problematiku **Úřad obchodního zmocněnce (US Trade Representative - USTR)**, jehož ředitelka Susan Schwabová oznámila, že Američané ročně ztrácejí v Číně kvůli nedostatečné ochraně autorských práv a duševního vlastnictví miliardy dolarů. Čínská lidová republika reagovala ústy vedoucího **Úřadu pro intelektuální vlastnictví (Internationaux Réunis nalévat la Protection de la Propriété Intellectuelle)** Tiana Lipua, označila žalobu USA za nešťastnou a ignorující úsilí vlády, které problematice věnuje. Navíc tvrdí, že rozvojové země potřebují čas, aby mohly vyhovět všem požadavkům Světové obchodní organizace. Vláda Čínské lidové republiky dokonce pohrozila,
že tento akt může výrazně narušit ekonomickou spolupráci obou zemí. Důsledkem tohoto prohlášení byl dle Světové banky pokles amerického dolaru. Americká iniciativa je také vyvolána ekonomickými zájmy státu. Kongres USA je znepokojen dlouhodobým obchodním deficitem, který mají Spojené státy americké s Čínou. Ten vzrostl za rok 2006 o 15 % na hodnotu 232,5 miliardy dolarů. Žaloba na porušování copyrightu sice není jedinou žalobou, kterou Spojené státy americké na Čínu v poslední době podaly (další jsou např. žaloba na nelegální subvence čínské vlády svým průmyslovým podnikům či stížnost na obstrukce s dovozem náhradních automobilových součástek do Číny), ale síla reakce, kterou tato akce vyvolala, se řadí mezi nejdůležitější a zřejmě potvrzuje teorii, že počítačové pirátství, obchod s nelegálním softwarem a další způsoby porušování práv na duševní vlastnictví jsou tématem, které je řešeno nejen na soukromé, národní, ale i mezinárodní úrovni [*USA si stěžují*…, 2007].

První mediálně velmi sledovanou akcí státních organizací zabývajících se problematikou softwarového pirátství byl pravděpodobně zátah na softwarové piráty a hackery v USA. Dne 9. května 1990 byl státním zástupcem v Phoenixu v Arizoně vyhlášen výsledek operace *„Sundevil“*

[SUNDEVIL, 2002]. Během této operace byl provedeno 27 domovních prohlídek, tři zatčení ve dvanácti státech USA. **Úřad státního zástupce** ve Phoenixu udával jako hlavní důvod této operace ztráty telefonních společností v důsledku kriminální činnosti ve výši dosahující miliony dolarů. Na operaci spolupracovala i Tajná služba USA (ASS). Dodnes je velmi citován výrok, zástupce ředitele Tajné služby USA Jankinse, který byl nejvýše postaveným státním zástupcem zapojeným v operaci: *„Dnes vyslala Tajná služba jasný signál všem počítačovým hackerům, kteří se rozhodli porušovat zákony této země v mylné víře, že se mohou vyhnout dopadení úkrytem za své relativně anonymní počítačové terminály. (…) Vytvořili organizované skupiny za účelem výměny informací usnadňujících jejich kriminální aktivity. Tyto skupiny spolu často komunikují prostřednictvím systému pro předávání zpráv mezi počítači, zvaných „bulletin boardy“. (…) Naše zkušenosti ukazují, že mnozí z počítačových hackerů nejsou již pouhými svedenými nezletilci zneužívajícími počítačů ve svých ložnicích ke zlomyslným hrám. Nyní jsou mezi nimi i vysoce kvalifikovaní počítačoví profesionálové páchající pomocí počítačů trestnou činnost.“* [STERLING, 1994].

Pokud sledujeme tiskové zprávy a oficiální vyjádření, které doprovází současné operace policie (nejen Policie ČR) a spolupracujících mezinárodních organizací zabývajících se problematikou nelegálního softwaru, můžeme dojít k dojmu, že reakce a prohlášení výkonných složek státní moci se prakticky nezměnily. Například operace Policie ČR ve spolupráci s BSA, o kterých informuje iDnes: *„9.10.2006 - Softwaroví piráti v Česku budou mít brzy těžší život. Nová opatření, která se proti nim chystají, se zaměří především na malé a střední firmy zejména v Praze, policie tak vyhlásila další kolo boje softwarovým pirátům.“* [NÝVLT, 2007], či například postup slovenského **Národného bezpečného úradu (NBÚ**) ve spolupráci s **Federal Bureau of Investigation (FBI)** proti společnosti vlastnící servery, na kterých byly umístněny mimo jiné dvoje webové stránky sloužící ke komunikaci, převážně využívané počítačovými specialisty, serverovými administrátory a hackery a následnému

vyjádření zástupců zúčastněných institucí [ANONYMOUS, 2006]. Této reakci a tomu, co jí předcházelo, bude věnována pozornost v kapitole o metodách softwarového pirátství [NOSTUR, 2006].

Operace *Sundevil* se uskutečnila před 17 lety [*Sundevil*, 2002], přesto zůstává stále v paměti hackerů a příslušníků počítačového undergroundu. Je pokládána za první z represivních akcí, které vedou k potlačování jejich práv a svobod. Tento pohled je prakticky konzistentní a stejné názory jsou prezentovány na všech možných diskusních fórech a digitálních komunikačních centrech využívaných hackery k prezentaci jejich názorů. Pravdou zůstává, že i v dnešní době lze stále nalézt mnoho pravdivého na slovech Bruce Sterlinga: *„Ze své strany policisté běžně kladou rovnítko mezi všechny hackerské trestné činy a rozbíjení veřejných telefonů krumpáčem. Výčty „finančních ztrát“ vzniklých v důsledku průniku do počítačů jsou notoricky přehnané. Neautorizované zkopírování dokumentu z cizího počítače je morálně postaveno na stejnou úroveň jako loupež, řekneme, půl milionu dolarů z majetku společnosti. Nezletilý hacker, který se zmocnil „důvěrného“ dokumentu, ho za takovou sumu zaručeně neprodal, nemá pravděpodobně žádnou představu, jak jeho prodej zařídit, a ještě pravděpodobněji ani neví, co vlastně sebral. Nezískal ze svého zločinu ani cent zisku, nicméně morálně je postaven na úroveň zloději, který vykradl kostelní pokladničku a zmizel do Brazílie. Policisté jsou přesvědčení, že všichni hackeři jsou zloději. V americkém právním systému je nesnadné, téměř nemožné odsoudit lidi do vězení jen proto, že se chtějí dozvědět věci, jež je jim zakázáno znát. V americkém kontextu je téměř každý důvod k potrestání lepší než věznit lidi kvůli ochraně jistých druhů informací. Nicméně „restrikce informací“ je esencí boje proti hackerům.“* [STERLING, 1994]

První represivní akce proti hackerům na území USA měli také významný efekt a to vyprovokování debaty o elektronickém zločinu, svobodě tisku, domovních prohlídkách a politice v kyberprostoru. Ještě jeden důsledek byl zpočátku přehlížen, a to fakt, že po

srozumitelném seznámení společnosti s telefonní a informační trestnou činností a za pomoci zvýšené popularizace a medializace této činnosti, došlo k jejímu zvýšení. Stejného efektu často nešetrnými a tvrdě vedenými žalobami dosahují organizace zabývající se problematikou softwarového pirátství.

5. Právní problematika softwarového pirátství

Zamyslíme-li se nad právní problematikou softwarového pirátství z širšího hlediska, můžeme konstatovat, že v rámci mezinárodního práva tato problematika spadá pod pojem „duševní vlastnictví“. Ochrana duševního vlastnictví se systematicky začala rozvíjet již koncem 19. století. V roce 1893 byla ke správě několika v té době platných mezinárodních úmluv (Pařížská úmluva na ochranu průmyslového vlastnictví z roku 1883, Bernská úmluva na ochranu literárních a uměleckých děl z roku 1886 [Bernská úmluva, 1886] a Madridská dohoda o mezinárodním zápisu továrních nebo obchodních známek z roku 1891) zřízena organizace Spojených mezinárodních úřadů duševního vlastnictví. Její reorganizace vedla ke zřízení **Světové organizace duševního vlastnictví (World Intellectual Property Organization - WIPO)**.

Úmluva o zřízení této organizace byla schválena na mezinárodní konferenci ve Stockholmu dne 14. července 1967 a vstoupila v platnost dne 26. dubna 1970.

Světová organizace duševního vlastnictví je specializovanou odbornou organizací v systému **Organizace spojených národů (United Nations - UN)** s mandátem koordinovat mezinárodně právní ochranu duševního vlastnictví. Sdružuje 179 států světa. Česká republika je členem organizace od 1. 1. 1993, bývalé Československo bylo členem od jejího vzniku v roce 1970 a členským státem obou hlavních úmluv od roku 1921.

Úmluva o zřízení Světové organizace duševního vlastnictví pod pojmem duševní vlastnictví rozumí práva k literárním, uměleckým a vědeckým dílům, k výkonům umělců, ke zvukovým záznamům a rozhlasovému vysílání. Dále sem řadí práva k vynálezům ze všech oblastí lidské činnosti, k vědeckým objevům, k průmyslových vzorům a modelům, k továrním, obchodním známkám a známkám služeb, k obchodním firmám a obchodním

názvům, práva na ochranu proti nekalé soutěži a jakož i všechna ostatní práva vztahující se k duševní činnosti v oblasti průmyslové, vědecké, literární a umělecké [*26. duben...*].
Na konferenci v Ženevě v roce 1996 byla přijata **Smlouva Světové organizace duševního vlastnictví (WIPO)** o právu autorském. Smlouva vstoupila v platnost dne 6. března 2002.

V současné době WIPO spravuje v oblasti práv k duševnímu vlastnictví 24 různých mezinárodních dokumentů.

Jak již bylo zmíněno, požadavky na přijetí normy pro ochranu softwaru na mezinárodní úrovni vedly pod záštitou WIPO v roce 1979 k vydání typového zákona, který měl sloužit jako vzor pro zákony na ochranu počítačových programů vydávané v jednotlivých státech.

5.1 Problematika copyrightu v USA

Prudký rozvoj počítačového průmyslu ve Spojených státech amerických vyvolal v této zemi nutnost řešit ochranu softwaru již dříve [BUNN, c2005]. Základ obecné autorskoprávní ochrany je v USA zakotven v článku 1/8/8 americké ústavy. Ten stanoví výhradní právo autorů (původců) a vynálezců na jejich díla a vynálezy. Konkrétní právní ochrana je vymezena v autorském zákoně z roku 1976.

V roce 1980 byl jako doplněk autorského zákona přijat **Zákon o softwarovém copyrightu (Software Copyright Act)**. Za nejpodstatnější část tohoto amerického zákona lze považovat sekci 117.[28]

---

[28] „Notwithstanding the provisions of section 106, it is not an infringement for the owner of copy of a computer program to make or authorize the making of another copy or adaptation of the computer program provided:
(1) that such a new copy or adaptation is created as an Essentials step in utilization of the computer program in conjunction with a machine and than it is used in no other manner, or
(2) that such a copy or adaptation is for archival purposes only and that all archival copies are destroyed in
the ebony that continued possession of the computer program should cease to be rightful.
Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale or other transfer of all rights in the program. Adaptations so prepared may be transferred only with such authorization of the copyright owner." [*Software*...]

Počítačový program je v tomto zákonu definován jako posloupnost instrukcí nebo příkazů, která je určena pro přímé nebo nepřímé použití počítačem za účelem dosažení požadovaného výsledku. Je zde zakotvena možnost převedení copyrightu na zaměstnavatele nebo jinou právnickou či fyzickou osobu. Vytváření kopií nebo drobných úprav počítačového programu je povoleno, pokud budou využívány na jednom konkrétním počítači nebo k archivním účelům. Po skončení platnosti licence musejí být všechny kopie programu zničeny.

Do roku 1988 existovala v USA povinná registrace děl, a to včetně počítačových programů. Neregistrovaným dílům nebyla právní ochrana poskytována. V současnosti je tato registrace dobrovolná. Je však velmi často používána, protože v případném autorskoprávním sporu podstatně usnadňuje důkazní situaci:

V oblasti angloamerického systému práva se jako obecně závazný pramen práva používají i soudní precedenty, tedy rozhodnutí soudů v konkrétních věcech, zatímco v kontinentální Evropě jsou obecně závazné pouze zákony. Vzhledem k tomu jsou některé problémy v USA ponechány k uvážení a dořešení soudní praxi. Mezi takové případy patří i otázka, v jaké formě je počítačový program chráněn, tedy jestli je chráněn jenom jako zdrojový text nebo strojový kód, nebo jestli je chráněn i ve spustitelném tvaru (operační systém, ostatní softwarové nadstavby nad technickým vybavením, veškeré aplikace) [KREMEROVÁ,1998].

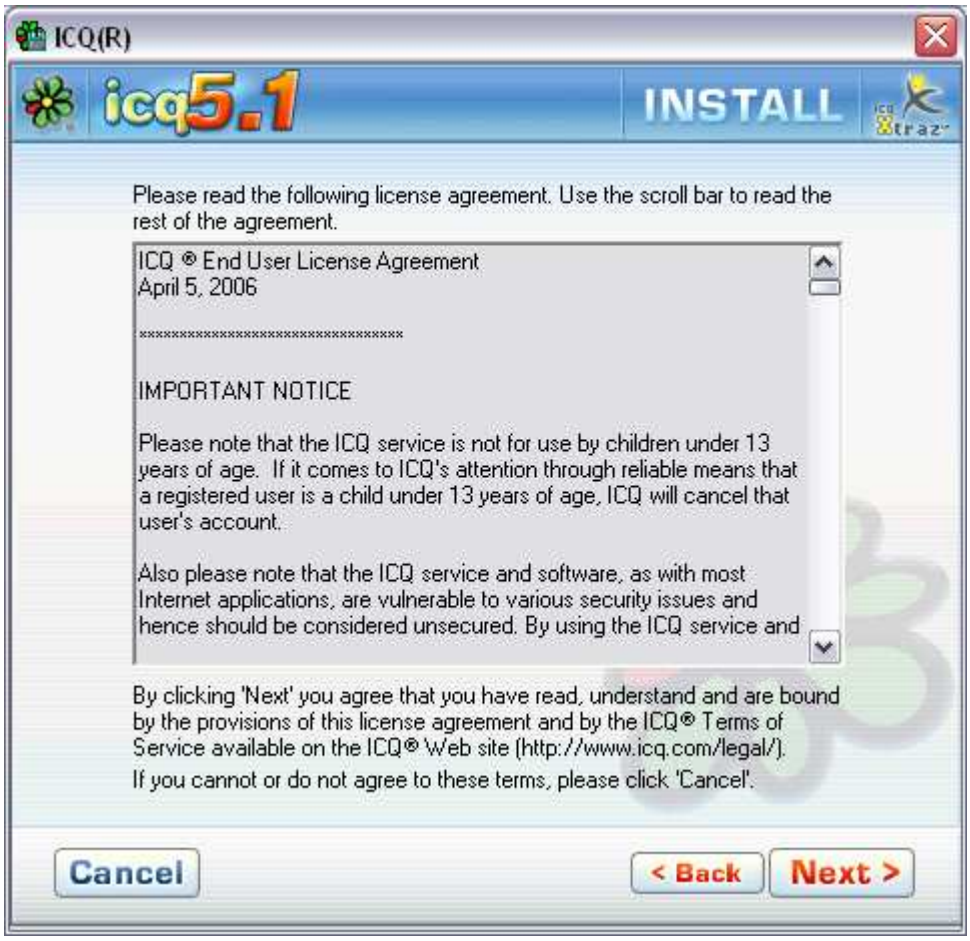
Vymezení softwarového pirátství ve vztahu k autorskému právu však zůstává stále nedořešeno. Softwarové společnosti častěji licencují software raději, než aby ho pouze prodávaly. Pokud je software licencován a s jeho provozem jsou spojeny další potřeby kontaktu

a komunikace s dodavatelskou společností (např. aktivace softwaru, autentizace[29] softwaru na

[29] Autorizace je postup, který omezuje přístup k informacím, funkcím a dalším objektům. Přístup mají pouze oprávněné subjekty. Proces autorizace vyžaduje auntetizaci (proces prověření identity) subjektu a vyhledání v seznamu oprávněných subjektů, jejich rolí a práv.

webových stránkách dodavatele, stahování a implementace upgrade pouze po autentizaci uživatele). Navíc, pokud je softwaru licencován, uživatel si kupuje pouze licenci a jeho práva a možnosti nakládat se softwarem jsou omezenější, většinou například přichází o právo vytvářet si kopii softwaru pro vlastní potřebu.

Často bývá od uživatele vyžadován podpis/souhlas s takzvanou smlouvou typu **„shrink-wrap“** i při nelicencovaném prodeji nebo instalaci softwaru v jakékoliv formě. Tato smlouva vymezuje práva uživatele nakládat s produktem a její ustanovení bývají běžně striktnější než autorské právo. Typické limitace softwarových licencí, které přesahují autorské právo jsou např. omezení použití softwaru pouze na jednom počítači (standardně je počítač identifikován při internetovém ověřovacím procesu číslem tzv. MAC adresy), restrikce na vytváření kopií softwaru a dokumentace k němu, restrikce zamezující modifikaci softwaru a na prodávání jeho kopií [GEMIGNANI, 1986].



Obrázek č. 3 - Licenční ujednání při instalaci upgrade programu ICQ 5.1
Zdroj: [http://www.icq.com].

5.2 Problematika duševního vlastnictví v EU

V rámci Evropské unie rozpracovávají problematiku duševního vlastnictví dokumenty vydané jako směrnice Evropského parlamentu a Rady:

- Směrnice Rady 91/250/EHS ze dne 14. 5. 1991 o právní ochraně počítačových programů [Evropská unie, 1991].
- Směrnice Rady 92/100/EHS ze dne 19. 11.1992 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s autorským právem [Evropská unie, 1992].

- Směrnice Rady 93/83/EHS ze dne 27. 9. 1993 o koordinaci určitých předpisů týkajících se autorského práva a práv s ním souvisejících při družicovém vysílání a kabelovém přenosu [Evropská unie, 1993a].
- Směrnice Rady 93/98/EHS ze dne 29. 10. 1993 o harmonizaci doby ochrany autorských práv a určitých práv souvisejících [Evropská unie, 1993b].
- Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11.3.1996 o právní ochraně databází [Evropská unie, 1996].
- Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. 5. 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti [Evropská unie, 2001a].
- Směrnice Evropského parlamentu a Rady 2001/84/ES ze dne 27. 9. 2001 o právu na opětný prodej ve prospěch autora originálu uměleckého díla [Evropská unie, 2001b].
- Směrnice Evropského parlamentu a Rady. 2004/48/ES ze dne 29. 4. 2004 o vymáhání práv duševního vlastnictví [Evropská unie, 2004].

Dále pak směrnice související se směrnicemi upravujícími autorskoprávní problematiku, a to zejména:

- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu (Směrnice o elektronickém obchodu).
- Směrnice Evropského parlamentu a Rady 98/94/ES ze dne 20. 11. 1998 o právní ochraně služeb založených na podmíněném přístupu nebo na něm spočívajících.
- Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. 12. 1999 o zásadách Společenství pro elektronické podpisy.

Směrnice Rady 91/250/EHS ze dne 14. 5. 1991 o právní ochraně počítačových programů definuje předmět ochrany v článku 1 a vymezuje omezení pro manipulaci s programy ve článku 4 a výjimky k tomuto omezení v článku 5:

Článek 1

Předmět ochrany

1. V souladu s ustanoveními této směrnice chrání členské státy počítačové programy autorskými právy stejně jako literární díla ve smyslu Bernské úmluvy o ochraně literárních a uměleckých děl. Pro účely této směrnice se „počítačovým programem“ rozumí i přípravný koncepční materiál.

2. Ochrana podle této směrnice se vztahuje na vyjádření počítačového programu v jakékoliv formě. Myšlenky a zásady, na kterých je založen kterýkoliv z prvků počítačového programu, včetně myšlenek a zásad, na kterých je založeno jeho rozhraní, nejsou chráněny autorským právem podle této směrnice.

3. Počítačový program je chráněn, pokud je původní, v tom smyslu, že je vlastním duševním výtvorem autora. Pro stanovení způsobilosti k ochraně není uplatňováno žádné jiné kritérium.

Článek 4

Úkony podléhající omezení

S výhradou ustanovení článků 5 a 6, zahrnují výlučná práva nositele práv ve smyslu článku 2 právo činit sám a právo udělovat svolení jinému k

- stálému nebo dočasnému rozmnožování počítačového programu jako celku nebo jeho části, a to jakýmikoliv prostředky a v jakékoliv formě. Pokud je takové rozmnožování nezbytné pro zavedení,
- zobrazení, provoz, přenos nebo ukládání počítačového programu do paměti, vyžadují tyto rozmnožovací úkony svolení nositele práva

- překladům, zpracování, úpravám a k jakékoliv jiné změně počítačového programu a k rozmnožování programu z těchto úkonů vyplývajícímu, aniž jsou dotčena práva osoby provádějící změnu programu
- jakékoliv formě veřejného šíření, včetně pronájmu, jehož předmětem je původní počítačový program nebo jeho rozmnoženiny. První prodej rozmnoženiny počítačového programu ve Společenství provedený nositelem práv nebo s jeho svolením je vyčerpáním práva na šíření této rozmnoženiny v rámci Společenství s výjimkou práva na kontrolu dalšího pronájmu počítačového programu nebo jeho rozmnoženin.

Článek 5

Výjimky z úkonů podléhajících omezení

1. Pokud nejsou ve smlouvě sjednána zvláštní ustanovení, nevyžadují svolení nositele práv úkony uvedené v čl. 4 písm. a) a b), pokud se jedná o úkony nezbytné k tomu, aby umožnily oprávněnému nabyvateli užívat počítačový program způsobem, ke kterému je určen, včetně opravy chyb.

2. Oprávněnému uživateli počítačového programu nemůže být smluvně bráněno, aby z něho pořizoval záložní rozmnoženinu, pokud je nezbytná pro užívání programu [Evropská unie, 1991].

Jednotlivé směrnice Evropského parlamentu a Rady jsou postupně implementovány do zákonů členských států Evropské unie, tato implementace však neprobíhá ve stejném tempu ani ve stejném rozsahu a právní předpisy týkající se duševního vlastnictví zůstávají v jednotlivých zemích nejednotné.

5.3 Problematika autorského práva v ČR

V České republice se pojem duševní vlastnictví začal používat po roce 1990, a to nejprve v oblasti průmyslových práv. Do té doby byl jednotně používán pro předměty duševního vlastnictví pojem nehmotné statky.

Softwarové pirátství je porušováním autorských práv k softwaru, která jsou podle českého právního řádu chráněna především Zákonem č. 121/2000 Sb. ze dne 7. dubna 2000, částka 106/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorským zákonem).

V rámci šetření policie mnohdy dochází k prošetřování podezření z jiných druhů trestné činnosti, přičemž vyjdou zároveň najevo i poznatky, jež vedou k odhalení tzv. softwarové kriminality.

Autorský zákon upravuje:

a) práva autora k jeho dílu,

b) práva související s právem autorským:

1. práva výkonného umělce k jeho uměleckému výkonu,

2. právo výrobce zvukového záznamu k jeho záznamu,

3. právo výrobce zvukově obrazového záznamu k jeho záznamu,

4. právo rozhlasového nebo televizního vysílatele k jeho původnímu vysílání,

5. právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,

6. právo nakladatele na odměnu v souvislosti se zhotovením rozmnoženiny jím vydaného díla pro osobní potřebu,

c) právo pořizovatele k jím pořízené databázi,

d) ochranu práv podle tohoto zákona,

e) kolektivní správu práv autorských a práv souvisejících s právem autorským.

Předmětem autorského práva je podle § 2 autorského zákona

(1) dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen „dílo“). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické.

(2) Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Za dílo souborné se považuje databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem.

(3) Právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav, pokud splňují podmínky podle odstavce 1 nebo podle odstavce 2, jde-li o předměty práva autorského v něm uvedené [Česko, 2000].

Dalším českým zákonem, který je možno používat k postihování softwarového pirátství je Zákon č. 140/1961 Sb. ze dne 29.11.1961 (trestní zákon). Konkrétně se jedná o následující paragrafy zákona:

§ 150 - Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu

1. Kdo doveze, vyveze nebo uvede do oběhu výrobky nebo služby neoprávněně označované ochrannou známkou, k níž přísluší výhradní právo jinému, nebo známkou snadno s ní zaměnitelnou, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci.

2. Stejně bude potrestán, kdo pro dosažení hospodářského prospěchu

a) neoprávněně užívá obchodní jméno nebo jakékoliv označení s ním zaměnitelné, nebo

b) uvede do oběhu výrobky neoprávněně opatřené označením původu, k němuž přísluší výhradní právo jinému, nebo označením původu snadno s ním zaměnitelným.

§ 151 - Porušování průmyslových práv

Kdo neoprávněně zasáhne do práv k chráněnému vynálezu, průmyslovému vzoru, užitnému vzoru nebo topografii polovodičového výrobku, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

§ 152 - Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi

1. Kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci.
2. Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem nebo propadnutím věci bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 značný prospěch, nebo

b) dopustí-li se takového činu ve značném rozsah propadnutím věci [Česko, 1961].

Shrneme-li možné právní následky porušování těchto zákonů v České republice, můžeme konstatovat, že to mohou být:

- peněžité tresty,

- tresty propadnutí věci,
- tresty odnětí svobody až na 5 let,
- sankce finančních úřadů.

Odpovědnost za porušení autorského práva je ve smyslu trestních předpisů odpovědný ten, kdo úmyslným jednáním porušil autorské právo. Tento trestný čin může spáchat sám či spolu s jinými osobami ve spolupachatelství, popřípadě se může na trestném činu podílet jako účastník trestného činu, tedy jako ten, kdo spáchání trestného činu zosnoval nebo řídil, navedl jiného ke spáchání trestného činu nebo poskytl jinému pomoc při spáchání trestného činu.

Autorské právo je založeno na zásadě teritoriality.[30] Zároveň platí, že otázka aplikovatelnosti autorského zákona jako celku se řeší pomocí norem mezinárodního práva soukromého (konkrétně Bernské úmluvy na ochranu literárních a uměleckých děl). Zásada teritoriality uvedená v této úmluvě říká, že ochrana autorských práv se řídí právní úpravou státu, kde se ochrana uplatňuje, tedy toho státu, kde ke (zne)užití díla došlo (lex loci protectionis). Tento princip je vyjádřen na několika místech Bernské úmluvy, například v článku 5 odst. 2, článku 6 odst. 3 a v dalších [Bernská úmluva, 1886].

Z uvedeného vyplývá, že se český autorský zákon aplikuje i na práva zahraničních autorů, jestliže se jejich díla[31] stávají předmětem (zne)užití na území ČR. V případě (zne)užití českého softwaru v zahraničí je nutné postupovat podle autorského práva v konkrétním státě [ČERMÁK, 2001].

Autorský zákon poprvé akceptuje řadu moderních technologií. Rozšiřuje právní ochranu i na databáze jako dílo souborné a významným způsobem mění právní úpravu pro počítačové

[30] Právní zásada, podle které se k posuzování právních skutečností užívá právní řád příslušného území.

[31] V souvislosti s tématem diplomové práce jde o software.

programy, které jsou v rámci kategorie děl jmenovitě uvedeny a mají v mnoha ohledech svůj specifický režim. Zákon pamatuje i na internet či jinou podobnou síť a na možnost uveřejňovat dílo autorem prostřednictvím takové sítě. Zpřístupnění díla na internetu – upload[32] je řešeno dle §18 autorského zákona (sdělování díla veřejnosti), stahování díla koncovým uživatelem - download je řešeno dle § 13 autorského zákona (rozmnožování díla). Ochrana majetkových autorských práv platí po dobu života autora a z 50ti let byla rozšířena na 70 let po smrti autora. Nadále platí, že se autor nemůže vzdát svého autorství resp. osobnostních práv k dílu. Tato problematika je řešena v § 26, podle které autor nemůže majetkové právo jako celek nebo jednotlivá majetková oprávnění převést (zcizit); nemůže se jich ani vzdát a tato práva nelze postihnout výkonem rozhodnutí, ani se neoceňují.

Velmi podrobně byla zpracována otázka bezúplatné zákonné licence, tedy případů kdy k užití díla není zapotřebí souhlas autora. Obecnou zásadu výjimky z výlučného práva autorského obsahuje jak Bernská úmluva, tak Dohoda TRIPS (**Agreement on Trade-Related Aspects of Intellectual Property Rights)** a v českém autorském právu ji upravuje ustanovení v § 29 Autorského zákona. Jde o výkladové pravidlo ve vztahu ke všem způsobům volného užití chráněných děl a užití těchto děl, ke kterým není třeba souhlasu autora ani zaplacení odměny [*Důvodová zpráva, 1999*].

Volně šiřitelné programy tvoří důležitou část problematiky autorského práva a je třeba si uvědomit, že volně šiřitelné programy nejsou vždy volně použitelné:

- **shareware** (po určité době užívání programu je nutné autorům/producentům zaplatit; ve srovnání s komerčním softwarem jsou většinou poměrně levné; programy je možné kopírovat; není možné je bez svolení autora/producenta měnit; programy často bývají časově omezeny a/nebo funkčně limitovány; po zaplacení je fungování

[32] Upload - nahrávání souborů na FTP servery či servery typu RapidShare. (Zde za účelem jejich zveřejnění.)

programu obnoveno) – používání po autory/producenty stanovené lhůtě, za jiných podmínek a samozřejmě zásahy do programu jsou v rozporu s autorským právem

- **freeware** (programy je možné šířit, kopírovat a instalovat na jakémkoliv počítači; často jde o části komerčních balíků, demoverze apod.; do programů není většinou dovoleno zasahovat)
- **public domain** (autoři se formálně vzdali autorských práv; převážně to jsou zdrojové soubory programů nebo části algoritmů často umístěné na vývojářských serverech; programy je možné běžně upravovat a šířit)
- **trialware** (zkušební verze komerčních programů; doba fungování zkoušeních programů je omezena; volné šíření není možné; pro hromadné šíření je nutný souhlas autora/producenta; po zaplacení získává uživatel plnohodnotný produkt)
- **lite verze a demoverze** (běžně nejsou časově omezeny; někdy jsou volně šiřitelné, někdy účel přesně vymezen, někdy nutný minimální poplatek)[KREJČÍ, 2000].

Právní aspekty problematiky softwarového pirátství je nutné považovat za velmi důležité. Aktuální postihnutí současného stavu není jednoduché, protože problematika se neustále vyvíjí. V rámci mezinárodních organizací dochází průběžně ke vzniku a aktualizaci mezinárodních dohod, které se touto problematikou zabývají. Návazně jsou v jednotlivých zemích aktualizovány dotčené zákony. Je však nutné připomenout, že zatímco řada států definuje a stíhá softwarové pirátství jako trestný čin, existují stále státy, které některé nakládání se softwarem pokládají za legální. V zákonodárství několika dalších zemí dokonce problematika softwarového práva není dosud řešena vůbec [SCAMBREY, 2001]. Zároveň je třeba samozřejmě zmínit fakt, že samotné přijetí dohod a zákonů pro zlepšení právního povědomí v této oblasti nestačí.

6. Metody softwarového pirátství

Proces softwarového pirátství můžeme obecně rozdělit do několika fází. Jde prakticky o proces získání dat či softwaru, jeho přípravu na šíření a následné nezákonné šíření. V každé fázi tohoto procesu jsou použity specializované metody vedoucí k překonání všech bariér a ochran. Vzhledem k velmi rychlému vývoji na poli ochrany softwaru a nástrojů na její překonání konkrétní metody a software velmi rychle zastarávají a stávají se nepoužívanými. Tento proces velmi rychlého zastarávání informací o softwaru, nástrojích a metodách je také zapříčiněn velmi rychlým vývojem nových programů a verzí programů stávajících. Na každou z těchto změn je potřeba reagovat zcela novým zkoumáním a hledáním prostředků na jeho získání.

Ve zkratce můžeme proces vzniku nelegálního softwaru typu „warez“ popsat takto:

1. Je vydána nějaká očekávaná verze komerčního softwaru.
2. Warezová skupina využije svých kontaktů k tomu, aby získala kopii ještě před vydáním (nebo odcizí CD z továrny, kde se vyrábí).
3. Software je předán zkušenému programátorovi (crackerovi), který ze softwaru odstraní ochranu proti kopírování.
4. Takto upravený software je předán tzv. kurýrovi, který ho rozšíří na mnoho FTP serverů či serverů P2P.

6.1 Metody sloužící k získání originálních dat a programů

Pro pořízení kopií legálních dat či warezu potřebují softwaroví piráti v první řadě získat originální vzor, ze kterého pak za pomoci sofistikovaných metod získávají a šíří kopie. V této první fázi je nejdůležitějším faktorem úspěšnosti pirátů rychlost, s jakou se k zdrojovým datům dostanou.

V dnešní době se setkáme se stavem, kdy producenti softwaru, knižní nakladatelé či distributorské společnosti musejí vynakládat obrovské prostředky na ochranu svých produktů, ještě než se dostanou do oficiálního prodeje. Stalo se pravidlem, že software je k dispozici hackerům a pirátům několik týdnů před datem svého oficiálního prodeje (Dnem 0)[33]. Tomuto faktu napomáhá nejen zvyk zveřejňovat beta verze a testovací verze softwaru pro odbornou veřejnost, které slouží k získání zpětné vazby od budoucích uživatelů, a tedy k urychlení a zlevnění vývoje programu. Toto zveřejňování, ale zároveň umožňuje hledat bezpečnostní chyby v zdrojovém kódu programů a předběžné přípravě nástrojů a metod na uveřejnění. Druhou a značně nebezpečnější formou jsou úniky hotových produktů při závěrečné fázi výrobního procesu nebo ještě před ní [McGUIRE, 2001, s. 20]. Důvodem je velká poptávka po produktu a leckdy

i oddalování data vydání samotnými producenty. Příkladem mohou být úniky filmů v té nejlepší možné DVD kvalitě ještě před oficiální produkcí v USA, kde zdrojem těchto kopií byli porotci hodnotící filmovou produkci navrženou na cenu Akademie filmového umění a věd USA - Oscar[34].

[33] Den prodeje je hackerskou komunirou označován jako den 0. Od tohoto dne se pak odpočítává, za jak dlouho bude prolomena ochrana tohoto softwaru. Na BBS jsoupravidelně popsány postupy použité pro překonání a doba (počet dní), za kterou k němu došlo.

[34] The Academy of Motion Picture Arts and Sciences.

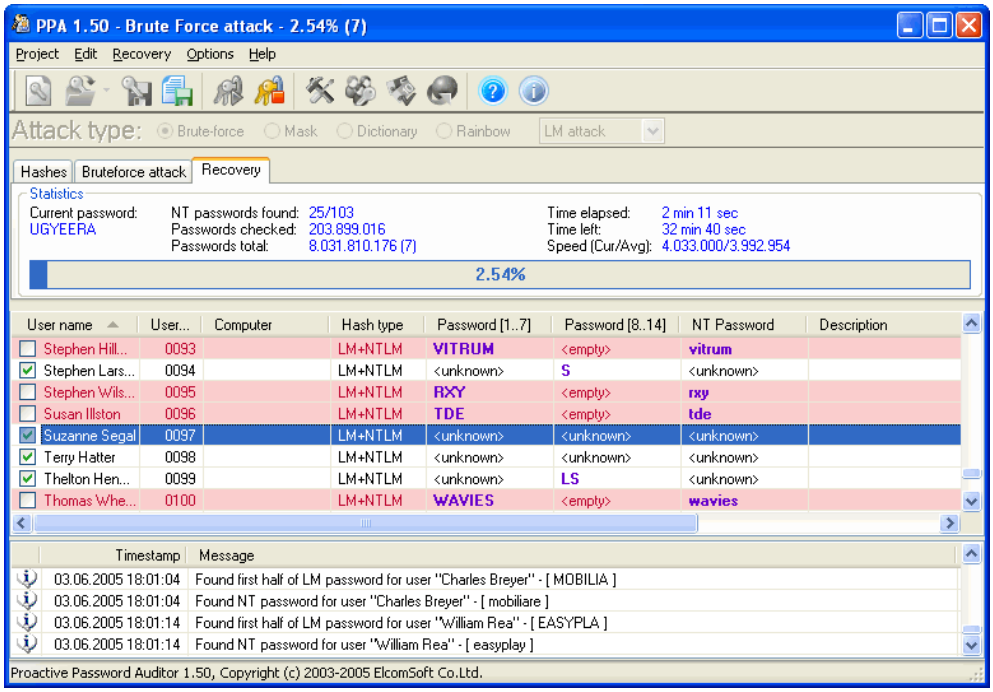
Metody jsou velmi rozličné, od sociálního inženýrství, hackerkých útoků, obyčejných krádeží v obchodech, jako v případě obchodu s hudebními nosiči a video nahrávkami v Seattlu, který byl vykraden zloději, kteří způsobili škodu za asi 7 000 USD (cca 145 000 Kč). Zajímavostí však zůstává to, že zloději podle serveru Dvddossier.com zcizili filmy ve formátu Blu-Ray Disc, zatímco HD DVD kvůli jeho kvalitnější ochraně neukradli *[Blu-Ray Disc vede…]*. Velmi často je warezovými skupinami CD ukradeno přímo z výrobní továrny. A stále zůstává jedna metoda, kterou může jakýkoliv softwarový pirát produkt získat – může ho legálně koupit v obchodě.

6.2 Metody překonání antipirátských ochran

Po získání originálního softwaru či původních dat (ať již se jedná o video, audio nebo textové soubory) nastává fáze přípravy těchto dat pro masovou distribuci nebo pouze pro lokální používání. Pro oba typy užívání je nejprve nutné odstranit či překonat **všechny** ochrany použité distributorem softwaru či média, na kterém je software uložen. Tento krok velmi často dělá softwarový pirát **cracker**, který se na tuto činnost specializuje. Prostředky crackerů pro překonávání ochran přímo implementovaných do nosičů dat (CD, DVD, HD DVD) se velice často stávají upravené softwarové nástroje dodávané samotnými tvůrci softwaru, či vydavateli mediálních dat. Příkladem může být prolomení ochrany DVD-Audio za pomoci přehrávače InterVideo WinDVD. Ten lze ve verzích 5, 6 a 7 využít k uložení disku DVD-Audio do souborů WAV. Utilita DVD-A Ripper dokáže prolomit ochranu CPPM souborů AOB i VOB, k čemuž využívá dekodéry DVD-Audio a MLP v InterVideo WinDVD, pomocí nichž získává přístup k nechráněným tokům Packet PCM dat, jež pak utilita PPCM Ripper ukládá do souborů WAV. DVD-A Explorer pak umí procházet strukturou stop na disku [ROBINSON, 2005]. Za pomoci této utility a standardní funkce dodávaného přehrávače byla softwarovými piráty v roce 2005 během pár dní překonána ochrana jejíž vývoj a nasazení

stálo mnoho miliónů dolarů. Při zkoumání metody překonávání ochrany disku DVD-Audio docházíme k závěru, že z použitých tří softwarových nástrojů byl pouze jeden vytvářen přímo jako pirátský, zbylé dva jsou standardní prohlížeč a přehrávač.

Další fází ochrany softwaru bývá standardně ochrana za pomoci **instalačního** či **aktivačního** kódu. První z nich je po uživateli vyžadován již v Průvodci instalací (Instalation Wizard), bez správného zadání tohoto kódu instalace neproběhne. Postupy crackerů jsou zde dvojí, první možností je překonání kódu „hrubou silou“ (**brutal force attack**), při této metodě se využívají programy typu Passwordcracker, které se snaží na základě matematických algoritmů a integrovaných slovníků kód získat, viz obr. číslo 4.



Obrázek č. 4 - ukázka programu PPA 1.50 při luštění osobních hesel.
Zdroj: [http://www.s2services.com/miscpasswordfreeware.htm].

Protože však výrobci softwaru používají v poslední době kódy dostatečné délky, jejich prolomení touto metodou není časově výhodné. Častěji využívaným prostředkem jsou tzv. **generátory klíčů (Key Geny)** založené na zjištěných algoritmech vytváření klíče samotnou

ochranou. Tyto nástroje po spuštění vygenerují kód stejně jako software provozovaný dodavatelem, jsou napsány zkušenými crackery a uveřejněny na internetu.

Další možností získání instalačního kódu je internet samotný. Na webových serverech undergroundového charakteru (jako kupříkladu www.astalavista.com, známá hackerská alternativa serveru www.altavista.com) se nacházejí celé databáze **seriálových čísel (Serial Numbers)** a klíčů **(CD - Key)**[35], kde po zadání názvu požadovaného softwaru uživatel získá funkční klíč.

Uživatelsky nejsnazší, a proto nejčastější metodou vytvoření warezové verze legálního programu je přeprogramování spouštěcího souboru, aby již žádnou ochranu nepotřeboval a vytvoření tzv. „**Cracku**“. Důležitost warezových skupin v dnešní době již ani tak nezáleží na distribuci nelegálního softwaru, ale právě na vzniku warezové obdoby originálního softwaru, tzv. **„Rippu"**[36].

6.3 Metody distribuce nelegálního softwaru a dat

Warezové verze komerčního softwaru jsou typicky vydávány ve dvou podobách: v plné a tzv. ořezané (Ripp). V případě počítačových her v ripp-verzi obvykle chybí vložené videosekvence, některé části jsou také někdy před distribucí zkomprimovány (např. do MP3) a uživatelé je musejí před použitím dekomprimovat. Plné verze se obvykle šíří jako obrazy CD či DVD disků (tzv. soubory BIN, ISO, CCD či MDF).

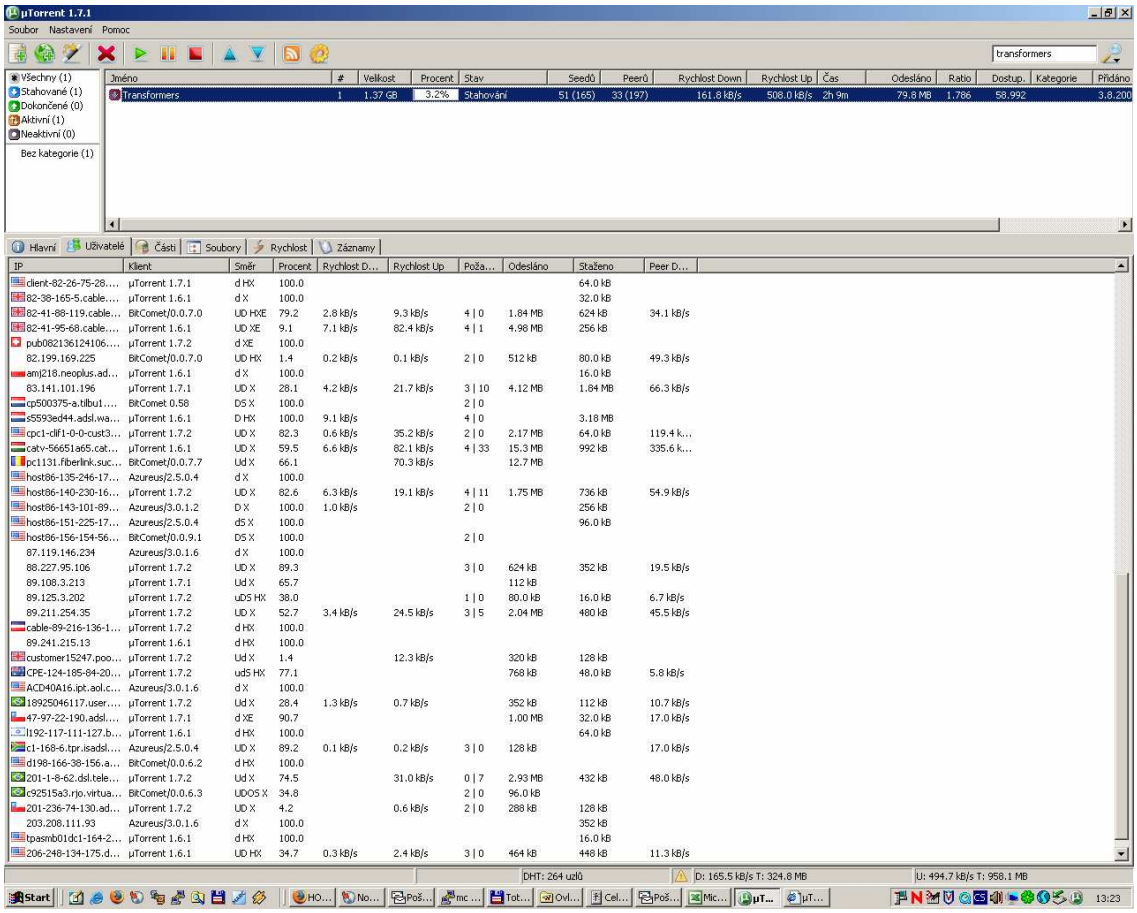
Velká část warezu je distribuována tak, že ***„uploader“*** (ten, kdo soubory poskytuje ostatním) odešle soubory s tímto obsahem na nějaký server poskytující úložné místo pro data, v současnosti mezi nejoblíbenější patří **RapidShare**. Kvůli tomu, že tyto servery mají

[35] Příkladem může být databáze http://www.serials.ws/, jde o profesionálně tvořené informační databáze s kvalitními vyhledávacími stroji (Search Engines) a mnoha možnostmi zpřesnění dotazu.
[36] Jak již bylo uvedeno, ripp je kopie původního softwaru či audiovizuálního souboru, bez příloh jako jsou: PDF nápovědy, protipirátské ochrany, a další.

omezení na velikost jednoho souboru, se soubory většinou rozdělí pomocí komprimačních programů jako WinRAR na menší části a celý RAR soubor se zahesluje (aby se správci nemohli podívat, co v souboru je a nesmazali ho). Tato forma distribuce je zvlášť oblíbená na tzv. **warez fórech**.

Ještě rozšířenější formou šíření warezu a nelegálních kopií filmů a hudby jsou **P2P** (**peer –to –peer**) výměnné sítě. Dnes se označení P2P vztahuje hlavně na výměnné sítě, prostřednictvím kterých si mnoho uživatelů může vyměňovat data. Příkladem takových sítí jsou např. Gnutella či původní verze Napsteru.

Jednou ze základních výhod sítí P2P je fakt, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste, zatímco u modelu client-server se musí uživatelé dělit o konstantní kapacitu serveru, takže při nárůstu uživatelů klesá průměrná přenosová rychlost.



Obrázek č. 5 - Ukázka stahování jednoho nelegálního .avi souboru za pomoci programu Bittorrent.
Zdroj: Neznámý.

Vývoj programů na sdílení není poháněn pouze snahou o vylepšení technologie a zjednodušení práce, ale také snahou nalézt systémové řešení, které by bylo jen obtížně napadnutelné právní cestou. V tom se liší případ Napsteru a ten současný se společností Grokster a Streamcast Networks. Tentýž soud dospěl k úplně opačným rozhodnutím. Odpověď je nutné hledat v technologické podstatě posuzovaných sítí. Zatímco Napster byl tvořen centrální databází odkazů na jednotlivé soubory, většina současných sítí P2P (kupříkladu Morphea či FastTrack) poskytuje jen nástroj k výměně informací, které jsou uloženy v počítačích jednotlivých uživatelů. Tento rozdíl (**služba versus nástroj**) je také zásadním činitelem, který ovlivňuje verdikty soudů. Při žalobách proti sítím Morphea či

FastTrack trojice soudců zdůraznila, že žalované firmy poskytují jen prostředek ke sdílení informací, nad nimiž však už nemohou mít žádnou kontrolu. Toto je překlad stanoviska Sidneye R. Thomase, jednoho ze soudců v usnesení soudu: *„Samotná technologie může být použita k řadě účelů, významně snižuje distribuční náklady volně šiřitelného softwaru a uměleckých děl, stejně jako umožňuje centralizovanou kontrolu této distribuce…“* [MIKLÍK, 2004].

6.4 Sebeochranné metody (Self-defense metods)

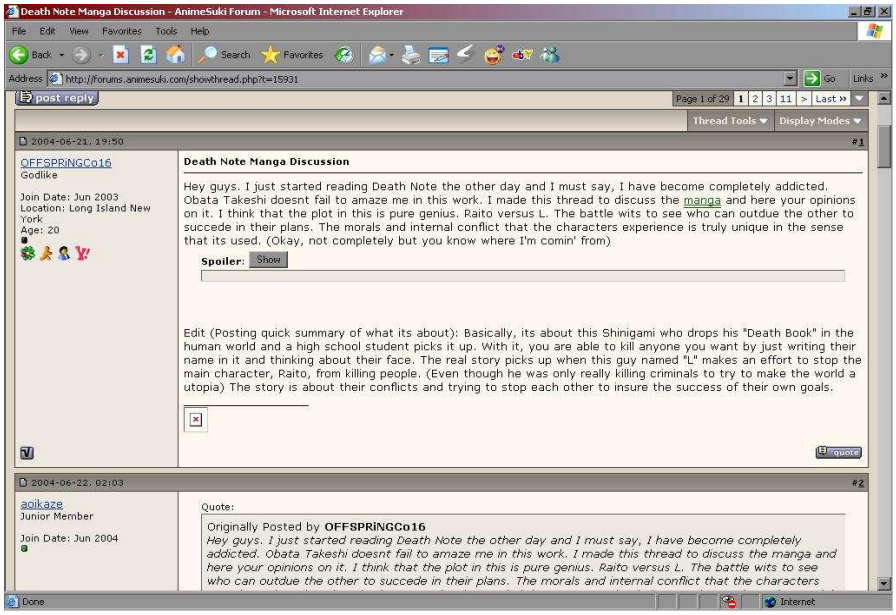
Jednou z nejdůležitějších předpokladů života softwarových pirátů je nutnost anonymity. V okamžiku, kdy softwarové firmy a organizace problematikou se zabývající zjistí pomocí pátracích prostředků či nátlaku na poskytovatele (Providery) adresu IP softwarového piráta, který získává, či distribuuje software za pomoci internetu, mohu ho sledovat a identifikovat. Programy typu PeerGuardian a PeerGuardian 2 slouží k zabezpečení anonymity softwarových pirátů. Jde o volně přístupné programy (OpenSource) na blokování příchozích a odchozích spojení ze a na zadané IP adresy. Používají se na blokování „špehování“ organizacemi jako jsou např. BSA, RIAA nebo MPAA. Programy fungují, jak již bylo zmíněno, na principu přímé blokace IP adres. V jejich databázi IP adres se nachází několik stovek milionů adres, které program blokuje. Pokud je tedy inkriminovaná adresa v seznamu, bude jednoduše zablokována a zapsána do historie připojení. Posléze se můžete kdykoli podívat, kdy a kdo se pokoušel připojit. Seznamy z těchto programů lze bez jakýchkoli obtíží zkopírovat do jiných programů, jako je například firewall a jiné blokovací programy [ŠEBÍK, 2007].

6.5 Ostatní metody a postupy

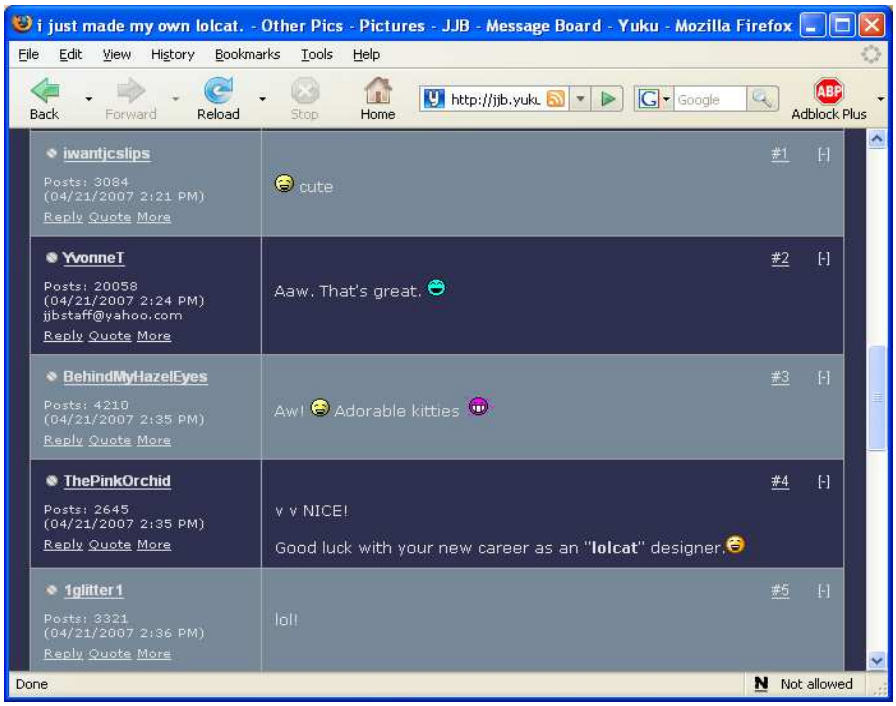
Do softwaru a prostředků, které piráti využívají ke své činnosti, bývají často zahrnovány (převážně vyšetřujícími orgány) také virtuální diskusní servery, internetová fóra, chaty a další místa kyberprostoru, která slouží k seznamování lidí, vyměňování informací, znalostí a vytváření sociálních skupin a vazeb. Předchůdci dnešních systémů byly takzvané **nástěnkové systémy (Bulletin Board Systems - BBS)**, které vznikaly od 70. let 20. století na prvních sálových a osobních počítačích. Tyto počítače byly uživateli kontaktovány pomocí modemů, telnetu a telefonů. Rychle se rozšířily a v roce 1985 bylo v USA kolem 4 000 těchto boardů, v roce 1990 již kolem 30 000 [CHRISTIANSEN, 1992]. Tato „místa“ se stala jedinými viditelnými spojeními softwarových pirátů a hackerů.

Od prvních okamžiků byla tato komunikační místa používána nejen k výměně citlivých informací a návodů, hackerských a pirátských postupů atd., ale sloužila také k přímému stahování nelegálního softwaru, výměně ukradených osobních dat, jako jsou třeba čísla kreditních karet a hesel, rootovských[37] a přístupových hesel k napadeným serverům a dalších. K této nelegální činnosti docházelo a dochází pouze na minimálním množství serverů. Většina jich slouží pouze k výměně technických informací a setkávání lidí. V dnešní době se BBS systémy postupně vyvinuly ve **webové diskusní servery (Communits Servers),** např. české servery Nyx (http://www.nyx.cz), Cyberspace (http://www.cyberspace.cz), Hofyland (http://www.hofyland.cz), slovenské Kyberia (www.kyberia.sk) a Hysteria (www.hysteria.sk) a světové Yuku (http://jjb.yuku.com), Yahoo Groups (http://groups.yahoo.com /) a další. Tato místa byla vždy nejsnazšími cíli v represivním postupu proti softwarovým pirátům a hackerům.

[37] Pojem rootovský je v tomto případě přebírán z linuxového prostředí, kde root je označení pro administrátorskou úroveň přístupu.



Obrázek č. 6 - Příklad vzhledu webových diskusních serverů
Zdroj: [http://en.wikipedia.org/wiki/Internet_forum].



Obrázek č. 7 – Příklad vzhledu webových diskusních serverů.
Zdroj: [http://en.wikipedia.org/wiki/Internet_forum].

Často dochází k úřednímu zabavení serverů, na kterých jsou komunikační systémy provozovány. Toto nastalo jak v roce 1990 v případu Sundevil, tak v době nedávné na Slovensku v případě serverů Kyberia (www.kyberia.sk) a Hysteria (www.hysteria.sk). Cílem této diplomové práce není hodnotit oprávněnost těchto kroků, ale pravdou zůstává, že diskusní skupiny, internetová fóra a další podobné nástroje jsou mediálním fenoménem, který slouží ke komunikaci a umožňuje šíření informací a znalostí zcela nezastupitelnými metodami [INTERNET forum, 2007].

7. Zhodnocení nákladů na ochranu dat a ceny výsledného softwaru

Zatímco v roce 1986 udávaly softwarové společnosti ve Spojených státech amerických ztrátu ve velikosti jedné miliardy dolarů jako důsledek nelegálního kopírování softwaru obecně připisovanému softwarovým pirátům, v roce 1991 to již byly tři miliardy dolarů za rok a v Evropě dokonce 5,3 miliard dolarů [BULKLEY, 1990], [GLEN, 1991], [RICE, 1991]. Jelikož šlo o období, kdy nebyly postupy softwarových společností pro sledování údajů o pirátství plně vyvinuty, musíme brát tyto údaje s jistou rezervou [CHRISTENSEN, 1991].

V roce 1997 se podle **Massachusettské softwarové rady (Massachusetts Software Council)** softwarový průmysl podílel na celkovém průmyslu ve státě Massachusetts v USA asi 9,2 miliardami dolarů. Softwarové pirátství však podle průmyslové studie společnosti **Microsoft** z roku 1998 připravilo stát Massachusetts v roce 1997 o více než 4 300 pracovních míst a alespoň o 850 milionů dolarů na platech, daních a maloobchodním prodeji. Microsoft uvedl, že 25 procentní podíl pirátského softwaru tak Massachusetts stál 240 milionů dolarů na platech, 600 milionů dolarů na maloobchodním prodeji a 11 milionů dolarů na daních. Orlando Ayala, jeden z předních představitelů **Microsoftu**, prohlásil, že tato čísla nezvratně dokazují, že softwarové pirátství není bez obětí. [*Software Piracy* ...]

Statistiky BSA dokazují, že důsledky softwarového pirátství rostou, ale stoupá také částka vynakládaná každým rokem na ochranu softwaru proti němu a náklady spojené s ochranou produktu tvoří podstatnou část jeho výsledné ceny [HUNLEY, 2002]. Pokud se podrobněji zabýváme složením této částky, jde nejen o výpočet ztrát z potenciálně prodaného softwaru, ale jsou zde započítány i náklady na zabezpečení nově vyvíjeného softwaru, na bezpečnostní postupy i analýzy bezpečnosti vytvořené s ohledem na možnost poškození

softwarovými piráty. Často sem je zahrnuta také cena důsledků způsobených negativní publicitou. Všechny společnosti informačního průmyslu investují velké množství času a peněz do sběru dat a shromažďování, třídění a publikování informací [CHRISTENSEN,1991].

Používání nelegálně získaného softwaru vlastními zaměstnanci společností může vyvolat vážné problémy a způsobit porušení integrity těchto dat. Příkladem jsou počítačové viry, se kterými jsou často nelegální programy propojeny. Na boj s tímto problémem mnoho společností a univerzit aktuálně vyvíjí a implementuje metody, které slouží k boji s nelegálním kopírováním softwaru zaměstnanci a studenty [EVELOFF, 1990].

Investice softwarových společností, které jsou vynakládány na boj se softwarovým pirátstvím, můžeme rozčlenit do několika kategorií podle zaměření dané ochrany. Výčet jistě nebude úplný, ale hlavní oblasti vynakládání prostředků jsou tyto: náklady na analýzu a propagaci problematiky, náklady na podporu represe a vymáhání autorského práva a náklady na zabezpečení produktů a postupů. Podrobněji budou náklady popsány dále.

7.1 Náklady na analýzu a propagaci problematiky

Od konce devadesátých let, kdy si komerční firmy a státní instituce začaly uvědomovat nárůst nákladů na boj se softwarovým pirátstvím, které se v té době již nedaly pominout, začaly analyzovat úspěšnost svých investic. Dospěly k poznatku, že pouze dokonalá znalost problematiky softwarového pirátství, vlastních postupů a nejnovějších trendů a technologií může vést k efektivnímu investování prostředků [KŘÍŽ, 1999]. Výsledkem nebyla pouze zvýšená pozornost věnovaná odděleními vztahů s veřejností (Public Relations) této problematice ve firmách. Došlo také ke zvýšení podpory stávajících sdružení a organizací zaměřených na boj proti softwarovým pirátům a k zakládání nových. Dále došlo také k přesunu uvedené problematiky a propagační činnosti právě na organizace typu BSA. Zde díky

centralizovanému a systematickému zpracovávání dat mohou vznikat ucelené statistiky mapující tuto problematiku. Spojení zdrojů umožnilo mohutnější propagační kampaně, které kupříkladu BSA pořádá přibližně třikrát ročně (tato periodicita má být udržena i pro rok 2008) a jejichž dosah je dnes již prakticky celosvětový [BSA, osobní komunikace pomocí hotline, 2007].

7.2 Náklady na podporu represe a vymáhání autorského práva

Náklady vynakládané v této oblasti pokrývají nejen právní služby renomovaných firem, ale také lobbistické postupy a ovlivňování tvorby zákonů jednotlivých států. Při sledování vývoje v oblasti působení softwarových firem a organizací zřízených na ochranu autorského práva je patrný jistý rýsující se rozpor. Na jedné straně jsou vynakládány stále vyšší prostředky na soudní boj jak proti softwarovým pirátům [*Třetí výroční zpráva BSA,* 2007], tak proti jedincům a organizacím porušujícím autorské právo. Příkladem může být postup společnosti **Softwarová bezpečnost** (**Software Security - SWS)**, kdy za přispění SWS bylo za posledních pět let z důvodů porušování autorských práv a jiné trestné činnosti zavřeno v České republice přes 50 podniků z řad internetových kaváren a heren. Firmám byly zabaveny počítače a v řadě případů jim byly uloženy pokuty v řádech statisíců korun [*Kvůli pirátství,* 2007].

Dalším příkladem právního tlaku může být snaha amerického generálního prokurátora Alberta R. Gonzalese o prosazení návrhu zákona týkajícího se ochrany duševního vlastnictví (**Intellectual Property Protection Act of 2007**), který by postihoval již samotný pokus o porušení autorského zákona, ne až dokonaný čin. Tímto by byla, mimo jiné, **existence jakéhokoli softwaru na sdílení dat prakticky postavena mimo zákon, protože by jakékoliv použití takového softwaru, mohlo být chápáno jako pokus o porušování**

autorských práv [BANGEMAN, 2007]. Přijetí tohoto zákona by zásadně ovlivnilo problematiku softwarového pirátství.

V naprostém rozporu s touto sílící právně-represivní celosvětovou kampaní softwarových společností je prohlášení Billa Gatese, zakladatele společnosti Microsoft, která je jedním z zakladatelů BSA a doposud byla považována za jednoho z hlavních odpůrců softwarového pirátství. Přesný výrok zní: "Je snazší pro náš program soupeřit s Linuxem, když existuje softwarové pirátství, než kdyby neexistovalo" [KIRKPATRICK, 2007]. [38] Navazuje tak na prohlášení prezidenta divize obchodu společnosti Microsoft Jeffa Raikse proneseném na Morgan Stanley Technology konferenci v San Franciscu, které znělo: „Pokud budou uživatelé krást software, chtěli bychom to být my, komu bude kraden, než někdo jiný.“ Zároveň Raikes dodal, že Microsoft nehodlá potírání pirátství omezovat, jen jej hodlá udržet ve vyrovnané formě. Jak totiž dále řekl: „ pirátství je třeba potírat, ale ne moc, abyste neztratili jednu z největších výhod v obchodu, totiž to, že váš software už někdo používá, i když nelegálně, z takových uživatelů se časem mohou stát uživatelé legální“ [VAŠEK, 2007].

7.3 Náklady na zabezpečení produktů a postupů

Tato velmi důležitá oblast investic se velkou měrou podílí na výsledné ceně produktů distributorů softwaru. Ročně jsou vynakládány obrovské částky na výzkum nových šifrovacích algoritmů sloužících k zabezpečení produktů, nových technologií na ochranu softwaru i jeho nosičů před možným kopírováním a následnou nelegální distribucí. Na konkrétních příkladech jednotlivých technologií může dojít k lepšímu pochopení problematiky překotného technologického závodu, který je veden mezi techniky softwarových společností na straně jedné a hackery a softwarovými piráty na straně druhé.

[38] „It's easier for our software to compete with Linux when there's piracy than when there's not…“

Prvním příkladem může být snaha o zabezpečení všech cest, po kterých jsou data šířena, ať již jde o šifrování datových toků mezi zákazníkem a prodejcem při internetovém prodeji nebo o zabezpečení rádiového vysílání proti možnému nahrávání a kopírování za účelem komerčního využití přímo při přenosu [MURRAY, 2003, s. 10-15].

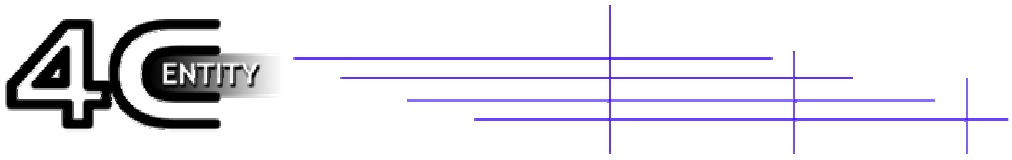
Tento zájem vedl nejen k objevu nových šifrovacích algoritmů, ale také k velkému rozvoji kryptologie jako vědní disciplíny. Za podpory vládních a soukromých organizací se rozvíjejí odvětví kryptografie, jakým je např. steganografie.

Toto „znovu objevené“ odvětví vychází z matematicky dokázaného faktu, že při sebelepším šifrovacím algoritmu může dojít k jeho prolomení a následnému rozluštění dokumentu. Navíc veškerá šifrovaná komunikace na internetu je zkoumána bezpečnostními institucemi jednotlivých států. Proto nyní steganografie zkoumá novou metodu, která umožňuje rozložení zasílaného textového dokumentu, obrazového či zvukového záznamu do jiného metodou počítačové substituce. Vychází z faktu, že každý dokument obsahuje množství redundantních informací a je tedy možné část z nich nahradit, aniž by došlo k změně původní podoby [JOHNSON, 2000, s. 17-30]. Steganografie je využívána např. při obchodním styku či při šíření uměleckých děl. Do zasílaných souborů jde vložit jednoznačný identifikační údaj - **vodoznak (watermark)** a tak zabránit nekontrolovatelnému šíření těchto děl.

Dalším příkladem může být snaha hudebních a filmových vydavatelství o vytvoření neproniknutelné ochrany nejen médií CD/DVD, které jsou dnes majoritními nosiči zvukových a obrazových informací, ale všech médií a informačních kanálů, jež slouží k distribuci mezi vydavateli/prodejci a zákazníky [DVD Copy Control Association, 2000]. K prvním výsledkům této snahy můžeme řadit pokus americké společnosti Fox Broadcasting o zavedení digitálního kódování do všech vysílání s cílem dosažení možnosti jeho přehrávání pouze na schválených počítačích či televizorech. Nikdo jiný než vybrané společnosti (Panasonic, Sony,

Intel, Toshiba a Hitachi) nemohl vyrobit přístroj, na kterém by mohlo být vysílání přijímáno. Celý projekt byl zaštítěn Americkou asociací filmového průmyslu **(Motion Picture Association of America - MPAA)**. Realizace tohoto projektu se však nezdařila. V roce 2005 odvolací soud zakázal Americké komisi pro kontrolu vysílání **(Federal Communications Commission - FCC)** uvedenou technologii využívat. Obrovské náklady společností vyšly tímto naprázdno [LEE, 2005].

V Evropě byla podobá metoda zavedena prostřednictvím projektu **Digital Video Broadcasting - DVB**, autorem projektu je stejnojmenné konsorcium 250 subjektů informačního průmyslu, jako jsou vývojáři softwaru, vysílací společností a regulační úřady. Vyvinutá technologie a metodika se nazývá Správa ochrany obsahu a pořizování kopií (**Content Protection and Copy Management -CPCM**), někdy také obecněji Ochrana obsahu nahrávatelných a předem nahraných médií **(Content Protection for Recordable Media and Pre-Recorded Media - CPRM/CPPM**) Technologie je vybudována na základě výsledků výzkumu a práce konsorcia **4C Entity.** Obrázek č. 8 uvádí logo společnosti 4C Entity, které je velmi často využívané jako vodoznak v oblasti licenčních smluv.



Obrázek č. 8 – Logo společnosti 4C Entity.
Zdroj: [http://www.pbs.org/newshour/media/digital_copyright/terms.html].

Toto konsorcium se skládá ze společností IBM, Intel, Machushita a Toshiba, jeho technologie Cryptomeria Cipher (také známé jako **C2**) se stala bezpečnostním standardem v oblasti managementu digitálních práv [CONTENT, 2007]. Technologie je založena na označení každého vysílání v Evropě vysílacím **CPCM kódem**, který bude načítat

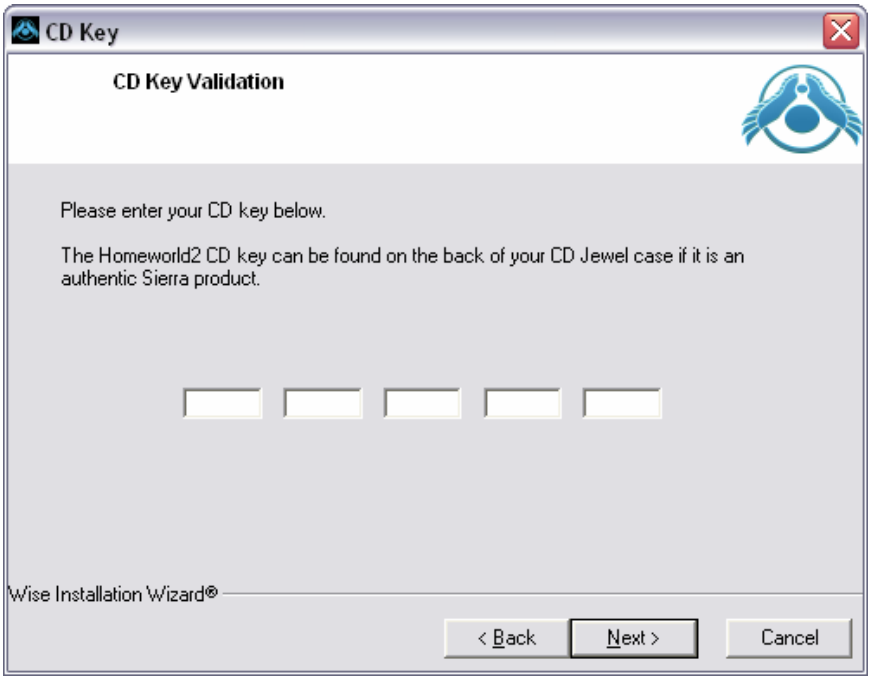
bezpečnostní čip v digitálním televizním přijímači. Technologie má umožňovat kontrolované kopírování, časově omezené licencování a vypalování na pevná média DVD [HIBBERT, 2002 s. 1-6]. Uvedená technologie však naráží na mnoho problémů ať již technologických (nutnost bezchybné komunikace přehrávače s televizorem[39]), nebo právních (stále existují státy, kde má každý právo na vytvoření kopie pro vlastní potřebu, tudíž jakékoliv omezování tohoto práva je v rozporu se zákonem[40]).

Pokud se vrátíme k přímé ochraně dat a softwaru na CD/DVD, lze konstatovat, že dnes hromadně nasazována dvoustupňová metoda. Prvním stupněm je **ochrana CD/DVD jako nosiče** a druhým stupněm je zabezpečení samotných programů pomocí **autentikačních prvků.** Dnes jsou v případě softwaru nejčastěji používané tzv. ***CD-klíčů (CD-Key´s*)**, a v případě mediálních dokumentů tzv. **blokátory médií (Media Key Block´s**). Do vývoje obou autentikačních metod investovaly a stále investují softwarové společnosti velké finanční prostředky i když jejich úspěšnost a trvanlivost je diskutabilní [ROBINSON, 2005]. Krátce po prvním nasazení dlouho vyvíjené ochrany DVD uveřejnil v roce 2002 Jon Lech Johansen na svých webových stránkách program DeCSS, který ji překonává. DVD Jon, jak se Johansenovi přezdívá, je jedním z nejznámějších „kyberzločinců". Za zveřejnění programu byl zažalován Americkou asociací pro kontrolu kopírování (**DVD-CCA**) a **Asociace nahrávacího průmyslu (Motion Picture Association - MPA)** [JOHANSEN, 2007]. J. L. Johansen se v současné době zaměřuje na jinou část informačního průmyslu a to na telefon iPhone, ke kterému na svém blogu „So Sue Me" (Tak mě zažaluj) uveřejnil aktivační nástroj. Jeho „záplata" umožňuje využít všech služeb telefonu, aniž by majitel musel podepisovat smlouvu s operátorem AT&T vlastnícím exkluzivní práva na prodej iPhone [*Apple iPhone* ...].

Druhý stupeň zabezpečení založený na **autentikaci softwaru** či média

[39] V okamžiku, kdy dojde k narušení vysílaného kódu, nedojde k jeho ověření a přehrání neproběhne.
[40] Mimo jiné i Česká republika, kde je právo na vytvoření záložní kopie dáno zákonem.

oproti databázi je asi nejčastěji využívanou metodou, kterou standardně používají všichni komerční výrobci. Náklady spojené s touto metodou se neodvíjejí pouze od nutnosti implementace stále novějších šifrovacích metod, ale také o udržování databáze existujících klíčů, od financování fungující telefonické podpory (help line) pro případ ztracení klíče a nutnosti sledování (nejčastěji za pomoci softwarových prostředků) warezových stránek, na kterých hackeři pravidelně publikují generátory klíčů (key-geny) [MOSQUERA, 1999, s. 76-77].



Obrázek č. 9 – Příklad typické ochrany softwaru při procesu instalace za pomoci CD-klíče. Zdroj:[http://en.wikipedia.org/wiki/Homeworld].

Nemalé částky jsou vynakládány také na základní fyzické zabezpečení produktů proti krádeži. Běžnou metodou softwarových pirátů je krádež programu, nového přehrávače či jen filmu nebo knihy, které ještě nebyly uvolněny pro distribuci na trh. Piráti pak mohou využít takto získaných produktů nejen k jejich prodeji za zvýšené ceny, ale také k jejich důkladnému zkoumání a překonání případných ochran, a to ještě před uvedením produktu na trh. Společnostem tímto vznikají velké ztráty [DENNING, 1998]. Částky vynaložené na uvedený

působ ochrany nebývají často publikovány, jednou z aktuálních výjimek v tomto pravidle je nakladatelství Bloomsbury, které přiznalo náklady na ochranu při výrobě a distribuci své knihy Harry Potter and the Deathly Hallows ve výši 12 miliónů eur [POHŮNEK, 2007].

S vývojem a zaváděním protipirátských ochran jsou spojeny nejenom finanční náklady, dopadem implementace ochrany bývá leckdy také zdržení při uvádění softwaru do produkce či také snížení uživatelské příjemnosti daného softwaru. Ochranné prvky musejí proto být velmi vyváženým kompromisem mezi bezpečností a **uživatelsky přívětivým (User Frendly)** přístupem [*User friendly*, 2007].

Příkladem může být zavedení protipirátských ochran do nové verze operačního systému Windows Vista. Windows Vista obsahují rozsáhlé změny hlavních součástí operačního systému, aby Windows mohly poskytovat ochranu obsahu pro tzv. „bonusový obsah“ - typicky jde o data ve **vysokém rozlišení (High Definition – HD)** ze zdrojů Blu-Ray nebo HD-DVD. Aby nebylo možné vytvářet hardwarové emulátory zařízení s chráněným výstupem vyžaduje Vista tzv. **„Snímání funkce hardwaru“ (Hardware Functionality Scan - HFS)**, které může být použito k jednoznačné identifikaci zařízení a k ověření, že zařízení je (pravděpodobně[41]) originální. Proto ovladač na počítači provede se zařízením nějakou operaci (např. vykreslení trojrozměrného obsahu pomocí grafické karty), jejíž výsledek je na daném zařízení unikátní. Dochází tak
k nutnosti „utajování“ zdrojového kódu a praktické likvidaci open-source programů. Navíc poskytování Vista ochrany má nezanedbatelný negativní dopad na výkon a stabilitu systému, režii technické podpory a cenu hardwaru a softwaru. Uvedené problémy se netýkají pouze uživatelů Vista, ale celého odvětví výpočetní techniky, protože tato ochranná opatření ovlivňují veškerý hardware a software, který kdy přijde s Vista do kontaktu, i když není přímo s Vista používán (například hardware v počítači Macintosh nebo v serveru Llinux).

[41] Po překonání této ochrany identifikuje jako originální i kopírované nosiče.

Tato opatření mohou způsobovat další, takzvané přidružené škody (Collateral Damane) v celém počítačovém průmyslu [GUTMANN, 2007].

8. Závěr

Tato diplomová práce se zabývá problematikou softwarového pirátství, příčinami vzniku, fázemi vývoje a důsledky jeho dopadu na informační průmysl a tak i na všechny běžné uživatele softwaru.

První dvě kapitoly práce se zaměřily na definici pojmů a vymezení historického rámce problematiky softwarového pirátství od jeho vzniku do současnosti. Další kapitoly se pokusily postihnout problematiku z několika úhlů pohledu a to jak z pohledu legislativy, pohledu informačního průmyslu i pohledu, který je v současnosti nejčastěji veřejnosti předkládán, a to pohledu národních a mezinárodní organizací specializujících se na ochranu duševního vlastnictví a na boj proti softwarovému pirátství. Indikátorem rostoucí důležitosti problematiky softwarového pirátství jsou i rostoucí náklady na boj proti němu, jak ukazuje kapitola sedmá. Nejdůležitější částí mé práce je kapitola šestá, ve které jsem se pokusil popsat metodologii procesu softwarového pirátství a nástroje, které v současnosti využívá.

Na tomto místě bych rád uvedl, že v budoucnu by mělo při vývoji softwaru, informačních databází a dalších informačních produktů dojít ke změnám v pohledu na tuto problematiku. Cílem procesu změn by mělo být odstranění motivů i skutků protiprávního chování nazývaného - softwarové pirátství, jako celku. Jak vyplývá z kapitoly 2.1, jakýkoliv pokus o snížení úrovně pirátství nemůže být zaměřen pouze na změny ekonomických faktorů, ale i na změny sociálních struktur a vztahů. Proto můžeme s úspěchem pochybovat o legitimnosti striktního vymáhání zákonů soukromými organizacemi, a při existenci takových zákonů, které podle výsledků dostupných průzkumů porušuje průměrně 40 % uživatelů softwaru. Proto by mělo dojít k obecnému přehodnocení myšlení a využití vynakládaných prostředků spíše na vytvoření právního povědomí a následného vymáhání práva, jak již k tomu v mnoha případech dochází. A tyto ušetřené prostředky investovat do propagace

problematiky, dále do snižování nákladů na produkci a hlavně do výrazné podpory technologického výzkumu, jenž, jak se ukazuje, může následně nabídnout zcela nové metody distribuce a šíření softwaru i jednotlivých druhů dat oprávněným uživatelům. Jedním z možných řešení je model zahrnující striktní vymáhání používání legálního softwaru v komerčních i neziskových organizacích a zároveň umožňující tolerantnější postup proti soukromým osobám, zejména proti studentům, kteří tvoří hlavní skupinu nekomerčních softwarových pirátů.

Další oblastí kterou se tato práce již nezabývala by byl vztah průmyslově rozvinutých a rozvojových zemí ve vztahu k softwarovému pirátství. Nicméně podle mého názoru je to otázka spíše sociologie, než informačních studií, k nímž měla tato práce být platným příspěvkem.

SEZNAM POUŽITÉ LITERATURY

26. duben – Světový den duševního vlastnictví [online]. Praha : MK ČR, 2006 [cit. 2007-07-31]. Dostupné na Word Wide Web: <http://www.mkcr.cz/scripts/detail.php?id=1731>.

Adobe - Anti-piracy initiative : What is software piracy [online]. c2007 [cit. 2007-08-07]. Dostupné na Word Wide Web: <http://www.adobe.com/aboutadobe/antipiracy/piracy.html>.

Agreement on Trade-Related Aspects of Intellectual Property Rights: Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization. Signed in Marrakesh, Morocco on 15 April 1994. [online]. c2007 [cit. 2007-08-07]. Dostupné na Word Wide Web: <http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm >

ANONYMOUS. 2001. *Narodny Bezpecnostny Urad pwn3d* [online]. 2001 [cit. 2007-07-19]. Dostupné na Word Wide Web: <http://blackhole.sk/node/442>.

Apple iPhone středem pozornosti uživatelů i hackerů. *Novinky.cz* [online]. 6. 7. 2007 [cit. 2007-07-16]. Dostupné na World Wide Web: < http://www.novinky.cz/internet/apple-iphone-stredem-pozornosti-uzivatelu-i-hackeru_118402_9619j.html>.

BAGHI, Kallol, KIS, Peeter , CERVENY, Robert. 2006. Global software piracy : Can economic factors alone explain the trend? . *Communications of the ACM* [online]. 2006, vol. 49, no. 6, s. 70-76.

BANGEMAN, Eric. 2007. Intellectual Property Protection Act to make attemped infringement illegal. *Ars technica: the art of technology* [online]. 2007 [cit. 2007-07-23].

Dostupné na World Wide Web: <http://arstechnica.com/news.ars/post/20070515-intellectual-property-protection-act-to-make-attemped-infringement-illegal.html>.

Bernská úmluva o ochraně literárních a uměleckých děl. 1886. *Wikisource* [online]. 1886 [cit. 2007-06-30]. Dostupné na World Wide Web: <http://cs.wikisource.org/wiki/Bernsk%C3%A1_%C3%BAmluva_o_ochran%C4%9B_liter%C3%A1rn%C3%ADch_a_um%C4%9Bleck%C3%BDch_d%C4%9Bl>.

Blu-Ray Disc vede – u zlodějů. *Technet.cz* [online]. 2007 [cit. 2007-07-31]. Dostupné na World Wide Web: <http://technet.idnes.cz/blu-ray-disc-vede-u-zlodeju-d04-/tec_video.asp?c=A070726_131042_tec_video_vse>.

BOYARSKI, Jason R. Thailand to enforce IP law. Intellectual Property & Technology Law Journal. 2002, vol. 14, no. 3, s. 35.

British Broadcasting Corporation [online]. 2001 [cit. 2007-07-19]. Dostupné na World Wide Web: <http://www.bbc.co.uk/schools/gcsebitesize/ict/legal/1misuesrev5.shtml>.

BUNN, E. DeV., GAINESVILLE, Jr. c2005. *Internet software piracy and the NET Act : a historical and perspective analysis of cyberlaw in the United States* . [S.l.] : Cambridge Lighthouse Press, c2005. 80 s. ISBN 0976707578.

BULKLEY, W. 1990. Software users are beginning to rebel against the steady stream of upgrades. *Wall Street Journal*, x, B4 (1991).

Business Software Alliance. 2007 *Podrobná studie BSA-IDC o globální míře softwarového pirátství* . Praha : BSA, 2006. 2 s. Dostupné na World Wide Web: <http://w3.bsa.org/czechrepublic/upload/200704_studiebsa_stat_table.pdf>.

Business Software Alliance [online]. 2000 [cit. 2007-07-19]. Dostupné na World Wide Web: <http://www.bsa.org/Piracy%20Portal.aspx>.

CASIRAYA, Lawrence D. 2002. Firms given 45 days to legalize unlicensed software. *BusinessWorld.* 2002, vol.12, no. 2, s.1.

Copyright infringement of software. *Wikipedia : the Free Encyclopedia* [online]. 2007 [cit. 2007-07-07]. Dostupné na World Wide Web: < http://en.wikipedia.org/wiki/Software_piracy>.

CRAIG, Paul, BURNETT, Mark. 2005. *Software Piracy Exposed* . [S.l.] : Syngress Publishing, 2005. 356 s. ISBN 1932266984 .

Content protection for recordable media. *Wikipedia : the Free Encyclopedia* [online]. 2007 [cit. 2007-07-07]. Dostupný na World Wide Web: <http://en.wikipedia.org/wiki/Content_Protection_for_Recordable_Media>.

ČERMÁK, Jiří. 2001. Omyly znalce počítačového práva. *Občanské právo* [online]. 2001 [cit. 2007-07-30]. Dostupné na World Wide Web: <http://obcanskepravo.juristic.cz/79693/ >.

Česko. *Zákon č. 121/2000 Sb. ze dne 7. dubna 2000, částka 106/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorským zákonem).* [online]. 2000 [cit. 2007-07-31]. Dostupné na World Wide Web: <http://www.nkp.cz/o_knihovnach/AutZak/Index.htm>.

Česko. *Zákon č. 140/1961 Sb. ze dne 29.11.1961 (trestní zákon).* [online]. 2006 [cit. 2007-07-31]. Dostupné na World Wide Web:

<http://www.zakony.cz/?sekce=zakony&akce=view&zdarma=true&odkaz=140/1961%20Sb>

.

DENNING, Dorothy E. 1998. Information warfare and security. 1st ed. : Addison-Wesley, 1998. 544 s. ISBN 0201433036.

DIODATO, V. *Dictionary of bibliometrics*. New York : The Haworth Press, 1994. ISBN 156024853X.

DVD Copy Control Association [online]. c2000 [cit. 2007-07-22]. Dostupné na World Wide Web: <http://www.dvdcca.org/>.

Essential Concepts : Apendix A [online]. c2007 [cit. 2007-07-19]. Dostupné na World Wide Web: <http://www.glencoe.com/norton/online/essential/appendixa/content.html>.

EVELOFF, S. H., FABIUS, M.L. 1990. What clients need to know about software piracy. *Journal of Accountancy*. 1990, no. 1, s. 134-140.

Evropská unie. Rada. 1991. Směrnice Rady 91/250/EHS ze dne 14. 5. 1991 o právní ochraně počítačových programů. *Official Journal of the European Communities*. L 122, 17. 5. 1991, s. 42-46.

EVROPSKÁ UNIE. Rada. 1992. Směrnice Rady 92/100/EHS ze dne 19. 11.1992 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s autorským právem. *Official Journal of the European Communities*. L 346, 27. 11. 1992, s. 61-66.

EVROPSKÁ UNIE. Rada. 1993a. Směrnice Rady 93/83/EHS ze dne 27. 9. 1993 o koordinaci určitých předpisů týkajících se autorského práva a práv s ním souvisejících při družicovém vysílání a kabelovém přenosu. *Official Journal of the European Communities*. L 248, 6. 10. 1993, s. 15-21.

EVROPSKÁ UNIE. Rada. 1992b. Směrnice Rady 93/98/EHS ze dne 29. 10. 1993 o harmonizaci doby ochrany autorských práv a určitých práv souvisejících. *Official Journal of the European Communities*. L 290, 24. 11. 1993. s. 9-1.

EVROPSKÁ UNIE. Evropský parlament a Rada. 1996. Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11.3.1996 o právní ochraně databází. *Official Journal of the European Communities*. L 077, 27. 03. 1996, s. 20-28.

EVROPSKÁ UNIE. Evropský parlament a Rada. 2001a. Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. 5. 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. *Official Journal of the European Communities*. L 167, 22. 6. 2001, s. 10-19.

EVROPSKÁ UNIE. Evropský parlament a Rada. 2001b. Směrnice Evropského parlamentu a Rady 2001/84/ES ze dne 27. 9. 2001 o právu na opětný prodej ve prospěch autora originálu uměleckého díla. *Official Journal of the European Communities*. L 272, 13. 10. 2001, s. 32-36]

EVROPSKÁ UNIE. Evropský parlament a Rada. 2004. Směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. 4. 2004 o vymáhání práv duševního vlastnictví. *Official Journal of the European Communities*. L 195, 2. 6. 2004, s. 16-25.

Forum Section. Commun. *ACM*. 2000, vol. 43, no. 12, s. 11-13.

FYODOR. 2007. *Insecure.org : Nmap Free Security Scanner, Tools & Hacking resources* [online]. [2006] [cit. 2007-07-04]. Dostupné na World Wide Web: <http://insecure.org/>.

GEMIGNANI, M. 1986. A College´s liability for unauthorized copying of microcomputer software by students. *Journal of Law Education.* Fall 1986, no.15, s. 421-437.

Glossary of IT Terms [online]. Yahoo! Geocities, [2000] [cit. 2007-07-17]. Dostupné na World Wide Web: <http://www.geocities.com/mitalib16/FYHMCT/internet/IT_terms.htm>.

GOPAL, R. D., SANDERS, G.L. 1997. Preventive and deterrent controls for software piracy. *J.MIS* . 1997, vol. 4, no. 13, s. 29-47.

GREGURAS, Fred M. 1998. Trends in software licensing and legal protection for software. *Fenwick & West* [online]. 1998 [cit. 2007-08-17]. Dostupné na World Wide Web: <http://www.fenwick.com/docstore/Publications/IP/IP_Articles/98_Trends_in_Software_Lice.pdf>.

GUTMANN, Peter. 2007. *A Cost Analysis of Windows Vista Content Protection* [online]. 2007 , 12th June 2007 [cit. 2007-07-22]. Dostupné na WWW: <http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html>.

HERITAGE Foundation index of economic freedom [online]. The Heritge Foundation/Wall Street Journal , [2006], [cit. 2006-08-18]. Dostupné na World Wide Web: <http://www.heritage.org/research/features/index/>.

HIBBERT, Chris. 2002. *A copy protection and content management system*. [s.l.] : [s.n.], [2002]. 6 s. Dostupný na World Wide Web: <http://www.dvb.org/documents/newsletters/DVB-SCENE-05-CopyProtectionArticle.pdf>.

History of software piracy [online]. 2004. [cit. 2003-01-25] Dostupné na World Wide Web: <http://www.wbglinks.net/pages/history>.

Hoax. 2007. *Wikipedia : the Free Encyclopedia* [online]. 2007 [cit. 2007-07-07]. Dostupné na World Wide Web: <http://en.wikipedia.org/wiki/Hoax>.

HOFSTEDE, G. 2001 . *Culture`s consequences : inernational differences in workrelated values*. 1st ed.. Beverly Hills : Sage Publishers, 2001.

HONICK, Ron. *Software piracy exposed.* Rockland (Mass.) : Syngress, 2005. xvi, 310 s. ISBN 1932266984

HROUŽEK, Daniel. 2007, 09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0. *High-Def Mag* [online]. 2007 [cit. 2007-07-31]. Dostupné na World Wide Web: <http://highdefmag.cz/clanek/09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63-56-88-c0>. ISSN 1802-516.

HUNDLEY, Richard O. 2002, et al. The Future of the Information Revolution in Europe : Proceedings of an International Conferences. *International Relations and Security Network.* c2002, [cit. 2002-06-17]. Dostupné na World Wide Web: <http://www.isn.ethz.ch/researchpub/publihouse/misc/RAND/CF.172.chap11.html>

HUNT, Nathan. 2004. Internet Pirate Pleads Guiltly. *Communications Today.* 2004, vol. 8, no. 67, s.1-3.

CHIN, W. 2000. Partial least squares for IS researchers : An overview and presentation of recent advances using the PLS approach. *Proceedings of CIS*. 1.1. 2000, no. 1, s. 741-742.

CHRISTENSEN, L. EINING, Martha M. 1991. Factors Influencing Software Piracy : Implicationsfor Accountnts. *Journal of Information Systems*. 1991, vol. 5, is. 1, s. 67-80.

CHRISTENSEN, Ward. 1990. *Collection of Memories of writing and running the first BBS (Circa 1992)* [online]. 1990 [cit. 2007-06-14]. Dostupné na World Wide Web: <http://www.bbsdocumentary.com/software/AAA/AAA/CBBS/memories.txt>.

CHUDÍČEK, Tomáš.2007, *Definice informační kriminality* [online]. [2005] [cit. 2007-08-08]. Dostupné na World Wide Web: <http://www.chudicek.cz/prispevek8.aspx>.

Internet forum. *Wikipedia : the Free Encyclopedia* [online]. 2007 [cit. 2007-07-07]. Dostupné na World Wide Web: <http://en.wikipedia.org/wiki/Internet_forum>.

JK thief faces jail. *Mirror.co.uk* [online]. 21/12/2005 [cit. 2007-07-16]. Dostupné na World Wide Web:

<http://www.mirror.co.uk/archive/tm_method=full%26objectid=16508384%26siteid=89520-name_page.html>.

JOHNSON , Neil F., DURIC , Zoran, JAJODIA, 2000. Sushil. *Information Hiding : teganography and Watermarking - Attacks and Countermeasures*. 1st ed. [S.l.] : Springer, 2000. 160 s. ISBN 978-0792372042.

JON Lech Johansen. 2007. *Wikipedia : the Free Encyclopedia* [online]. 2007. [cit. 2007-07-21]. Dostupný na World Wide Web: <http://en.wikipedia.org/wiki/ Jon_Lech_Johansen>.

KIRKPATRICK, David. 2007, How Microsoft conquered China. *CNNMoney.com* [online]. 2007 [cit. 2007-07-24]. Dostupné na World Wide Web: <http://money.cnn.com/magazines/fortune/fortune_archive/2007/07/23/100134488/index.htm >.

KRAUSE, Micki, TIPTON, Harold F. Information security management handbook. 1st ed. NY: CRC Press, 1999. 728 s. ISBN 0849398290.

KREJČÍ, Jaromír. 2000, *Shareware, freeware, trialware - konečně jasno* [online]. 2000 [cit. 2007-07-29]. Dostupné na World Wide Web: <http://interval.cz/clanky/shareware-freeware-trialware-konecne-jasno/ >.

KREMEROVÁ, Pavla. 1998a, *Ochrana softwaru narozena v USA. Živě.cz* [online]. 1998 [cit. 2007-07-31]. Dostupné na World Wide Web: <http://www.zive.sk/h/Spravy/AR.asp?ARI=3546>.

KREMEROVÁ, Pavla. 1998b, *Na softwarové pirátství doplácí i nepočítačníci. Živě.cz* [online]. 1998 [cit. 2007-07-25]. Dostupné na World Wide Web: <http://www.zive.cz/default.aspx?textart=1&article=4750>.

KREMEROVÁ, Pavla. 1998c. *Piráti pozor. Živě.cz* [online]. 1998 [cit. 2007-07-25]. Dostupné na World Wide Web: < http://www.zive.cz/default.aspx?section=21&server=1&article=4480>.

KRUG, Steve. 2000. *Don't Make Me Think : A Common Sense Approach to Web Usability* . 1st ed. [S.l.] : New Riders Press, 2000. 195 s. ISBN 978-0789723109.

KŘÍŽ, Jan. 1999, Ochrana autorských práv v informační společnosti. 1. vyd. Praha : Linde, 1999. s. 252. ISBN 80-7201-190-1.

Kvůli pirátství zavřelo v Česku 50 počítačových kaváren a heren. *Technet* [online]. 2007 [cit. 2007-07-23]. Dostupné na World Wide Web: <http://technet.idnes.cz/kvuli-piratstvi-zavrelo-v-cesku-50-pocitacovych-kavaren-a-heren-pvf-/software.asp?c=A070427_110353_software_vse>.

LANCASTER, F.W. 1978. *Toward paperless information systems*. New York : Academic Press, 1978.

LEE, Mark S. 2005,*Entertainment and Intellectual Property Law*. (MA,USA) : Thomson/Glasser LegalWorks, c2005. 1 v. (loose-leaf) ; 26 cm. + 1 CD-ROM (4 3/4 in.)

LINDEROVÁ, Marta. Efektivnější využívání zdrojů společnosti. *MM Průmyslové spektrum*. 1998, roč. 2, č. 6, s. 53. ISSN 1211-6653.

LITCHFIELD, David, ANLEY, Chris, HEASMAN, John. 2005. *The Database Hacker's Handbook : Defending Database Servers* . [S.l.] : Wiley, 2005. 500 s. ISBN 0764578014 .

LUDRAM, Michael. 1999. Buy now or pay later. *Director magazin.* 1999. vol. 52, no. 11, s. 80.

MESO, P. et al. 2005. Bounded rationality and sectoral differences in diffusion of national IT policies. *Electronic Journal of Information Systems in Developing Countries*. 2005, vol.1.

MIKLÍK, Aleš. 2004, Americký soud prohlásil výměnné sítě za legální. *Lupa.cz : Server o českém internetu* [online]. 2004 [cit. 2007-08-07]. Dostupné na World Wide Web: <http://www.lupa.cz/clanky/americky-soud-prohlasil-vymenne-site-za-legalni/>.

MISHRA, Birendra K., RAGHU, T.S., PRASAD, 2007. Ashutosh. Strategic Analysis of Corporate Software Piracy Prevenion and Detection. *Journal of Organizational Computing and Electronic Commerce*. 2005, Vol. 15, no. 15, s. 223-252.

McGUIRE, Stryker. 2001, Microsoft Cops : As gangsters take over the software-piracy trade, one company is fighting back with its own global force of crime busters. *Newsweek.* 2001, no. 1, s. 20.

MORES, T., DHILLON, G. 2000. Software piracy : A view from Hong Kong. *Commun. ACM*. 2000, vol. 43, no. 12, s. 88-93.

MOSQUERA, Mary. 1999. The high price of software piracy. *Computer Reseller News*. 24 May 1999, no. 843, s. 76-77.

Motion Picture Association of America. *Wikipedia : the Free Encyclopedia* [online]. 2007 [cit. 2007-07-23]. Dostupný na World Wide Web: <http://en.wikipedia.org/wiki/Motion_Picture_Association_of_America>.

MURRAY, Brian H. 2003. *Defending the brand : aggressive strategies for protecting your brand in the online arena* . New York : American Management Association , 2003. 272 s., ISBN 978-0814407547.

NOSTUR, MINOR. 2006. *Policia zhabala server komunity - UPDATED* [online]. 2006 [cit. 2007-08-17]. Dostupné na World Wide Web: <http://sk.zone-h.org/content/view/42/9/>.

NÝVLT, Václav. 2007a. *Sekera na softwarové piráty. Policejní zásah na vlastní oči* [online]. *Technet*. 2007 [cit. 2007-07-31]. Dostupné na World Wide Web: <http://technet.idnes.cz/sekera-na-softwarove-piraty-policejni-zasah-na-vlastni-oci-pof-/software.asp?c=A061008_104436_software_NYV>.

NÝVLT, Václav. 2007b. *Konec internetových rádií? Možná již v květnu* [online] *Technet*. 2005 , 17. dubna 2007 [cit. 2007-08-17]. Dostupné na World Wide Web: <http://czechtek.bloguje.cz/523558-americka-organizace-na-ochranu-autorskych-prav-chce-zlikvidovat-internetova-radia-technet-cz.php>.

POHŮNEK, Vojtěch. 2007. Přísně střežený Harry Potter už je na internetu. *ITBiz.cz* [online]. 2007 [cit. 2007-07-22]. Dostupný z WWW: <http://itbiz.cz/harry-potter-pronikl>.

PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita [Electronic information crime]*. Praha, 2006. 114 s., 6 s. příl. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2006. Vedoucí diplomové práce PhDr. Richard Papík, PhD.

RADA EVROPSKÝCH SPOLEČENSTVÍ, 1991 . *Směrnice Rady ze dne 14. května 1991 o právní ochraně počítačových programů (91/250/EHS).* [s.l.] : [s.n.], 1991. 5 s. Dostupné na World Wide Web: <http://eur-lex.europa.eu/LexUriServ/site/cs/dd/17/01/31991L0250CS.pdf>.

Reuters. 2007. Hacker claims alleged 'Harry Potter' ending : Ahead of book release, debate has raged about whether boy wizard dies. *Msnbc* [online]. 2007 [cit. 2007-07-10]. Dostupný z WWW: <http://www.msnbc.msn.com/id/19352126/>.

RIAA opět podává žaloby. *Telmedi* [online]. 02/01/2004 [cit. 2007-07-17]. Dostupné na World Wide Web: <http://www.telmedia.cz/php/index2.php?cat=&showid=RIAA%20op%ect%20pod%e1v%e1%20%9ealoby&Telmedia=460ed1d846fc80cecbb83fb971ed5240>.

RICE, F. 1991. How copycats steal billions. *Fortune*. 1991, no. 22, s. 157-164.

ROBINSON, Stuart. 2005. *DVD-Audio Copy Protection Defeated via WinDVD Software Hack* [online]. 2005 , 2005 [cit. 2007-07-21]. Dostupné na World Wide Web: <http://highfidelityreview.com/news/news.asp?newsnumber=14550899>.

SCAMBREY, Joel, MCCLURE, Stuart, KURTZ, George. 2001. Hacking bez tajemství. 1. vyd. Praha: Computer Press, 2001. s. 592.

Sedmá výroční zpráva BSA o softwarovém pirátství ve světě [online]. 2003. [cit. 2003-01-25].
Dostupné na World Wide Web: <http://www.bsa.cz>.

SHIMEALL, Timothy J. 1999. Software security in an internet world : an executive sumary. *IEEE Software*. 1999, vol. 16, no. 4, s. 58.

SHIN, S. K., GOPAL, R. D., SANDERS, G.I. 2004. Global software piracy revised. *ACM*. 1. 1.2004, vol. 47, no. 1, s. 103-107.

SMITH, J. K 1987. The computer software rental act : amending the first sale doctrine to protect computer software copyright. Loyola of Los Angeles Law Review (June): 1613-1639.

Software piracy and the law. [online]. In Business software Alliance. c2002 [cit. 2002-06-18].
Dostupné na World Wide Web:
<http://www.bsa.org/usa/antipiracy/press/materials/resources.phtml>

STANIFORD, Stuart, PAXSON, Vern, WEAVER, Nicholas. 2002. *How to own the internet in your spare time*. 2002. 19 s. Dostupné na World Wide Web: <http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf>.

STERLING, Bruce. 1992. The Hacker Crackdown. [online]. 1992 [cit. 2007-07-19]. Dostupné na World Wide Web: <http://martin.hinner.info/crackdown/english/index.html>.

Sundevil. 2002. *Mispedia* [online]. 2002 [cit. 2007-07-07]. Dostupný na World Wide Web: <http://www.mispedia.org/Operation_Sundevil.html>.

SWINIARD, W. R., RINNE, H., KAU, A.K. 1990. The morality of software piracy : a cross-cultural analysis. *Journal of Bussiness Ethics*. 1. 1. 1990, no. 9, s. 655-664.

ŠEBÍK, Antonín. 2007. *PeerGuardian 2.0* [online]. 2007 [cit. 2007-08-05]. Dostupné z World Wide Web: <http://vseohw.net/clanky/software/peerguardian-2-0>.

TDKIV : Česká terminologická databáze z oblasti knihovnictví a informační vědy [online databáze]. 2003- . Praha : Knihovnický institut NK ČR, 2003- [cit. 2007-01-20]. Databáze vznikla v letech 2001-2002 v rámci projektu podpořeného grantem MK ČR. Dostupná na World Wide Web: <http://sigma.nkp.cz/cze/ktd>.

Transparency International, Internet Center for Corruption Reserch : The Corruption Index [online]. 2006 [cit. 2007-07-15]. Dostupné na World Wide Web: <http://www.gwdg.de/~uwvw/icr.htm>.

Třetí výroční zpráva BSA a IDC o softwarovém [online]. BSA-IDC, 2000, 2006 [cit. 2007-08-17]. Dostupné na World Wide Web: <http://w3.bsa.org/czechrepublic/statistiky/upload/Czech%20Republic%20-%20IDC%20Global%20Piracy%20Study2005_SK.pdf>.

TUDOR, Jan Killmeyer. Information security architecture: an integrated approach to security in the organization. 1st ed. NY : CRC Press, 2000. 424 s. ISBN 0849399882

USA si stěžují na Čínu kvůli autorským právům. *iHned.cz : Zpravodajský Server Hospodářských Novin*. [online]. 2007. Dostupné na World Wide Web: <http://ihned.cz/c4-10073040-20852920-000000_d-usa-si-stezuji-na-cinu-kvuli-autorskym-pravum>.

User friendly. *Wikipedia : the free encyclopedia* [online]. 2007 [cit. 2007-07-22]. Dostupné na World Wide Web: <http://en.wikipedia.org/wiki/ User_Friendly>.

VAŠEK, Václav. 2007. Microsoft přiznává, že těží ze softwarového pirátství. *CD-R Server* [online]. 2007 [cit. 2007-07-24]. Dostupné na World Wide Web: <http://www.cdr.cz/a/20810>.

WhatIs.com : The Leading IT Encyclopedia and Learning Center [online]. c2007 [cit. 2007-07-19]. Dostupné na WWW: <http://whatis.techtarget.com/definition/0,,sid9_gci213592,00.html>.

Who We Are : RIAA [online]. 2004 [cit. 2007-07-31]. Dostupné na World Wide Web: <http://www.riaa.com/aboutus.php>.

World Economic Forum. The Global Information Technology Report. [S.l.] : Oxford University Press, 2003. 238 s.

Příloha

TABLE 1. SAMPLE DEMOGRAPHICS

	OWN COMPUTER		
	YES	NO	TOTAL
Gender: Male	100	67	167
Female	39	56	95
Total	139	123	262[a]
Average Age:	25.0	24.9	25.0
Average Years in College	3.8	3.7	3.8
Percent Employed	91%	88%	90%
Percent Married	46%	63%	54%
Percent who Pirate Software (AMOUNT)	73%	28%	52%

a Not all subjects responded to all questions so totals do not equal 269

FIGURE 2. THEORY OF REASONED ACTION VARIABLES
Independent Variables[b]

1. AP Attitudes toward software piracy

DISHONEST People who make copies of software programs they did not purchase are truly dishonest.

[a]GIVING There is nothing wrong with giving friends copies of my software as long as I don't charge them for it.

GUILTY I would feel guilty if I copied a program I had not purchased.

ONETIME There is nothing wrong with making a copy of a software program for a one time project.

[a]STUDENT There is nothing wrong with copying software as a student since students have limited financial resources.

2. SN Subjective norms surrounding software piracy

SCHOOL My school encourages/discourages copying

(semantic scale).

COMPANY My company encourages/discourages copying (semantic scale).

F-WRONG My friends think it is wrong to copy software.

[a]F-COPY My friends make copies of software and share it with others.

Dependent Variable--Pirating behavior

[a]RECEIVE I make copies of software programs that my friends have purchased.

[a]GIVE People I know sometimes give me copies of their software programs.

AMOUNT How many software programs do you have?

Please indicate the number of software packages obtained from each of the following sources by placing the number of software packages on the appropriate lines. If you are not sure of the exact count, please approximate.
Copyrighted software:
Purchased with computer, from local vendor or from catalog vendor -----
Copied from friends, work or school -----
Non-copyrighted software:
Freeware (public domain) or shareware -----
Developed myself -----
Other (Please be specific) -----
TOTAL NUMBER -----

a Items were reversed scored.
b All statements refer to copyrighted software.

TABLE 2. KNOWLEDGE AND AWARENESS OF COPYRIGHT LAWS

Legend for Chart:

A - STATEMENTS CONCERNING COPYRIGHTED SOFTWARE:
B - PERCENTAGE AGREEING WITH STATEMENTS, WHO PIRATE SOFTWARE
C - PERCENTAGE AGREEING WITH STATEMENTS, WHO DO NOT PIRATE SOFTWARE

A	B	C
It is illegal to purchase and	29.6%	30.6%

use on multiple machines.

It is illegal if purchased by school and used on my home computer.	49.5%	55.6%
It is illegal if purchased by employer and used on my home computer.	69.1%	80.6%
It is illegal if purchased by friends and used on my home computer.[a]	73.2%	99.9%
It is illegal to possess unauthorized software.	32.3%	25.0%
The copyright laws are enforced strongly.	3.3%	5.7%
I have read the licensing agreement on software packages.	50.0%	51.4%

a significant at p < .055

TABLE 3. FACTOR ANALYSIS VARIMAX ROTATED MATRIX

	FACTOR 1	FACTOR 2	FACTOR 3
AP = Attitude Toward Piracy			
DISHONEST	.76	-.04	.02
STUDENT	.74	.15	.00
GIVING	.72	.31	.26
GUILTY	.69	.17	.31
ONETIME	.59	-.05	.44
SN = Subjective Norms - Superiors			
SCHOOL	.16	.84	-.13
COMPANY	.06	.80	.29
SN = Subjective Norms - Friends			
F-COPY	.05	.22	.76
F-WRONG	.23	-.06	.71
Variance Accounted for by Each Factor			
Eigen value	3.32	1.29	1.04
Percent	36.91	4.41	1.6
Cumulative	36.95	1.26	2.8

TABLE 4. CHARACTERISTICS OF MEASURES

Legend for Chart:

A - No heading
B - Number of Items
C - Means
D - Standard Deviations
E - Scale Reliability (Cronbach's Alpha)

A	B	C	D	E
AP = Piracy Attitudes	5	4.08	.68	.81
SN = Subjective Norms	4	3.08	1.08	.57
P = Pirating Behavior	3	3.84	.33	.67

TABLE 5. MULTIPLE REGRESSION ANALYSIS

Independent Variables	b	Beta	t
AP = Piracy Attitudes	.63	.51	5.77[b]
SN = Subjective Norms	.34	.13	2.59[a]
Intercept	-.04	--	-.07

Adjusted R^2 = .43 F = 39.00[b]
a $p < .015$
b $p < .001$

Evidence výpůjček

Prohlášení:
Dávám svolení k půjčování této diplomové práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze, 8. 8. 2007.

Jan Kolátor

Jméno	Katedra / Pracoviště	Datum	Podpis