Vysoká škola ekonomická v Praze
Fakulta managementu v Jindřichově Hradci

Bakalářská práce

2008 Petr Kuk

Vysoká škola ekonomická v Praze
Fakulta managementu v Jindřichově Hradci

TÉMA BAKALÁŘSKÉ PRÁCE:

Postihování nelegálního šíření počítačových programů

Vypracoval: Petr Kuk
Vedoucí bakalářské práce: Doc. Dr. JUDr. Jan Hejda

Školní rok 2007 / 2008

VŠE

FAKULTA MANAGEMENTU

Vysoká škola ekonomická v Praze
Jarošovská 1117/II, 377 01 Jindřichův Hradec

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro akademický rok 2006/2007

Název práce:	**Postihování nelegálního šíření počítačových programů.**
Zadání práce:	Cílem práce bude vymezit ochranu autorského práva při šíření počítačových programů a možnosti postihů jejich nelegálního šíření podle jednotlivých právních odvětví. Dále student vymezí způsoby, nástroje a techniky nelegálního šíření software a jejich možný dopad na postih.
Jméno studenta:	Petr Kuk
Ročník:	2.
Obor:	MANAGEMENT
Vedoucí práce:	doc. Dr. JUDr. Jan Hejda
Katedra:	Katedra společenských věd
Termín zadání:	23.6.2006
Termín odevzdání:	Dle vyhlášky o průběhu státních závěrečných zkoušek v ak. roce 2006/2007

V Jindřichově Hradci 23.6.2006

Ing. Vladimír Přibyl
proděkan pro pedagogickou činnost

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny významné použité prameny a literaturu, ze kterých jsem čerpal.

V Praze dne 10. dubna 2008 .....

podpis

Za odborné vedení při vypracování Bakalářské práce, za její pečlivé posouzení, připomínky a rady, které mi byly poskytnuty v průběhu zpracování bych chtěl touto cestou poděkovat **doc. Dr. JUDr. Janu Hejdovi** z Vysoké školy ekonomické v Praze, Fakulty managementu v Jindřichově Hradci

Abstrakt

Práce se zabývá problematikou nelegálního šíření počítačových programů. Problematika nelegálního šíření počítačových programů je dnes neoddělitelnou součástí našich životů. Tato práce by měla laikovi poskytnout poměrně ucelený přehled o problematice jak z pohledu práva, tak z pohledu těch kdo autorské právo porušují. V první části je zaměřena zejména na vysvětlení základních pojmů, které s problematikou souvisí. Následuje část věnovaná právním normám a postihování nelegálního šíření počítačových programů. Druhá část je pak věnována praktické stránce šíření nelegálních programů, zejména v síti internet.

Cílem práce je zejména shrnutí poznatků o problematice do ucelené formy, které čtenáři umožní utřídit a rozšířit si vědomosti z této oblasti a dozvědět se i některé skutečnosti, které nejsou obecně známy.

Abstract

The subject of this Bachelor's thsesis is problematics of illegaly distributed software. Problematics of illegaly distributed software is today integral part of our lives. This Bachelor's thesis is focused on giving quite complete overview of this problematics from position of law as well as from position of those, who are violating copyright laws. First part of this thesis contains explanation of basic terms, legal standards and recourse of illegal distribution of software. Second part is focused on practical aspects of illegal software distribution, especially via internet.

Objective of this thesis is digest of knowledges into integrated form that allows readers to sort and extend his knowledges and to learn some new, not commonly known, facts.

Obsah

Úvod

Tato bakalářská práce je věnována problematice nelegálního šíření počítačových programů. Od masového nástupu výpočetní techniky v 80. a 90. letech 20. století se nelegální šíření softwaru, chcete-li pirátství, velmi rozmohlo a i v dnešní době je významným fenoménem. V práci se pokusím zaměřit na problematiku jak z pohledu zákona a těch, kteří jsou počítačovým pirátstvím poškozování tak z pohledu uživatelů, kteří se snaží pořídit si software bezúplatně.

Téma práce jsem si zvolil zejména proto, že se již několik let pohybuji v oblasti předtiskové přípravy, kde jsou problémy s dodržováním autorského zákona v oblasti softwaru poměrně časté. Proto mne i osobně zajímalo, jak to vlastně s autorským právem je a co může těm, kdo jej porušují, hrozit. Navíc výpočetní technika je mým velkým koníčkem a zajímá mne takřka vše, co se jí týká. Měl jsem tedy z dřívějška základní znalosti, na kterých jsem mohl stavět. Téma práce bylo navíc koncipováno tak, že mi dovolilo se věnovat oběma stránkám problematiky – teoretické i praktické. Jsem přesvědčen, že nabyté znalosti mohu v budoucnu zúročit. Kupříkladu ve chvíli, kdy bych se rozhodl věnovat se podnikatelské činnosti. Porušení autorského práva, byť z neznalosti, by mohlo mít v počátcích podnikání fatální následky, a proto jsou znalosti z této oblasti dobře využitelné i v praxi.

Práce je zaměřena na problematiku zejména ze stránky praktické. V textu se objevují některé odbornější termíny, ale často se dopouštím i značných zjednodušení. Nicméně jsem přesvědčen, že to není ke škodě a spíše to přispěje ke snadnějšímu pochopení u laiků v dané oblasti.

V první polovině práce přiblížím zejména základní pojmy a problematiku nelegálního softwaru z teoretické stránky. Patří sem tedy vše od názvosloví přes metody licencování počítačových programů, ochrany proti pirátskému šíření až po právní aspekty počítačového pirátství. Pokusím se nastínit také některé ekonomické aspekty problematiky, jelikož nelegální šíření softwaru není jen právní či morální problém, ale dopadá i do ekonomické oblasti.

Druhá část se zaměřuje na praktickou stránku počítačového pirátství. Pokusím se přiblížit techniky, jakými se nelegální programy šířily dříve, a techniky, které se používají dnes. Vzhledem k významnému zastoupení internetu v této oblasti se tato část bude věnovat využití tohoto média. Pokusím se zmínit některé programy, které se dnes k šíření nelegálního softwaru používají, jaká je jejich obliba u uživatelů, kde lze na internetu nalézt nelegální data ke stažení či jak piráti obchází ochranu programů, která je do nich implementována výrobci.

Na závěr nabízím krátké shrnutí, vlastní názor na problematiku a odhad, jak se asi bude tato oblast vyvíjet dále v budoucnu.

Při zpracování práce jsem nejprve prostudoval autorský zákon a další literaturu a odpovídající internetové zdroje. To mi poskytlo základ pro zpracování teoretické části práce. Pro zpracování praktické části jsem opět musel nejprve nastudovat příslušné teoretické zdroje týkající se principů šíření nelegálních dat. Poté jsem se pokusil najít a v praxi vyzkoušet všechny zmíněné softwarové nástroje a internetové zdroje, o kterých je v druhé části práce řeč. To mi dovolilo zpracovat praktickou část z pohledu „zasvěceného“ uživatele.

Práce se tedy věnuje spíše shrnutí poznatků do ucelené formy. Nesnaží se tedy navrhovat nějaká obecná řešení, ani vynášet soudy nad piráty. Cílem je zejména poskytnout čtenáři ucelený přehled o problematice nelegálního softwaru, který bude moci využít v praxi a který mu pomůže lépe se v této oblasti orientovat. Do budoucna potom bude třeba věnovat větší pozornost tomu, jaké programy v práci či doma využívá a jak je to s jejich legalitou.

1 Vysvětlení základních pojmů

V úvodní kapitole se krátce seznámíme s některými základními pojmy, které se v následujícím textu mohou objevit. Samozřejmě je jen těžko možné uvést veškeré pojmy. Pokusil jsem se tedy zejména uvést několik slov k nejrozšířenějším druhům softwarových licencí. Dále se krátce věnuji pojmům týkajícím se nelegálního kopírování softwaru. Některé další pojmy pak jsou v textu vysvětleny poznámkou na konci stránky.

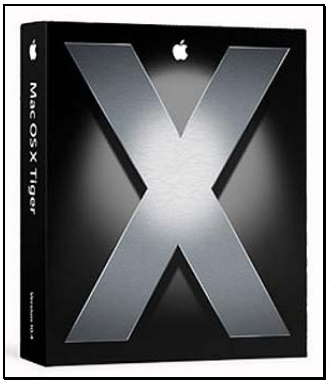
Ke zpracování této kapitoly jsem využíval jak svých teoretických a praktických znalostí, tak i externích zdrojů. Velmi se mi osvědčila zejména Wikipedia – otevřená internetová encyklopedie, kterou aktualizují a doplňují nadšenci z celého světa. Po ověření informací v ní obsažených na více místech ji považuji za vynikající zdroj informací. Navíc vzhledem k tématu mi její použití připadá velmi vhodné.

1.1 Počítačový program

Počítačový program je zaznamenaný postup realizace zadané úlohy. Co to znamená? Je to v podstatě systém, který na základě nějakých vstupních dat vrací nějaká data výstupní. Obvykle je počítačový program napsán v některém z programovacích jazyků[1], kterému počítač rozumí, případně může být napsán i ve strojovém kódu[2]. Samozřejmě by mohl být program realizován i jiným způsobem, například přímo pomocí elektronických obvodů (myčka nádobí). Počítačové programy bývají označovány také jako počítačový software (zkr. SW) [22].

Počítačový SW je nedělitelným doplňkem hardwaru (HW). HW je technické vybavení, na kterém jsou počítačové programy provozovány, případně se může jednat i o různé periferie či doplňky potřebné k běhu počítače samotného. Počítačový SW se dělí na dvě hlavní skupiny. Těmi jsou systémový a aplikační SW. Do první skupiny spadají programy sloužící primárně k obsluze HW a zajišťují běh počítače na těch nejnižších úrovních. Aplikační SW je potom v podstatě nadstavbou systémového SW. Slouží pro zpracování konkrétních úloh, je to ta část softwaru, kterou obsluhuje naprostá většina uživatelů. K jeho provozování zpravidla nejsou potřebné žádné další znalosti HW počítače či systémového SW.

Systémový software se dále dělí na dvě části. Tou první je firmware, což je vlastně software, který je napevno zabudován v HW a má velmi omezené možnosti editace. Obvykle to bývají velmi malé programy, které slouží k základní obsluze HW. Příkladem budiž například BIOS (Basic Input-Output System) v ROM (Read-Only Memory) počítače. Druhou částí systémového SW je potom operační systém (MS Windows, Linux, MacOS X…). Operační systém je v podstatě sadou programů, které slouží k zajištění co nejefektivnějšího běhu HW. Pro uživatele je důležitá zejména funkce zabezpečení běhu a podpory pro aplikační SW.



zdroj: www.apple.com

MAC OS X – příklad systémového SW

Aplikační software je programové vybavení, které slouží a je navrženo již pro nějakou konkrétní úlohu, nějaký konkrétní problém, který je třeba s jeho pomocí vyřešit. Spadá sem

[1] Programovací jazyk – komunikační nástroj mezi programátorem a počítačem. Slouží ke psaní počítačových programů. Patří mezi ně například C++, Python, Java, Assembler a řada dalších. V průběhu let prošly dlouhým vývojem a zjednodušením.
[2] Strojový kód – je to zápis instrukcí pro procesor, provedený pomocí čísel. Dříve se používal i k programování. Pro laika je dost složitý.

naprostá většina programů, které většina z nás denně používá a má je nainstalovány na svém počítači. Jedná se o různé databázové systémy, kancelářské aplikace, internetové prohlížeče, e-mailové klienty, přehrávače multimédií, hry, grafické editory a mnoho dalších.

1.2 Softwarové licence

Každý program, který je dostupný k použití na počítači, byl samozřejmě někým napsán, chcete-li vyroben, a dotyčný autor pak má možnost zvolit si, jakým způsobem bude s jeho produktem dále nakládáno. Zda jej bude nabízet ke komerčnímu prodeji, zda si jej ponechá jen pro vlastní potřebu, zda bude distribuován zdarma či bude vydělávat systémem internetové reklamy a tak dále. Každý výrobce softwaru se může svobodně rozhodnout, jaký typ licence pro svůj produkt použije. Volba samozřejmě závisí hlavně na tom, o jaký typ programu se jedná, a zároveň i na osobě výrobce. Je pravděpodobné, že komerční výrobce bude distribuci pod bezúplatnou licencí používat podstatně méně než nadšený amatér. Naopak začínající vývojář, který tvoří jednodušší aplikaci, asi nebude její rozšíření podporovat distribucí za úplatu a bude program nabízet spíše zdarma. Stejně tak lze jen těžko očekávat, že náročné grafické aplikace budou distribuovány zdarma. To se dá čekat spíše čekat u nějakých jednodušších utilit.

1.2.1 Přehled softwarových licencí

Nejprve je potřeba odlišit od sebe dvě základní filozofie šíření počítačových programů. Jedná se v prvé řadě o SW komerční, který si na svůj provoz a další vývoj vydělává prodejem komerčních licencí. Na opačné straně stojí tzv. svobodný SW, který není šířen za úplatu. Na svůj provoz si vydělává různými dalšími cestami, je často podporován skupinou nadšenců. K tomu, aby ho bylo možno legálně použít, není potřeba si kupovat nějakou licenci. Dá se zpravidla stáhnout zdarma z internetu a lze ho volně dále šířit. Mezi těmito dvěma konci se nachází řada „hybridních“ licencí, které jsou šířeny vlastně zdarma, ale na svůj provoz si vydělávají pomocí reklam, nebo je jejich funkčnost omezena a pro plné funkce je třeba připlatit.

Adware: Jsou to programy, které svým autorům vydělávají na principu prodeje reklamního prostoru. Jde o produkty znepříjemňující práci zobrazováním reklam. Ty mohou mít různou podobu a různý stupeň agresivity – od běžných bannerů až po neustále vyskakující pop-up okna[3]. Často se jedná o programy, které jsou spojeny s vývojem nějaké freeware aplikace a vydělávají tak na její další vývoj. Zpravidla nejsou pro uživatele nebezpečné [1].

BSD licence: Jde o jeden z druhů licencí pro svobodný software. Patří mezi nejsvobodnější varianty licencí. Umožňuje volné šíření licencovaného obsahu, přičemž vyžaduje pouze uvedení jeho autora a informace o licenci společně s upozorněním na zřeknutí se odpovědnosti za dílo. Pro legální šíření obsahu má dokonce menší nároky než níže uvedená licence GNU [5].


zdroj: wikipedia

Obr. 2 - Logo BSD - Daemon

[3] Pop-up okna – jedná se o samovolně se otvírající okna se zprávou. V případě Adware v nich zpravidla jde o reklamu.
S pop-up okny se lze často setkat i na interntu ve formě samovolně se otvírajících oken www prohlížeče obsahujících reklamu či přímo obsah další www stránky. Anglický výraz pop-up přeneseně znamená vynořit se, vyskočit.

Demo: Jedná se o omezenou verzi programu. Není to tedy plnohodnotná aplikace, ale nějakým způsobem jsou jí blokovány některé funkce. Nejčastější typy omezení jsou například nemožnost ukládání souborů, přidávání nějakého textu či znaku na pozadí (grafický software), omezení výstupních souborů maximální velikostí a tudíž kvalitou výstupu. Velmi často se tento druh licence objevuje u počítačových her. V tom případě jsou většinou hry omezeny jen na několik prvních úrovní, případně se jedná o verzi omezenou počtem spuštění nebo časově.

Donationware: Model, kdy výrobce dovoluje distribuovat plně funkční programy a žádá uživatele, aby jej podpořili finančním příspěvkem. V určité chvíli se při běhu programu objeví okno s žádostí autora o příspěvek na další vývoj programu. Bylo by možné se domnívat, že programy jsou v tom případě blízko k freeware licenci, ale tak tomu není. Tento druh licence je více podobný licenci typu shareware [9].

Freeware: Software, který je distribuován zdarma, bez nároku na odměnu. Autor si často ponechává autorská práva, případně omezuje použití SW pouze pro soukromé, nekomerční použití. Tím se liší od svobodného softwaru.

GNU GPL: Takzvaná „všeobecná veřejná licence GNU“ je licence pro svobodný software, která je jednou ze základních součástí projektu GNU. Zdrojové kódy pod GPL je možno volně upravovat a používat. Podmínkou však je, že budou-li dále šířeny, pak jedině opět pod GPL licencí. Toto šíření probíhá obvykle bezplatně, případně za nějakou minimální cenu sloužící k pokrytí distribučních nákladů. K SW pod GPL licencí musí jeho autor či ten, kdo jej upravoval, na požádání zdarma poskytnout zdrojové kódy programu [10].


zdroj: wikipedia

Obr. 3 - GNU GPL Logo

EULA: Uživatelé softwaru jsou někdy nazýváni také koncovými uživateli. V angličtině se pro ně používá název end-user. A právě s tímto označením pracuje licence, která nedovoluje volné šíření a nazývá se EULA. Znamená to End User License. Licence EULA je nejtypičtějším příkladem tzv. **proprietárního SW**. To je SW, který je šířen za úplatu a jeho zdrojové kódy nejsou uživateli k dispozici [26].

Open source: Počítačový software s otevřeným zdrojovým kódem. Otevřenost v tomto případě znamená, že je program dostupný jak z technického hlediska (kód programu), tak z právního hlediska. Jde o licenci, která při dodržení jistých pravidel umožňuje uživatelům program užívat, upravovat či prohlížet jeho zdrojový kód [18].

Public Domain: Autor díla se rozhodl, že dovolí svoje dílo volně užívat, bez nároku na další ochranu díla. Znamená to tedy, že se nebude domáhat svých práv.

V právním systému ČR se svých autorských práv nikdo zříci nemůže. Může jedině veřejnosti nabídnout bezúplatnou licenci [35].

Shareware: To je SW, který má kdokoliv možnost stáhnout si z internetu a užívat jej. Toto použití je však pouze zkušební. Po uplynutí lhůty je třeba program si buď zakoupit, nebo jej přestat užívat.

Trial: Podobné jako shareware. Rozdíl bývá v tom, že shareware obvykle po uplynutí doby nepřestane fungovat, trial verze často po uplynutí lhůty již nelze spustit.

Dalšími typy licencí jsou například: Cardware, DJB, IPL, LGPL, VIT License, MPL, NPL, Orphanware, PDL, PHP License, SCSL, SISSL, SPL a Vim's licence [29].

1.3 P2P

P2P neboli „peer to peer“ (v překladu *rovný s rovným*) je způsob, kterým mezi sebou uživatelé sdílí svá data. Zpravidla se tak děje za pomoci programů, kterým se říká P2P klienti. Uživatelé si program nainstalují, zprovozní a pak už jen označí, jakou část svého disku chtějí sdílet. Ostatní uživatelé P2P klienta mohou nahlížet do složky, kterou uživatel nasdílel, a stahovat si z ní data. Velkou devizou tohoto systému sdílení dat je to, že data nikde neleží. Nenacházejí se na nějakém veřejném místě. Každý uživatel má část nasdílených dat na svém počítači. Když se však připojí stovky, tisíce či desetitisíce uživatelů, tvoří objem nasdílených dat desítky či stovky terabytů[4]. Pro ty, kdo bojují proti nelegálně šířeným programům, jsou P2P systémy velkým problémem. Protože data leží u uživatelů doma, je třeba postihovat spíše provozovatele systému. Zastavit všechny uživatele je totiž nemožné. Asi nejdůležitějším mezníkem v P2P systémech byl Napster. Jednalo se o program na sdílení MP3 souborů. Ve své době byl velice populární. Po čase bylo jeho provozování napadeno u soudu a byl zakázán. Nahradily ho však desítky jiných, mnohdy důmyslnějších programů. Tentokrát však už neslouží jen ke sdílení MP3 souborů, ale veškerého obsahu. Napster se později vrátil v oficiálnější podobě a dnes nabízí legální obsah za úplatu.

1.4 Torrent

Torrent je soubor, který se používá pro stahování dat z internetu. Jedná se o internetový protokol, tedy jakási pravidla pro výměnu informací mezi dvěma počítači. Zjednodušeně jde o to, že v *.torrent* souboru jsou uloženy informace o souboru. Například jeho velikost, odkud stahovat či na jaké je rozdělen části. Když je tento soubor stažen do počítače, je možno pomocí programu (např. BitTorrent) soubor stahovat od dalších uživatelů, kteří jej mají v počítači a sdílí jej. Stahování neprobíhá ze serveru, ale z počítačů uživatelů. Každý soubor je rozdělen na části a uživatelé mezi sebou navzájem sdílí a stahují tyto části. Jakmile mají všechny části, soubor je kompletní a uživatel ho může používat. Systém je výhodný pro velmi aktuální či populární data (nová hudba, film…).

[4] 1) 1 TB (terabyte) = 1.000 GB (gigabyte) = 1.000.000 MB (megabyte) = 1.000.000.000 kB (kilobyte) = 1.000.000.000.000 bytů
Jen pro úplnost: 1 byte se skládá z 8 bitů přičemž 1 bit je základní jednotkou užívanou v oblasti výpočetní techniky.

1.5 Crack

Crack je něco, co uživateli dovolí používat program, i když nemá jeho platnou licenci. Zpravidla zabrání programu v detekci originálního DVD v mechanice či kontrolování licenčního čísla. Například u PC her se crack distribuuje rovnou s instalačním diskem hry. Znamená to tedy, že uživatel program nainstaluje s pomocí licenčního čísla z internetu a programu potom pomocí cracku zabrání v rozpoznání nelegálnosti instalace. Výrobu cracků zajišťují skupiny pirátů. Často jde o šikovné programátory, pro které je odstraňování ochrany programů vlastně koníčkem. Nicméně koníčkem nelegálním, jak vyplyne z dalších kapitol. Jen pro zajímavost, jednou z nejznámějších skupin věnujících se crackování programů (především her) je Razor1911.

1.6 Warez

Warez je nelegální obsah, který je k nalezení na internetu. Je šířen buď pomocí P2P, Torrentů nebo různých „warez“ serverů. Jde vlastně o vše, co je chráněno autorským zákonem, ale na internetu je to volně ke stažení. Nejde tak jen o počítačové programy, ale i o hudbu či video. Rozšiřování tohoto obsahu je ve většině států nelegální.

1.7 Datová média

Jen v krátkosti a pro doplnění následuje seznam datových médií, která se v dalším textu mohou objevit:

- **disketa** – dnes už zřídka používané médium. Velmi rozšířené v počátku 90. let minulého století. Z těch používanějších nejdříve kolovaly diskety 5,25“ s kapacitou 720 kB či 1,2 MB. Později se rozšířily diskety 3,5“ s kapacitou 1,44 MB. Záznam na diskety byl magnetický. Proto byly diskety poměrně choulostivé na podmínky, ve kterých byly skladovány.

- **CD** – modernější datové médium. Dnes kvůli nízké kapacitě již na ústupu. Velmi rozšířené koncem 90. let 20. století. V současnosti použití zejména pro hudební nosiče. Běžná kapacita CD je dnes 700 MB (80 min. hudby). Patří mezi optické disky a není náchylné k poškození.

- **DVD** – aktuálně asi nejpopulárnější datový nosič. Používán zejména k distribuci filmů a videa. S klesající cenou DVD přehrávačů a DVD rekordérů tento formát vytlačuje jak CD, tak i starší médium pro šíření videa – videokazetu. V současnosti jsou DVD vypalovačky běžnou součástí počítačů a tak jsou DVD velmi rozšířena právě i mezi uživateli počítačů. Běžná kapacita DVD se pohybuje od 4,7 GB (klasické DVD), přes 8,5 GB (dvouvrstvé médium) až po 17,1GB (oboustranné dvouvrstvé DVD). Patří také

- **HD DVD, Blu-ray** – nastupující formát uchovávání dat. Používá se zatím zejména pro distribuci filmů ve vysokém rozlišení. Na HD DVD disk se vejde mezi 15 a 60 GB dat, na Blu-ray disky mezi 25 a 50 GB dat. Oba typy patří také mezi optická média. Zatím nejsou moc rozšířené, ale do budoucna se mohou stát standardem místo CD a DVD. Nicméně se dá předpokládat,

že se prosadí jen jeden formát. Jak DVD tak HD DVD a Blu-ray disky obsahují ochranu proti kopírování.

Existuje samozřejmě i řada dalších datových nosičů, ale v současnosti jsou pro uživatele výpočetní techniky významné zejména tyto čtyři.

1.8 Počítačové pirátství

Je to souhrnný název pro porušování autorského práva při šíření nelegálních počítačových programů. Každý, kdo na svém počítači má nelegální software, je vlastně počítačovým pirátem. Počítačové pirátství je staré jako počítačový SW sám. Jakmile se začala výpočetní technika více přibližovat běžným lidem, začalo se šířit i počítačové pirátství. Zprvu se jednalo zejména o rozšiřování her na 8bitových počítačích, s masivním nástupem PC se počítačové pirátství týká prakticky jakéhokoliv SW či jiného elektronického autorského díla. Existuje několik druhů počítačového pirátství:

1.8.1 Pirátství koncových uživatelů (End User Piracy)

Jedná se o pirátství těch, kteří program užívají, tedy koncových uživatelů. Obvykle se spojuje hlavně s nelegálním jednáním zaměstnanců společností. Zaměstnanci porušují licenční podmínky, k jejichž dodržování se zaměstnavatel, jako nabyvatel licence, zavázal. Někdy se jedná o úmyslné jednání, někdy může jít spíše o neznalost problematiky a pravidel pro užívání SW. Zpravidla se jedná o:

- instalaci programu, ke kterému náleží pouze jediná licence, na větší množství počítačů.
- kopírování datových médií za účelem jejich neoprávněné instalace či distribuce.
- zneužívání nabídek na upgrade programu bez toho, aby uživatel vlastnil legální kopii, ke které by upgrade náležel.
- používání „školních“ verzí programu k užití v běžné komerční činnosti, aniž by k tomu byl uživatel oprávněn. Školní verze jsou vydávány pouze pro potřeby školství a v komerční sféře by neměly být používány.
- vyměňování datových médií za jiná v rámci zaměstnání či mimo něj [4], [12].

1.8.2 Pirátství prodejců (Dealer Piracy)

Jedná se o pirátské jednání firem, které se živí prodejem výpočetní techniky. Je závažnější v tom smyslu, že málokdy se dá tvrdit, že se jedná o omyl či neznalost problematiky. Prodejci výpočetní techniky by měli být natolik zkušení a s problematikou obeznámení, že prostý omyl lze obvykle vyloučit. V praxi jde o to, že prodejce počítače nahraje kupujícímu do počítače programy, ke kterým nevlastní potřebné licence. K něčemu takovému je oprávněn pouze v případě SW šířeného jako nekomerční programy. Někdy se také mluví o „nahrání na pevný disk“. To plně vystihuje podstatu. Prodejce tím obvykle sleduje vlastní pro-

spěch v tom smyslu, že chce prodávaný HW učinit pro kupujícího lákavějším. Toho docílí právě instalací programového vybavení. Na to, že k programu nedodá potřebné licence, už se jaksi pozapomene. Může dokonce docházet k situacím, že SW, který na počítače instaluje nelegálně, si nechá od kupujícího uhradit, i když ví, že dodal nelegální kopii. Toto však není problém pouze pro toho, kdo prodává HW s nelegálními programy. Problém to může bohužel být i pro kupujícího. Když totiž při koupi neobdrží žádný doklad k SW nainstalovanému v počítači a o programovém vybavení není zmínka ani na faktuře, je možné, že problémy bude mít nabyvatel. Pokud by jej přišla kontrolovat policie, nemá jedinou možnost, jak dokázat původ programového vybavení na svém počítači [4], [12].

1.8.3 Nadužívání softwaru

Jedná se o problém zejména ve firemní sféře. Uživatelé si na pracovišti pustí program ve více licencích, než je povoleno. Existují instalace programů, které umožňují používat jednu kopii programu několika uživatelům. Jsou nahrány někde na serveru a jednotliví uživatelé je odtamtud spouští. Porušením zákona však je, pokud si spustí kopii současně více uživatelů, než kolik zaměstnavatel zakoupil licencí. Řada programů je proti tomuto druhu pirátství chráněna a bez zásahu do programu (což už by samo o sobě bylo porušením zákona) není možné více licencí spustit [4], [12].

1.8.4 Padělání softwaru (Software Counterfeiting)

Padělání SW je závažný problém v tom smyslu, že se zpravidla jedná o jednoznačně ziskově orientovanou aktivitu – o výrobu neautorizovaných kopií instalačních disků. Pachatelé se snaží program napodobit tak, aby jej koncový uživatel jen těžko dokázal odhalit. Napodobují potisk datových médií, manuály, krabičky, ve kterých je vše zabaleno. Používají neoprávněně autorské známky, licenční smlouvy jsou nepravé a ani ostatní příslušenství není autorizováno výrobcem. Pro laického uživatele to může být problematické, jelikož ten nemusí někdy takový padělaný software od originálního rozeznat. Přesto se jeho používáním stává pirátem, jelikož nevlastní příslušnou licenci [4], [12].

1.8.5 Internetové pirátství (Internet Piracy)

Nakonec, ovšem nikoli významem, jsem si nechal internetové pirátství, na něž je tato práce zaměřena zejména. Je to asi nejrozšířenější druh pirátství, a pokud se budeme bavit přímo o **šíření** nelegálních programů, internet hraje v šíření nelegálních dat jednoznačně prim. Jedná se o neoprávněné stahování SW z internetu. Samozřejmě se tím nemyslí veškerý SW (ten může být i zdarma a legální), ale ten SW, který je šířen nelegálně (pirátsky). Tento druh pirátství má jedno specifikum. Ačkoli je asi nejrozšířenější, jsem přesvědčen, že na něj nemůžeme pohlížet jako na nejzávažnější. Internetové pirátství totiž má zřídka za cíl vydělávat peníze. Motivem je spíše finanční úspora. Ti, kdo SW nabízí, tak činí bezplatně. SW se na internetu šíří několika základními cestami, které jsou blíže rozvedeny v 8. kapitole. Jde o:

- Webové stránky, které obsahují buď přímo nelegální obsah, nebo na něj odkazují.
- Internetové stránky, které nabízí SW padělaný, který je šířen mimo oficiální cesty či jinak porušuje autorská práva.
- Výměnné sítě P2P, které umožňují sdílet i nelegální data [4], [12].

2 Pravidla pro používání softwaru

V druhé kapitole se blíže zaměříme na licence a pravidla pro šíření a používání softwaru. Kapitola je zpracována z mého laického pohledu a obecných znalostí. Nicméně se snažím využívat i některé relevantní zdroje k tomu, abych objasnil, jak fungují některé principy licencování počítačového softwaru. Krátce se věnuji oběma skupinám, tedy placenému i svobodnému SW. Záměrně se vyhýbám doslovným citacím z licenčních ujednání. Jsem přesvědčen, že jisté zobecnění není v tomto případě na škodu. Každá licenční smlouva se trochu liší a tak by uvádění některých pasáží nemělo příliš smysl. Každý uživatel počítače se s nějakou formou licenčního ujednání již pravděpodobně setkal a umí si udělat obrázek o tom, co obsahuje.

2.1 Co je to legální užití počítačového programu?

Zjednodušeně řečeno platí pravidlo, že legální je takové použití, které je v souladu s licencí, pod kterou je ten který program šířen. Legální je tedy jen takové použití, které se shoduje s licencí daného programu. Jakékoliv použití nad rámec licenčního ujednání je již nelegální a může být považováno za porušení autorského práva. Tím není myšleno pouze nainstalování programů, pro které uživatel nevlastní příslušnou licenci. Problém je trochu složitější. Bylo by nutné se vrátit k samotné podstatě SW. Odbočme teď stranou. Jako příklad lze uvést třeba koupi skříně. Je-li jednou zakoupena do bytu, je majetkem kupujícího a ten s ní může nakládat dle libosti, samozřejmě v rámci zákona. Může tedy zasahovat i do její fyzické podstaty, aniž by se vystavoval riziku postihu. Vymění-li jí dvířka či přidá poličky, nedopouští se majitel ničeho nekalého. Prostě provádí „upgrade“ svého majetku. Podobné to může být třeba s automobily (tuning). S počítačovými programy je to jiné. Po zakoupení licence se sice uživatel stává legálním uživatelem programu, ale nikoliv jeho vlastníkem ve stejném smyslu jako je tomu u věcí hmotných. Že je to podivné? Nikoli. Jedná se o to, že SW je ze své podstaty poněkud odlišná věc než fyzický majetek. Je to duševní vlastnictví a jako takové má právo na zvláštní ochranu. Takovou ochranou je například ochrana zdrojového kódu či ochrana samotného programu. Znamená to, že není možné si program upravovat dle potřeby a zasahovat do jeho podstaty (do jeho zdrojového kódu). Máme tedy možnost pouze mít software nainstalován na svém počítači a používat jej pouze pro práci či zábavu. Nikoli ho nějakým způsobem měnit či vylepšovat. To lze snad jen v rovině vizuální, pomocí různých „skinů“, případně v rovině funkční ve formě zásuvných modulů[5] či utilit. Takové programy však pouze rozšiřují funkčnost a nezasahují do podstaty programu.

Zakázáno je také software dále šířit, nechávat jej volně ke stažení či jinak jej distribuovat. Také je nelegální instalovat software na více počítačů než kolik licencí uživatel vlastní. Zpravidla platí, že pro každý počítač je třeba zakoupit si licenci zvlášť. Zkrátka je řada cest, jak může být autorské právo k počítačovým programům porušeno a v dalších kapitolách budou přiblíženy. Pro tuto chvíli postačí konstatování, že legální použití je takové, které je v souladu s licenčním ujednáním.

Z toho, co již bylo napsáno v předchozí kapitole, je jasné, že nakládání s programy nebude vždy stejné. Komerční programy není dovoleno bez zaplacení používat. Naproti tomu různé shareware programy je možné určitý čas používat bezplatně, jen je zakázáno je upra-

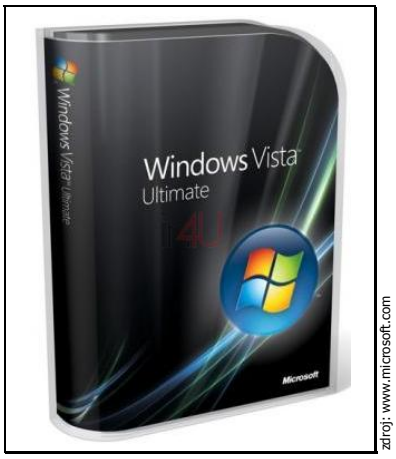
[5] 1) Zásuvné moduly neboli pluginy jsou doplňky, které přidávají programům nové funkce a rozšíření. Jsou velmi časté například u grafických či sázecích (DTP) programů.

vovat či jinak zasahovat do jejich integrity. Po určitém čase je nutné je buď přestat užívat, nebo si je zakoupit. Mimoto existuje i myšlenka takzvaného svobodného SW. Ten je možno mnohdy nejen užívat zdarma, ale také jej upravovat, vylepšovat, měnit a dále distribuovat. Platí tedy, že ne vždy může být zdánlivě nelegální nakládání opravdu označeno za nelegální. Dokud není jisté, o jaký typ SW se jedná a jaký typ licence k daném programu náleží, není možné dělat závěry o tom, zda je použití softwaru legální či nelegální. Je třeba se vždy důkladně seznámit s licenčním ujednáním, aby si uživatel mohl být jist, jak se SW smí nakládat a co už by mohlo být považováno za nelegální použití.

Druhým aspektem, který je třeba vzít v potaz při užívání SW, je, že nestačí se držet ujednání obsaženého v licenční smlouvě, ale je třeba dodržovat i základní právní normy vztahující se k tomuto odvětví. Tím je myšlen především zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) [28]. Ten vymezuje řadu pravidel a povinností, které se vztahují k užívání duševního vlastnictví, kam SW bezpochyby patří.

2.2 Placené licence

Do této kategorie spadá veškerý komerční software. Principem této licence je, že po zaplacení určité finanční částky získá uživatel právo užívat počítačový program, jehož licenci si zakoupil. Jak již bylo uvedeno dříve, získá však pouze právo užívat software, nestává se tedy jeho vlastníkem. Na toto je třeba dávat pozor, je to jeden ze základních rozdílů v porovnání s fyzickým majetkem. Majetkem kupujícího se při koupi softwaru stává pouze ono datové médium a případně připojená dokumentace a další doplňky zakoupené s programem. Program sám se však jeho majetkem nikdy nestane. Je mu přiznáno pouze právo na jeho užívání.



zdroj: www.microsoft.com

Obr. 4 – Windows Vista, zatím poslední z operačních systémů společnosti Microsoft

Například dle společnosti Microsoft[6] [16] existují dvě základní pravidla, která je třeba respektovat při nákupu a užívání počítačových programů. Tím prvním pravidlem je již výše zmíněná nutnost důkladně si prostudovat licenční smlouvu před tím, než je program nainstalován. Tato drobnost může uživatele ušetřit pozdějších nepříjemností a nedorozumění. Je to jako s kupní smlouvou. Také je nejprve nutné si přečíst všechny náležitosti, které obsahuje, a teprve potom se rozhodnout, zda na smlouvu přistoupit či nikoliv. Jde o to, aby se uživatel vyvaroval koupi „zajíce v pytli“. To se bohužel může stát, vzhledem k faktu, že někdy nemá možnost si licenční smlouvu přečíst před nákupem SW, ale až po něm, tedy těsně před instalací (shrinkwrapped software, viz. 2.5). Pokud by potom zjistil, že plánované užití SW je v rozporu s licenčním ujednáním, nezbude mu než od koupě upustit a software vrátit. Pak má možnost hledat jiný produkt podobných vlastností, jehož licenční politika mu bude více vyhovovat.

Druhým pravidlem je potom nutnost si licenční smlouvu vždy uchovat spolu s nabývacím dokladem daného produktu. Vždy může přijít situace, kdy bude uživatel povinen prokázat legalitu svého programového vybavení. Když u sebe pak smlouvu nemá, je poněkud problematické prokázat právo na užívání SW. Vhodné je také uchovávat si doklad

[6] Microsoft Software – největší SW firma na světě. Sídlí v USA ve městě Remond. Založena v roce 1975 Paulem Allenem a Billem Gatesem. Její produkty najdeme takřka na každém osobním počítači. Má dominantní postavení na trhu operačních systémů (Windows). Díky bezprecedentnímu úspěchu firmy na trhu operačních systémů se dnes Paul Allen i Bill Gates řadí mezi nejmajetnější obyvatele planety.

o koupi. Také ten je důležitým vodítkem při zjišťování, zda uživatel program nabyl legálně či nelegálně.

2.3 Bezplatné licence

Co se týká SW, který je pořízen bezúplatně a poskytuje i možnost být užíván bezúplatně, platí podobná pravidla jako pro programy komerční. Neznamená to, že pokud je program freeware nebo shareware, je možné s ním nakládat libovolně. Pravdou je, že jej lze zpravidla používat bez obav z postihu. I zde ale platí jistá omezení, stejně jako u komerčních licencí. Uživatel by si vždy měl přečíst licenční ujednání, které je společně s programem distribuováno.

Dnes už bohužel většina uživatelů pracuje tak, že licenční ujednání nečte a pouze při instalaci odklikne tlačítko „agreed“ či „accept“ bez toho, aby věnovali pozornost tomu, co se v licenčním ujednání píše. To samozřejmě nemusí vadit a u řady programů to je skutečně jedno. Zejména pokud se jedná o uživatele, který není příliš zkušený a nezamýšlí se SW nějaké širší využití. V takovém případě postačí držet se obecně známých principů pro takový druh SW. Navíc některé programy, jako je například různý shareware, uživatele obvykle upozorní na to, že doba, po kterou bylo program možno bezplatně využít, již vypršela. Pokud jej poté přestane používat, vše je v naprostém pořádku. Trial programy dokonce většinou přestanou po uplynutí určené doby pracovat automaticky.

Na druhou stranu v určitých situacích by přečtení licenční smlouvy mělo svůj smysl, a pokud tak uživatel neučiní, může se vystavit rizikům. Například ve chvíli, kdy se rozhodne užívat volně šířený program v podnikání. Řada programů totiž umožňuje jejich volné užití, ale pouze pro soukromé účely. Znamená to tedy, že pokud si dotyčný program nainstaluje doma nebo v zaměstnání, ale používá jej pouze pro soukromé účely (přehrávání hudby,…), není žádný problém. Ale pokud by takový program chtěl použít pro firemní účely, licence to mnohdy nedovoluje. Dobrým příkla-dem takového přístupu jsou dnes antivirové programy. Řada firem vyvíjejících antivirové programy, včetně největších hráčů na trhu, dnes vyvíjí vždy i verzi pro domácí užití. Bývají označeny jako „Home Edition“ a lze je leckdy najít i na různých serverech nabízejících SW ke stažení v kolonce freeware. Ale je třeba se mít na pozoru. V tomto případě se jedná o situaci, kdy je důležité si licenční ujednání přečíst. To, že program je freeware, totiž neznamená, že jej může použít každý.

zdroj: autor

Obr. 5 - www stránky programu avast! Home

Například společnost ALWIL nabízí zdarma svůj antivirový program **avast!4 Home.** Je volně ke stažení na stránkách firmy nebo například na softwarovém portálu www.stahuj.cz. Mohlo by se tedy zdát, že program může volně užívat kdokoliv. Ale tak to

není. Společnost ALWIL totiž verzi Home uvolnila pro bezplatné **nekomerční** využití. V tomto případě může tedy program užívat bezplatně fyzická osoba pro své soukromé potřeby, například nainstalovat si jej na svůj domácí počítač. Společnost ALWIL dokonce domácím uživatelům poskytuje podporu a stálé aktualizace programu zdarma. Jedná se tedy o plnohodnotný program zdarma. Ovšem chtěl-li by program využít například podnikatel a nainstalovat si jej do svých počítačů ve firmě, dopouští se nelegálního jednání. V takovém případě už se totiž nejedná o nekomerční využití. Na stránkách firmy se doslova píše: „Organizace (ani nevýdělečné) nesmějí avast! Home používat.“ [30].

Jak vidno, bezplatné licence nejsou vždy bezplatné pro každého bez omezení. Vždy je potřeba posoudit možnosti používání a šíření programů v širším kontextu. Je třeba brát do úvahy i to, kým bude program užíván a k jakému účelu. Jen takové použití je totiž v souladu s licencí a je tedy legální.

2.4 Licenční ujednání

Licenční ujednání je dokument, který je obvykle nedílnou součástí pořizovaného SW. Ať už má pouze formu jednoduchého prohlášení o tom, že SW je možno volně šířit, nebo se jedná o několikastránkový dokument, měl by být připojen u programu.

Pokud uživatel kupuje originální SW fyzicky na nějakém médiu (CD, DVD…), často je zkrácená či kompletní verze licenčního ujednání připojena v tištěné podobě (viz. 2.5). Nicméně závazná je pro uživatele zejména elektronická podoba licenčního ujednání. Tato je totiž zpravidla uživateli nabídnuta k přečtení před instalací programu. Pokud potvrdí, že chce SW na svůj počítač skutečně instalovat, potvrdí i to, že souhlasí s licenčním ujednáním. Tímto jednoduchým způsobem výrobci SW zajistili, že uživatel, který chce program užívat, musí vždy projít přes stránku s licenčním ujednáním a potvrdit souhlas s jeho obsahem.

V licenčním ujednání jsou zpravidla obsažena obecná pravidla pro užívání programu, různé ochranné známky a také případná zvláštní.

Bohužel je pravdou, že číst každé licenční ujednání při instalaci všech programů je poněkud náročné. Uživatel tak často sklouzne k tomu, že ujednání potvrdí bez toho, aby plně rozuměl jeho obsahu. Často i bez toho, aby jej vůbec četl. To je efekt přehlcení internetu množstvím informací, a uživatelé si tak vybírají jen to, co je zajímá a ostatní informace jednoduše ignorují. Lepší systém však zatím není k dispozici. Cesta potvrzení licenčního ujednání při instalaci je zdaleka nejjednodušší a nejspolehlivější z hlediska ochrany práv autora programu.

2.4.1 EULA

Asi nejrozšířenějším typem licenčního ujednání u komerčního SW je tzv. EULA neboli *End User Licence Agreement,* v překladu *Licenční smlouva s koncovým uživatelem.* Tato smlouva popisuje zákonná oprávnění týkající se používání daného programu. Například společnost Microsoft, která pod takovou smlouvou šíří svůj operační systém Microsoft Windows, dává uživateli k dispozici smlouvu nejen při instalaci systému, ale může ji také po instalaci nalézt uloženu na svém

zdroj: autor

Obr. 6 - Licenční ujednání - End User Licence Agreement

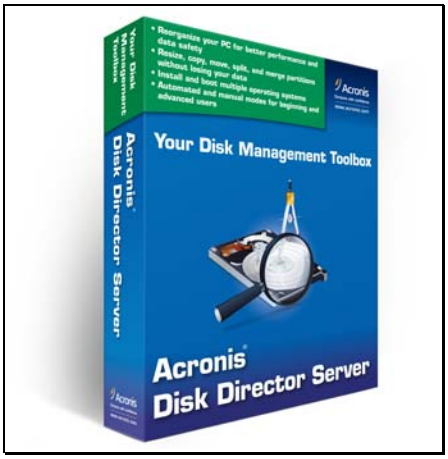
počítači (např. v souboru :\windows\system32\eula.txt). Má tedy možnost se vždy jednoduše přesvědčit, jestli smlouvu dodržuje a jaké je její konkrétní znění. Nedochází tak k tomu, že by po instalaci programu již neměl ke smlouvě přístup a neměl možnost se podívat na konkrétní podmínky, které jsou ve smlouvě obsaženy.

2.4.2 GNU GPL

Nejrozšířenější licencí používanou pro svobodný software je asi *GNU General Public Licence* neboli *Obecná veřejná licence GNU*. Tato smlouva vymezuje práva a povinnosti pro software šířený pod GNU licencí. Jedná se v podstatě o protiklad k licencím komerčním. Je-li v softwaru obsažena zmínka o tom že je šířen pod GNU licencí, pak se jeho používání řídí pravidly vymezenými v této smlouvě. Jádrem této licenční smlouvy je myšlenka svobodného software. V podstatě se jedná o povolení k tomu program volně šířit a modifikovat. Pouze vymezuje pravidla, která je nutno dodržet při takovýchto činnostech. Nejdůležitější je vždy zachovat v programu zmínku o původních autorech a záznam o tom, kým byl program modifikován a kdy [10]. GNU GPL je volně dostupná na internetu. Můžeme ji najít například na internetové adrese http://www.gnu.org/licenses/gpl.html.

2.5 Shrink-Wrap

Jak už bylo uvedeno výše, k softwaru je při koupi zpravidla připojena licenční smlouva. Když si uživatel SW koupí v obchodě, nachází se smlouva buď někde v plastovém obalu CD/DVD nebo v krabici, je-li v ní SW zabalen. Taková smlouva bývá obsáhlá a jistě pokrývá široké spektrum právních otázek týkajících se užívání SW. Ovšem je často také považována za neplatnou. Taková smlouva se někdy nazývá „shrink wrap“. Jde o smlouvu přibalenou k programu při koupi. Pokud si takový program uživatel koupí, kupuje tzv. „zajíce v pytli“. Jestliže totiž program chce, těžko mu jej někdo dovolí rozbalit před koupí a navíc už v momentu rozbalení se, dle tvrzení prodejců, distributorů SW a nyní již i autorského zákona, zavazuje k dodržování licence. Jde o tzv. konkludentní právní úkon. Mlčky tedy souhlasí se smlouvou, kterou však vlastně ani neviděl. Pokud není možné program rozbalit, těžko se mu podaří seznámit se s licenčním ujednáním, které se k používání daného programu vztahuje.



zdroj: eu.acronis.com

Obr. 7 – Třeba takto zabalený si koupíme tzv. „shrink wrapped“ software

Dostává se tak do situace, kdy má doma program, který si mohl koupit za velké sumy peněz, ale nemůže jej užívat, jelikož se ve smlouvě dozvěděl o klauzuli, která mu zabrání užívat program tak, jak by chtěl. A to je právě ten problém, proč v právních řádech některých států (Anglie, Německo, ale třeba i USA) bývají takové licenční smlouvy prohlašovány za neplatné. Prodejce či vývojář se na věc dívá tak, že pokud si uživatel program koupil v krabici, automaticky s licencí souhlasí. To je ovšem poněkud sporné. Nemůže přece automaticky souhlasit s něčím, co ani nečetl a být takovou smlouvou automaticky vázán. Z toho důvodu se takové smlouvy daří zpochybnit a prohlašovat za neplatné. I proto je důležité, aby vývojáři chtěli licenční smlouvu potvrdit ještě jednou, před instalací programu. K dodržování smlouvy se totiž uživatel zavazuje právě ve chvíli, kdy si program nainstaluje a začne používat.

V některých zemích se právníci přiklánějí k názoru, že existuje možnost SW po zakoupení do několika dní vrátit. Prodejce totiž musí kupujícímu poskytnout čas, aby se mohl se smlouvou nejdříve seznámit a teprve potom může vyžadovat jeho souhlas. Také s přihlédnutím k právnímu řádu řady zemí, ČR nevyjímaje, jsou takové „shrink wrap" smlouvy diskutabilním dokumentem. Smlouva totiž není uzavřena ze strany nabyvatele písemně, což je někdy vyžadováno (§46 odst. 4 Autorského zákona – Výhradní licence). Problém může spočívat i ve faktu, že chybí zpětné vyjádření poskytovatele licence, jestli smlouvu přijímá poté, co nabyvatel SW rozbalil a tak souhlasil se smlouvou ze své strany. Uzavřená smlouva by měla být doručena zpět navrhovateli, v tomto případě poskytovateli licence. To se ovšem při konkludentním právním úkonu neděje [2].

V novelizaci autorského zákona z roku 2006, konkrétně §46 odst. 5 a odst. 6, se zákon věnuje právě takovémuto způsobu uzavření licenční smlouvy. Odst. 5 se týká určení toho, co může být považováno za návrh na uzavření smlouvy ze strany poskytovatele licence:

„O podání návrhu na uzavření smlouvy se jedná i tehdy, směřuje-li projev vůle i vůči neurčitému okruhu osob."

Daleko více se ale tohoto tématu týká odst. 6:

„S přihlédnutím k obsahu návrhu nebo k praxi, kterou strany mezi sebou zavedly, nebo zvyklostem může osoba, které je návrh určen, vyjádřit souhlas s návrhem na uzavření smlouvy provedením určitého úkonu bez vyrozumění navrhovatele tím, že se podle ní zachová, zejména že poskytne nebo přijme plnění. V tomto případě je přijetí návrhu účinné v okamžiku, kdy byl tento úkon učiněn."

To ovšem znamená, že by se smlouva opravdu uzavírala pouze aktem rozbalení produktu. Osobně jsem však přesvědčen, že tento odstavec neřeší problém toho, že uživatel může jen obtížně souhlasit s licencí, se kterou se před koupí produktu nemohl seznámit a být jí vázán. Uzavření smlouvy samotným otevřením krabice s produktem je zkrátka problém a právníci z oboru by jistě našli celou řadů způsobů, jak takovou smlouvu později zpochybnit.

3 Problematika nelegálního využívání softwaru

Třetí kapitola je věnována analýze současné situace v oblasti nelegálního šíření a využívání počítačových programů. V této oblasti je hlavním informačním zdrojem každoročně zpracovávaná zpráva o stavu počítačového pirátství ve světě. V dalším textu si přiblížíme jak různé poměrové ukazatele o množství nelegálně využívaného softwaru, tak některé hospodářské aspekty. Čísla uváděná v podobných zprávách jsou velmi vysoká a napovídají, že ekonomické škody způsobené počítačovým pirátstvím jsou velkým problémem. Vezme-li se v potaz i další nelegálně šířený obsah na internetu, zdá se, že software může být jen špičkou ledovce.

3.1 Obecně


zdroj: wikipedia

Obr. 8 – Takto nějak vypadal v 80. letech představitel IBM PC třídy AT (Mazovia 1016)

S tím, jak se počítače začaly masově rozšiřovat na počátku 80. let, začal se více prosazovat i fenomén nelegálního šíření a užívání počítačových programů. Zprvu se jednalo spíše o okrajovou záležitost, avšak s tím, jak se počítače šířily a získávaly na důležitosti, nelegální software se začal objevovat čím dál častěji. A tak je tomu dodnes, ačkoliv se vývojáři a softwarové firmy snaží vymýšlet stále nové a nové způsoby, jak se tomu bránit. Přijímají se stále nové právní normy, které by měly pomáhat proti tomuto fenoménu bojovat. Policie a další státní orgány se zlepšují a daří se jim častěji proti takovému jednání zasáhnout. I přes toto všechno se však fenomén nelegálního šíření SW daří jen stěží omezit, natož pak zastavit. Pravdou sice je, že ve vyspělých zemích se procento nelegálního SW daří snižovat, ale naproti tomu rozvojové a různé postkomunistické státy jsou v této oblasti teprve na vzestupu a množství nelegálního SW se zvyšuje, stagnuje a nebo klesá jen velmi zvolna. Hlavním důvodem takového jednání je obvykle úspora, často nezanedbatelných finančních prostředků. Někdy se jedná o jednotlivce a nelegální SW je pořizován pro soukromé domácí použití. Jindy se jedná o velké podniky, které by na programy peníze měly, ale nepovažují za nutné si je kupovat. Stejně tak věkové složení těch, kdo používají nelegální programy, je různorodé. Od mladých lidí, i školního věku, až po dospělé. Nezáleží na pohlaví či národnosti. Počítačové pirátství je zkrátka celosvětový problém a musí jej řešit všechny státy a vlády, pokud je v jejich zemi používání počítačů běžnou záležitostí.

Díky tomu, že dnes existují organizace, které se potlačování nelegálního SW intenzivně věnují, je možno si udělat detailnější přehled o tom, jak to vlastně s nelegálním SW vypadá, kolik se ho kde pohybuje a tak podobně. I když samozřejmě každá statistika je v jistém smyslu nepřesná a údaje, které poskytují tyto organizace, nemusí úplně odpovídat skutečnosti. Realita bude v mnohých případech spíše horší než čísla, která je možné vyčíst ze zpráv těchto organizací.

3.2 Hospodářské aspekty

Začít lze například tím, co se velmi často ozývá i z médií a různých tiskových zpráv. Řeč je o škodách jako ušlý zisk, nezaplacené daně a tak podobně. Dle „VÝROČNÍ STUDIE BSA-IDC O SOFTWAROVÉM PIRÁTSTVÍ VE SVĚTĚ 2007“ [17], kterou zpracovala společnost BSA (Business Software Aliance), došlo v České republice v roce 2006 ke škodám ve výši 2,5 mld. korun (asi 90 mil. EUR). Tato částka se stále zvyšuje. Je to díky tomu, že i když se daří míru softwarového pirátství pozvolna snižovat, trh neustále roste. A pokud míra pirátství klesá jen pozvolna, ztráty z této činnosti se stále zvyšují. Například mezi roky 2005 a 2006 narostly škody o 230 mil. korun, a to i přesto, že ve stejném období klesla míra pirátství o jeden procentní bod. Tyto ztráty jsou kombinací škod způsobených jednotlivým článkům vyskytujícím se v procesu vývoje a prodeje SW.

Ztrátu samozřejmě utrpí vývojář. Tedy ten, kdo program napsal, vyzkoušel a zprovoznil. Je autorem programu a jako takový má samozřejmě nárok na **přiměřenou** odměnu. Pokud je ovšem SW pořízen nelegálně, nedostane nic. Někdo také musí SW dostat z vývojářova počítače k zákazníkům. Distributor je dalším článkem v řetězci. I on má samozřejmě nárok na odměnu za to, že se stará o distribuci softwaru k zákazníkům. Pokud si ale uživatel program stáhne zdarma na internetu, i distributor přijde zkrátka. Dalším článkem je potom stát. Ano, i když se na vývoji softwaru žádným způsobem nepodílel. Náleží mu totiž příjem z daní. Jednak se na SW samozřejmě vztahuje daň z přidané hodnoty (ať už se jmenuje jakkoliv) a potom je samozřejmě nutné uvažovat i o širších souvislostech. Stát totiž také přijde o daně firemní. Pokud firma nedostala za SW zaplaceno, sníží se jí příjmy a klesne tak částka, kterou zaplatí státu na daních. Půjdeme-li ještě dále, je možno také uvažovat o tom, že vývojář díky sníženým příjmům nemůže platit své zaměstnance tak dobře jak by v opačném případě mohl. Zaměstnanci tedy zaplatí nižší daň z příjmu a je tady další finanční škoda. A tak by se samozřejmě dalo pokračovat. Jsou zde prodejci, později technická podpora, výrobci médií, na kterých je SW distribuován a tak dále. Vezmou-li se pak v úvahu ztráty všech těchto mezičlánků vyskytujících se mezi vývojářem a konečným uživatelem SW, dají dohromady onu částku 2,5 miliardy korun. BSA také odhaduje, že pokud by se podařilo míru SW pirátství v ČR snížit v průběhu příštích 4 let o deset procent, mohlo by to přinést 2900 nových pracovních míst, posílit ekonomiku o 19,8 miliardy korun a stát by na daních v takovém případě získal další 2 miliardy korun.V souvislosti se softwarovým pirátstvím se tedy hovoří o velkých ekonomických ztrátách a i díky tomu začíná být v posledních letech bráno opravdu vážně. Vždyť který stát by se chtěl vzdávat svých daňových výnosů, pokud proti tomu může bojovat?

Nicméně je třeba uvést, že všechny tyto výpočty jsou pouze odhadem, i když kvalifikovaným, a jsou zde i jisté pochybnosti a reálnosti těchto čísel. Protipirátské organizace i státní orgány často operují s vysokými čísly jako způsobenou ztrátou. Je však třeba si uvědomit, že všechna tato čísla jsou přinejmenším nadsazená. Nelze předpokládat, že každý nelegálně instalovaný program by byl, v případě, že by nebylo možno jej získat bezúplatně, skutečně zakoupen. Kolik domácích uživatelů, kteří mají nainstalovány programy v hodnotě statisíců Kč, by si je skutečně koupili, kdyby je museli zaplatit? Dost možná by se pak skutečné ztráty pohybovaly hluboko pod odhady. Programy, které jsou pro uživatele skutečně nezbytné, jsou snad jen operační systém a nějaký kancelářský balík, ale většina ostatního SW by se, pokud by jej nebylo možné ukrást, masového rozšíření nedočkala. Nemluvě o tom, že k většině komerčních programů dnes existují kvalitní open-source alternativy. Proto je třeba brát všechna čísla zde uvedená s jistou rezervou.

V České republice mohou hospodářské aspekty nabývat ještě jiných podob. Skupina informační kriminality Policejního prezidia ČR, která se na boj s počítačovou kriminalitou specializuje, je dlouhodobě poněkud poddimenzována. A tak vyšetřování podezřelého z porušování autorských práv může trvat velmi dlouho. Pokud je Policii ČR oznámeno podezření ze spáchání trestného činu a dojde k vyšetřování podezřelého, dochází také k domovním prohlídkám či prohlídkám nebytových prostor. V takových případech se stává i to, že počítačový HW je pro podrobnější zkoumání zabaven a odvezen policií. Než je shromážděn potřebný důkazní materiál a je možno případ předat k soudu, může uběhnout poměrně hodně času. Pro podnikatelské subjekty mohou takové průtahy znamenat značnou finanční škodu. Může jít o menší firmu, která po odvezení svého počítačového vybavení zůstane v podstatě paralyzována. To by pak mělo vliv na dokončení rozjednaných zakázek a na vývoj firmy v nejbližší budoucnosti. Lze předpokládat, že firma bez počítačového vybavení nebude schopna dostát některým svým závazkům. To může v důsledku vést ke ztrátě zákazníků. Následně se pak projeví i škody finančního rázu. Pokud by vyšetřování trvalo velmi dlouho a firma při zabavení počítačového vybavení přišla o zásadní část svých pracovních prostředků, mohlo by jít o škody poměrně vysoké. Vyvstává tedy otázka, zda ekonomická škoda způsobená vyšetřováním firmy nemůže mít na celkový ekonomický užitek větší dopad, než porušení autorského zákona. Zde je samozřejmě řeč o drobných přestupcích spíše v rovině nepozornosti či neznalosti. A je třeba vzít v potaz, že v takových případech by Policie ČR i viník měli postupovat rozumně, spolupracovat a ukončit takový problém co nejdříve tak, aby způsobená škoda byla co nejmenší na obou stranách. Z praxe víme, že u řady firem se tak děje a obě strany se snaží vyřešit vše například mimosoudním vyrovnáním tak, aby celá kauza měla jen minimální dopad.

Přesto by se ale mohlo stát, že podezřelý prokáže svou nevinu, a přesto mu bude ze strany státních orgánů způsobena škoda. Pokud by se tak skutečně stalo, stává se vlastně „poškozeným“. V takovém případě má právo žádat o náhradu škody, která mu byla způsobena. Žádat o náhradu škody může v souladu se zákonem č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem. Ten upravuje odpovědnost za škodu při výkonu veřejné moci. Pokud by proti jednotlivci či firmě bylo zahájeno trestní stíhání ve věci nelegálního šíření či užívání nelegálních programů a obviněný prokázal svou nevinu, může u příslušného státního orgánu (Ministerstvo spravedlnosti…) žádat o přiměřené zadostiučinění. Samozřejmě takový postup je omezen v řadě bodů a musí být splněny některé podmínky, aby bylo možno o náhradu škody usilovat. Obecně však lze říci, že pokud jednotlivec či firma jsou vyšetřováni a případně i obviněni z nelegálního šíření či užívání počítačových programů a je prokázána jejich nevina, mají právo se domáhat na státních orgánech náhrady případné škody. Může jít jak o škodu majetkového, tak i nemajetkového charakteru. Zejména se však jedná o náhradu ušlého zisku, mzdy či nákladů řízení. Pokud příslušný státní orgán náhradu škody přizná, je povinen náhradu škody provést do šesti měsíců od uplatnění nároku. Pokud se tak nestane, může se poškozený domáhat náhrady škody u soudu.

Pokud by škodu způsobila Policie ČR již v průběhu vyšetřování, řídila by se náhrada škody také částečně podle zákona č. 283/1991 Sb., o Policii České republiky. [24]

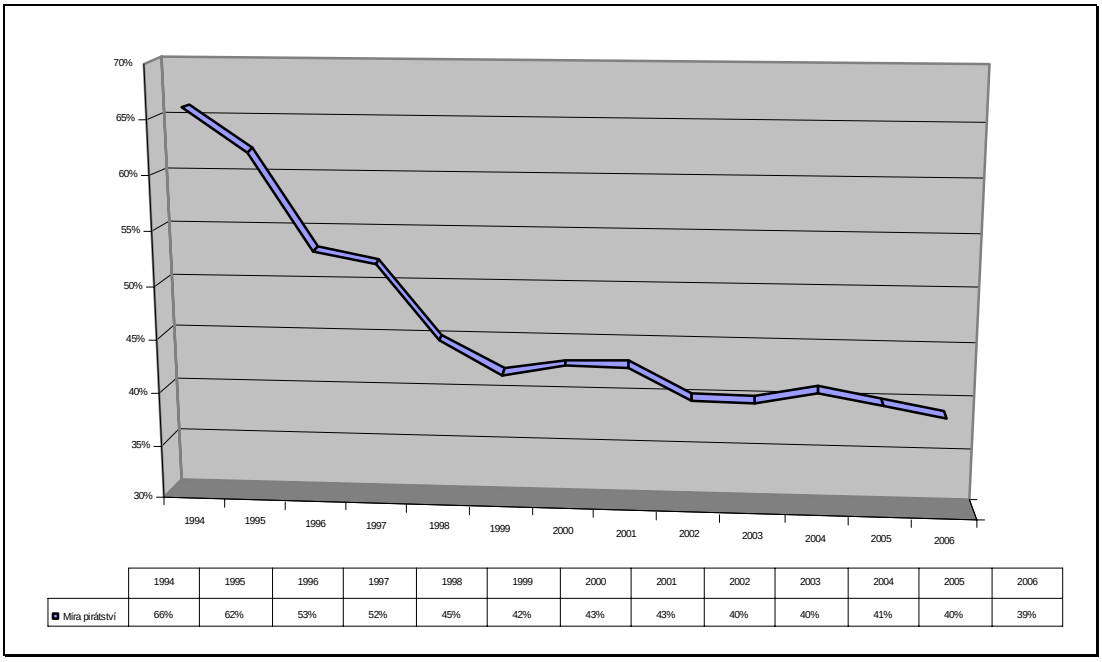
3.3 Stav v České republice

Jak už bylo zmíněno, softwarové pirátství způsobilo ekonomice České republiky v roce 2006 škody ve výši 2,5 miliardy korun. Toto všechno při míře softwarového pirátství ve výši 39 %. To znamená, že 39 % veškerého softwaru nainstalovaného na počítačích v České republice je nelegálního původu. Ačkoliv se to může zdát jako překvapivá skuteč-

nost, Česká republika se s takovouto mírou softwarového pirátství řadí na přední místa ve světě. Nikoliv v negativním slova smyslu, ale v tom pozitivním. Zařadila se totiž mezi 20 zemí s nejnižší mírou softwarového pirátství na světě. Vděčí za to zejména stále se zlepšující ochraně duševního vlastnictví v ČR. Stav se zlepšuje hlavně ve středních a velkých firmách, kde dříve bylo SW pirátství běžnou praxí. Navíc nejčastějším prohřeškem není opatřování si softwaru někde pokoutně, ale píše instalování více kopií programu, než kolik má firma zakoupeno licencí. V sektoru domácností se naopak míra softwarového pirátství zvyšuje. Důvodem je zejména dostupnost kvalitních HW prostředků, které se dají k takovému účelu použít. Řeč je zejména o kvalitních počítačích s rychlým připojením na internet. Internet je dnes největší a takřka nevyčerpatelnou zásobárnou softwaru. Nejen toho legálního, ale i toho, který by se takovou cestou k lidem vůbec dostat neměl. Často si tak uživatelé pořizují SW, který je profesionální a velmi drahý. Přitom výrobci často nabízí zjednodušené „light“ verze těchto programů, které by běžnému uživateli stačily a nestojí tolik peněz. Ale jak se říká – „příležitost dělá zloděje“.

Uvažuje-li se celý trh s pirátskými SW produkty dohromady, pak bezesporu nejčastěji šířenými nelegálními programy jsou různé kancelářské balíky, antivirové programy, grafické programy, hry a samozřejmě to základní, co v počítači bývá – operační systémy. Co se týče firem, k nejpoškozovanějším patří logicky největší hráči na trhu. Jedná se o společnosti Microsoft, Adobe, Symantec či Autodesk.

Od roku 1994 se podařilo v Česku snížit míru softwarového pirátství ze 66 % na již zmíněných 39 %. Detailnější vývoj trendu je vidět v grafu č. 1.



	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Míra pirátství	66%	62%	53%	52%	45%	42%	43%	43%	40%	40%	41%	40%	39%

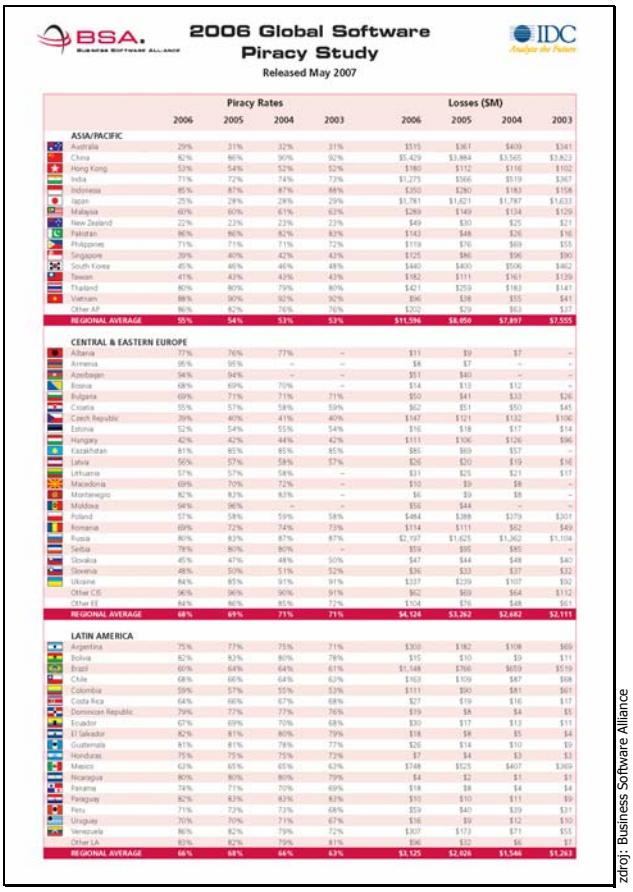
zdroj: autor

Graf 1 – Vývoj míry softwarového pirátství v České republice

To je velmi dobrý výsledek a svědčí o tom, že i v této oblasti se už Česká republika řadí mezi civilizované a vyspělé státy. Jak bude uvedeno dále, existuje řada států větších a vyspělejších, které mají se softwarovým pirátstvím výraznější problémy.

3.4 Stav ve světě

Míra softwarového pirátství se nesleduje jen v České republice, ale je sledována po celém světě. Je tak možné se dozvědět, že v Evropské unii se míra SW pirátství pohybuje kolem 35 %. Přesněji řečeno v roce 2005 byla na úrovni 36 %, o rok později klesla na zmíněných 35 %. Vyplývá z toho tedy, že ČR je jen lehce pod Evropským průměrem. Nicméně i tak se pohybuje ve výsledcích nad řadou evropských zemí. Horší výsledky vykazují například Francie (45 %), Slovinsko (48 %) nebo Itálie (51 %). Daleko horšími výsledky se pak mohou „pochlubit" nové členské země EU Rumunsko a Bulharsko. Míra softwarového pirátství tam dosahuje vysokých 69 %. To znamená, že více než dvě třetiny SW instalovaného na počítačích v těchto zemích nejsou legální.



zdroj: Business Software Alliance

Obr. 9 - 2006 Global Software Piracy Study

Celosvětově se míra SW pirátství pohybuje ve stejných či velmi podobných hladinách jako v EU. Poslední 3 roky se stabilně drží na 35 %. Nedochází tedy k růstu, ale na druhou stranu ani k výraznějšímu zlepšení. Pokud bychom svět rozdělili do regionů, tak nejlépe je na tom jednoznačně Severní Amerika s 22 %. Naopak nejhůře je na tom střední a východní Evropa se 69 %.

Jak už bylo uvedeno, ČR patří k nejlépe hodnoceným zemím světa. Konkrétně se řadí na 19. místo. Nejlepší výsledky vykazují Spojené státy (21 %), Nový Zéland (22 %), Japonsko (25 %), Dánsko (25 %) a další Evropské státy. Naopak k nejhorším hříšníkům patří státy východní Evropy a Afriky. Konkrétně se jedná o Arménii (95 %), Moldavsko (94 %), Ázerbajdžán (94 %) či Zimbabwe (91 %).

Co se týče ekonomických škod, na přední místa se řadí samozřejmě největší ekonomiky světa. Konkrétně Spojené státy s 7,28 mld. USD, Čína s 5,43 mld. USD, Francie 2,67 mld. USD a Rusko s 2,2 mld. USD. Z regionů jsou největší škody způsobeny v Asii a Pacifiku a činí vysokých 11,596 miliard dolarů. Celosvětově se pak způsobené ekonomické škody odhadují na 39,756 miliard [17].

3.5 Trendy

V naprosté většině sledovaných států se stav v oblasti softwarového pirátství zvolna zlepšuje a míra pirátství tam klesá. Výjimku tvoří jen několik států, ve kterých je trend opačný (Pakistán, Bolívie, Venezuela…). Pokud ovšem jde o konsolidované údaje za regiony či celosvětově, jedná se bez výjimky o zlepšující se trend. Tedy alespoň pokud jde o relativní míru softwarového pirátství. Trend u ekonomických škod je naprosto opačný. Jedná se zde

o velmi výrazný nárůst. I přes neustálý boj proti softwarovému pirátství a snahám vlád a organizací o jeho omezení se jedná za poslední 4 roky o nárůst o více než 10 miliard dolarů. Ještě v roce 2003 byly škody nižší než 30 miliard, konkrétně 28,8 mld. USD. Tento fakt je způsoben zejména tím, že trh softwarových produktů vytrvale roste a proto pozvolný trend poklesu míry softwarového pirátství nemůže kompenzovat narůstající ekonomické škody. V nejbližších letech se tento trend pravděpodobně nezmění. Trh softwarových produktů má stále růstový potenciál a to, že by míra softwarového pirátství začala klesat nějakým velmi výrazným tempem, se čekat nedá. Růstový potenciál trhu SW produktů leží v méně rozvinutých zemích. Největší potenciál leží pravděpodobně v Číně. Tam je poměrně malá vybavenost výpočetní technikou a proto i nízká potřeba SW produktů. Pokud se čínské domácnosti a firmy vybaví vyšším množstvím počítačů, bude nutně růst i potřeba SW vybavení. Jestliže míra pirátství nějak výrazně nepoklesne, dá se očekávat, že ekonomické škody porostou velmi rychle a brzy obsadí Čína ty nejvyšší příčky na světě. Dalšími státy, které v oblasti ekonomických ztrát budou hrát v budoucnu prim, jsou nepochybně třeba Indie, Rusko a další země Jihovýchodní Asie [3].

4 Právní normy vztahující se k nelegálnímu šíření softwaru

Tato kapitola se pokusí přiblížit některé pasáže zákonů, které se mohou týkat nelegálního šíření a užívání počítačových programů.

4.1 Právní normy týkající se nelegálního softwaru

Samozřejmě že softwarové pirátství není jen monitorováno a nejsou jen zpracovávány tiskové zprávy. Proti softwarovému pirátství se také bojuje. Hlavním prostředkem boje jsou kvalitní zákony, které upravují práva a povinnosti autorů a uživatelů počítačových programů.

Mimo to, že užívání každého programu se řídí licencí, se kterou před instalací programu musel uživatel souhlasit, existují také obecné právní normy, které se k počítačovému pirátství vztahují a které upravují nakládání s počítačovým SW. Tím hlavním je v České republice takzvaný autorský zákon. Přesněji řečeno zákon č. 121/200 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů. Tento zákon upravuje autorská práva obecně a ochrana v oblasti počítačových programů není hlavní náplní tohoto zákona. Nicméně je jeho součástí a většina obecných ustanovení se týká taktéž počítačových programů. Novely provedené zákonem č. 216/2006 Sb. byly dokonce zaměřeny zejména na počítačové programy a jejich ochranu z hlediska autorského práva. V zákoně tak je možné najít řadu zmínek o počítačových programech. Některé části zákona si přiblížíme.

V §2 odst. 2 najdeme definici počítačového programu jako autorského díla:

„Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným. Jiná kritéria pro stanovení způsobilosti počítačového programu a databáze k ochraně se neuplatňují. Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické.“

Tento odstavec tedy říká, že pokud má počítačový program autora, který program vytvoří a program je jeho duševním výtvorem, lze program považovat za autorské dílo. Jako na takové se na něj poté vztahuje ochrana na základě autorského zákona.

V zákoně je upraveno také to, kdo je autorem (§5) a jaká má jako takový práva ke svému výtvoru (§11 – §27). Takže například není možné bez povolení autora počítačový program kopírovat (§13), rozšiřovat (§14), pronajímat (§15), půjčovat (§16) či s ním nakládat jiným způsobem, který by mohl poškodit autorova majetková či osobnostní práva.

Pokud už jsou autorova práva nějakým způsobem poškozena, má tento nárok na opatření, která povedou k nápravě a zadostiučinění. Autor tak má například dle §40 odst. 1 písm. c) právo na sdělení informací o původu neoprávněně zhotovené rozmnoženiny programu, o způsobu a rozsahu neoprávněného užití programu. Toto právo lze uplatnit nejen přímo proti tomu, kdo do autorských práv přímo neoprávněně zasáhl, ale i vůči třetím osobám, kterým byly rozmnoženiny určeny za účelem jejich poskytnutí. Autor má také právo na informace o osobách, které mají nebo měly neoprávněně zhotovenou kopii v držení. Autor, do jehož

práv bylo neoprávněně zasaženo, má také právo na odstranění následků zásahu do práva (§40 odst. 1 písm. d)). Sem spadá zejména stažení neoprávněné kopie z obchodování či jiného užití, zničení neoprávněně pořízených rozmnoženin, zničení či odstranění materiálů a nástrojů použitých výlučně nebo převážně k výrobě těchto neoprávněně zhotovených rozmnoženin. Zajímavým ustanovením v této části autorského zákona je §40 odst. 1 písm. f). Ten říká, že autor, do jehož práv bylo neoprávněně zasaženo, se může domáhat také *„zákazu poskytování služby, kterou využívají třetí osoby k porušování nebo ohrožování práva autora“*. Toto ustanovení tedy autorovi dovoluje požadovat po ISP[71)], a jiných zodpovědných osobách zamezení přístupu na www stránky, ze kterých se dá nelegální SW stáhnout, či přímo odstranění takových stránek z internetu.

Autor má také právo na přiměřené zadostiučinění za způsobenou nemajetkovou újmu (§40 odst. 1 písm. e)). Tohoto zadostiučinění je možné dosáhnout buďto omluvou, nebo zadostiučiněním v penězích. To zejména v případě, pokud by přiznání jiného zadostiučinění nebylo, vzhledem k závažnosti vzniklé újmy, adekvátní. Samozřejmostí je pak právo na náhradu škody a vydání bezdůvodného obohacení (§40 odst. 4). To v praxi znamená náhradu ušlého zisku ve výši odměny, která by byla obvyklá při získání licence v době neoprávněného nakládání s dílem. Výše bezdůvodného obohacení pak činí dvojnásobek odměny za získání licence, která by byla obvyklá v době neoprávněného nakládání s dílem.

Dalším zajímavým ustanovením z hlediska počítačového SW je §43. Ten je věnován technickým prostředkům sloužícím k ochraně autorských práv. Odst. 1 říká že:

„Do práva autorského neoprávněně zasáhne ten, kdo obchází účinné technické prostředky a ochrany práv podle tohoto zákona.“

V praxi to znamená, že lze postihovat i to, pokud se někdo pokouší odstranit ochranu, kterou výrobce vybavil program jako ochranu proti neoprávněnému kopírování a užití. U počítačových programů toto ustanovení může najít široké uplatnění. Je to z toho důvodu, že počítačové programy jsou proti nelegálnímu kopírování a užívání často chráněny různými technickými prostředky. Ty musí potom pirát, chce-li program nelegálně užívat, obejít či odstranit, a právě v takovém případě by mohl být obviněn z neoprávněného zásahu do autorského práva. Stejně tak se postihu vystavuje i ten, kdo pirátům poskytne nějakým způsobem technické prostředky, nebo službu vedoucí ve svém důsledku k odstranění ochranných prostředků. Zmíněnými účinnými technickými prostředky k ochraně díla se pak podle §44 rozumí:

„Jakákoli technologie, zařízení nebo součástka, která je při své obvyklé funkci určena k tomu, aby zabraňovala nebo omezovala takové úkony ve vztahu k dílům, ke kterým autor neudělil oprávnění, jestliže užití díla může autor kontrolovat uplatněním kontroly přístupu nebo ochranného procesu jako je šifrování, kódování nebo jiná úprava díla nebo uplatněním kontrolního mechanismu rozmnožování.“

Ovšem autorský zákon nepokrývá jen eventuality porušení autorského práva, ale obsahuje i ustanovení týkající se povoleného zásahu do autorského práva. Kupříkladu §46 - §55 se zabývají úpravou licenční smlouvy. Zákon v těchto pasážích upravuje druhy licenčních smluv, právo na odměnu za udělení licence, omezení licence a odstoupení od licenční smlouvy či její zánik. I tyto pasáže mohou být z hlediska problematiky nelegálního softwaru zajímavé a poskytují podklady k tomu, aby bylo možno odlišit legální použití programu od nelegálního. Například již zmíněný §46 odst. 6, který může být problematický pro „shrink

[7] ISP – Internet Service Provider neboli poskytovatel internetového připojení. Je to ten, kdo nám umožňuje připojit se k internetové síti.

wrap“ smlouvy, je smysluplným ustanovením z hlediska svobodného softwaru a GNU licencí. V tomto případě má uzavření smlouvy mlčky smysl a toto ustanovení tak odstraňuje problematické vnímání GNU licencí.

Autorský zákon také obsahuje pasáže týkající se výhradně počítačových programů. Tak je tomu například v §65 a §66. Ty jsou zaměřeny právě na počítačové programy. Je zde vymezen způsob ochrany počítačového programu. Dle §65 odst. 1 je zřejmé, že počítačový program je autorským dílem a je chráněn stejně, jako dílo literární. §66 potom upravuje omezení rozsahu práv autora k počítačovému programu. Tato část zákona odstraňuje určité nelogičnosti, které by mohly potenciálně vyplynout z chápání počítačového programu ve stejné rovině, jako například díla literární či audiovizuální. Není tak zapovězeno si například počítačový program upravovat, pokud je to nezbytné k opravě chyb (§66 odst. 1 písm. a). Je také možno pořizovat kopie programu, pokud je to nutné k plnohodnotnému užívání programu (odst. 1 písm. c). Uživatel také může zkoumat a studovat základní myšlenky a principy počítačového programu, pokud je takový uživatel oprávněn program užívat (odst. 1 písm. d). Tato pasáž dále upravuje podmínky pro pořizování kopií a záložních kopií programu.

Autorský zákon tedy obsahuje dostatečné množství pravidel a nařízení pro danou problematiku. Nemělo by tedy být problémem jasně odlišit co je legální a co již nelegální použití počítačových programů. Netýká se sice jen počítačového SW, ale i tak tuto problematiku pokrývá dostatečně.

Pokud už k porušení autorského zákona dojde, mají státní orgány v rukou ještě opravné prostředky. Porušení autorských práv totiž zakládá trestněprávní důsledky. Pokud už je osoba porušující autorská práva odhalena a případ je předán k soudu, hrozí jí trest dle zákona č. 140/1961 Sb., trestní zákon. Ten upravuje tresty v případě, že je osoba uznána vinnou z porušování autorských práv. Nelegálního užívání počítačových programů se týká zejména §152. Výše možného trestu se liší podle toho, jaké povahy bylo porušení autorských práv. Pokud se nejednalo o závažný čin, hrozí viníkovi potrestání „*odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci*“. Pokud se jedná o závažné porušení, může pachatel být potrestán „*odnětím svobody na šest měsíců až pět let nebo peněžitým trestem nebo propadnutím věci*“. Závažným porušením zákona je zde myšleno buďto, že pachatel získá porušením autorských práv značný prospěch, nebo pokud se tak děje ve velkém rozsahu. V ČR se tresty pohybují spíše na spodní hranici výše trestu a navíc často dojde k mimosoudnímu vyrovnání [28].

Částečně se problematiky postihování nelegálního šíření počítačových programů dotýká i zákon č. 40/1964 Sb., občanský zákoník. Jedná se zejména o ustanovení §420 a §451. V prvním případě (§420 a následující) jde o definování odpovědnosti za škodu. To se nelegálního šíření počítačových programů bezesporu týká. Každý takový program způsobuje v důsledku škodu jeho tvůrci, který nedostane za své dílo řádně zaplaceno. Proto je pro něj důležité, aby věděl, kdo za způsobenou škodu odpovídá. §451 a následující se pak týká podobné problematiky. V tomto případě jde o články upravující pojem bezdůvodného obohacení, opět v souvislosti s nelegálním šířením počítačových programů najde tato část zákona své uplatnění. Pokud tedy osoba v souvislosti s porušováním autorského zákona získá nějaký majetkový prospěch (například šíří nelegální kopie SW), je povinna takové bezdůvodné obohacení vydat. Vydání bezdůvodného obohacení se pak může domáhat vlastník autorských práv.

4.2 Minulost a vývoj do budoucna

V minulosti se na ochranu autorského práva příliš nedbalo. Vlastně až do konce 19. století se duševní vlastnictví v širším měřítku neuznávalo, a tak bylo běžnou praxí kopírovat a „krást“ plody duševní práce. V té době samozřejmě nešlo o kopírování hudby či literatury, nebo alespoň ne tak intenzivně jako dnes. Ukrást se však dají i jiné věci chráněné autorským právem. Tehdy to byly zejména výrobní a technologické postupy. Až 20. března 1883 byla přijata tzv. Pařížská úmluva na ochranu průmyslového vlastnictví. Ta byla později několikrát revidována a v roce 1970 vstoupila v platnost i v tehdejším Československu. Tuto normu následovaly později další, které ochranu v oblasti autorského práva různě rozšiřovaly. Tato ochrana se pak v průběhu 20. století dále zdokonalovala. Vyspělé státy samozřejmě začaly přijímat i své vlastní normy a neřídily se jen těmi mezinárodními. Dalším významným dnem je potom 15. duben 1994, kdy se Česká republika stala členem Světové obchodní organizace (WTO). Z tohoto členství totiž vyplývají také povinnosti dodržování různých dohod, které mimo jiné vyžadují i dodržování přísné ochrany autorských práv. Další zpřísnění a platnost dalších norem na Českou republiku potom čekaly v souvislosti se vstupem do Evropské unie. Ta má tradičně velmi rozbujelou administrativu a autorským právem se zabývá řada směrnic EU (91/250/EHS). Ochrana autorských práv je tedy pokryta dobře. V souvislosti se vstupem do EU se navíc Česká republika zavázala zdokonalit vymáhání práv duševního vlastnictví. Posledním článkem do skládačky je potom novela autorského zákona přijatá v roce 2006. Jedná se o zákon č. 216/2006 Sb. a jak již bylo dříve uvedeno, tato novela v některých pasážích upravuje i podmínky pro používání počítačových programů a autorský zákon celkově opět zpřísnila [15].

Takový trend se dá očekávat i do budoucna. Za vydáváním autorských děl totiž stojí obvykle velké vydavatelské společnosti, které mají dostatečnou sílu na to, aby prosazovaly stálé zpřísňování zákonů na ochranu autorského práva. Jakékoliv snížení nelegálního šíření autorských děl totiž pro ně znamená zvýšení příjmů. Tím ovšem nelze úlohu autorského práva zlehčovat. Autorské dílo si právo na ochranu zaslouží, a pokud není možné proti nelegálnímu užívání děl bojovat jinak, nezbývá než jít cestou zpřísnění legislativy a později i postihů za porušování autorských práv. Nicméně ani sebelepší zákony nezabrání porušování autorských práv. Zákony mohou pouze pomoci a mohou být jakýmsi motivem či stimulem, který může přispět k zlepšení ochrany duševního vlastnictví. To zásadní ovšem je, jak jsem přesvědčen, kultura a vyspělost národa. Je přirozené, že ve státě, kde jsou lidé ve špatné sociální situaci, nemůžeme očekávat, že se budou příliš zajímat o nějakou ochranu duševního vlastnictví. A stejně tak to souvisí i s vyspělostí kulturní. Státy s dlouhou tradicí právního státu, kde jsou lidé zvyklí dodržovat zákony a chovat se podle určitých pravidel, mají v oblasti ochrany duševního vlastnictví větší úspěchy než státy „rozvojové“. Vrátíme-li se o několik odstavců zpět, najdeme mezi státy s nejvyšší mírou pirátství státy tak trochu exotické (Ázerbajdžán, Moldávie, Arménie, Zimbabwe). Ovšem i v těchto státech se dá do budoucna předpokládat pokrok v oblasti ochrany duševního vlastnictví, i když to jistě ještě nějaký čas potrvá.

5 Odhalování nelegálního softwaru u jednotlivců i firem

Tato pasáž se pokusí přiblížit orgány, které se odhalováním nelegálních kopií počítačového softwaru zabývají. Patří sem organizace státní i nestátní. Z těch státních hraje dominantní roli samozřejmě policie. Z nestátních organizací je nejčastěji slyšet o Business Software Alliance. Zmíněny jsou také další nestátní organizace. Součástí této kapitoly je i krátký pohled na to, jak probíhá vyšetřování a případné trestní řízení, nebo jak se snaží piráti před odhalením skrývat svou identitu.

5.1 Policie ČR

Tím hlavním, kdo by měl dbát o dodržování zákona v oblasti IT, je samozřejmě policie. Bohužel Policie ČR není doposud na boj s tímto druhem počítačové kriminality zcela adaptována. V rámci organizačního členění má šíření nelegálních počítačových programů na starosti Služba informační kriminality, která působí v rámci Policejního prezidia. Ta byla zřízena někdy v roce 1999. V současné době (počátek roku 2008) je ředitelem tohoto oddělení Karel Kuchařík. Bohužel dnes již toto jediné oddělení kapacitně naprosto nedostačuje. Ke konci roku 2007 mělo pouhých 6 členů. Přitom nárůst počtu uživatelů internetu, a výpočetní techniky obecně, je enormní a proto narůstá i množství osob, které se podílejí na šíření nelegálních počítačových programů. V jediném roce se tento tým šesti detektivů potýká s několika stovkami případů.

Od počátku roku 2008 by měla vznikat jakási krajská centra, která se budou informační kriminalitou zabývat. Pokud by se podařilo pracoviště (Skupiny informační kriminality) skutečně vytvořit tak, jak bylo naplánováno, velmi by to stávajícímu týmu detektivů pomohlo. Bohužel se ukazuje, že je velmi těžké sehnat dostatek kvalitních zaměstnanců na místa detektivů. Má-li někdo vykonávat funkci detektiva v oblasti informační kriminality, musí mít nutně také nějaké znalosti z oboru. Ovšem pokud zaměstnanec má kvalitní znalosti, není pro něj problém najít si zaměstnání ve firemním sektoru za mnohem lepších platových podmínek. A pokud bude policie zaměstnávat zaměstnance s nedostatečnými znalostmi, pak funkce Služby informační kriminality samozřejmě nemůže být zcela naplněna. Na straně počítačových pirátů stojí ti nejlepší odborníci, a pokud má být boj s nimi efektivní, musí být odborníci i na druhé straně barikády. Bohužel při modelu, jakým je Policie ČR financována je dnes spíše vyloučeno, že by se do řad policie dostal dostatek odborných pracovníků. To má za důsledek také nenaplňování plánu zakládání krajských středisek boje s informační kriminalitou. Například ve Východních Čechách či na Moravě není policie vůbec schopna oddělení naplnit, případně tam přesouvá své specialisty z jiných oddělení, kde ovšem později mohou zase chybět. Bude zajímavé sledovat, jak se bude situace do budoucna vyvíjet.

Trochu nešťastné je, že při vyšetřování informační kriminality se míchají různé druhy trestné činnosti dohromady. Z praktického hlediska by bylo ideální, kdyby existovaly speciální skupiny zabývající se nelegálním SW, jiné zabývající se hackingem, krádeží dat na internetu či dětskou pornografií na internetu. Všechny tyto obory spadají pod informační kriminalitu a zasloužily by si vlastní oddělení, která by se jim mohla plně věnovat. Bohužel opět je tu otázka peněz. Státní orgány nejsou schopny potřebné specialisty získat a zaplatit. Prestiž z práce v soukromé sféře je daleko vyšší, o finančních podmínkách nemluvě. Navíc požadavky na detektivy, kteří by práci mohli vykonávat, jsou poměrně vysoké. Kromě vysokoškolského vzdělání (které ovšem nemusí být vůbec nutností k tomu, aby někdo byl IT expertem) je to i devět let odpracovaných u Policie ČR. Skloubit všechny podmínky do jedné osoby je tedy velmi obtížné. O takové místo tak projeví zájem spíše nadšenec než někdo,

kdo se chce v oblasti IT živit. Samozřejmě všichni zaměstnanci zabývající se informační kriminalitou nemusí být ti největší odborníci. Je třeba i zaměstnanců, kteří budou provádět rutinní práci. Role specialistů je však klíčová. Dokud se nepodaří Policii ČR stav zaměstnanců naplnit, jejich práce nebude efektivní. [23]

Řešením by mohlo být i využívání externích specialistů. Tzv. outsourcing funguje ve firemní sféře docela dobře, a leckdy se ukazuje, že vede i k úspoře finančních prostředků. Soukromá firma totiž může pracovat daleko efektivněji než státní úřad a navíc často dokáže daleko lépe využívat i lidský potenciál. Správnou cestou by outsourcing mohl být i v případě boje s informační kriminalitou. Na druhou stranu je jasné, že zde vyvstává řada problémů. Mnohé informace, které je nutné k usvědčení pachatele získat, nejsou na internetu dostupné veřejně a proto jejich získání je v rukou Policie ČR. Pokud by je chtěla získávat soukromá firma, může sama postupovat nezákonně. Pokud potřebné pravomoci firma dostane, existuje riziko, že tyto budou zneužity k nekalým praktikám. Nicméně i řada informací, které lze na internetu získat bez problémů a legální cestou, mohou být velmi dobrým vodítkem při vyšetřování potenciálního piráta, a pokud by se nějaká firma zabývala jejich sběrem a Policie ČR pak tyto informace využívala, mohl by to být mocný pomocník. V současné době je tedy využití odborníků spíše na subjektech, které policii podávají případy k prošetření. Prakticky je to tak, že například Business Software Alliance může mít zaměstnánu celou řadu odborníků, kteří se budou věnovat odhalování nelegálních programů. Když shromáždí určitou sadu indicií a důkazů, předají případ Policii ČR. Policie potom sice musí provést stejně své vyšetření a opatřit si své důkazní materiály, ale přesto taková činnost odborníků soukromých subjektů může pomoci.

„Externí“ znalci a experti jsou státními orgány využíváni už v dnešní době, i když v trochu jiných rolích. Neúčastní se přímo vyšetřování, ale působí jako soudní znalci. To znamená, že se vyjadřují k trestnému činu, který byl spáchán z odborného hlediska. Jedná se o různé odborníky z vysokých škol a podobně, kteří spolupracují s Policií ČR či Ministerstvem spravedlnosti. Jejich role je důležitá z důvodu poskytnutí odborných stanovisek v oblastech, ve kterých státní orgány potřebné experty nezaměstnávají. Někdy tito experti pomáhají v při dalším vzdělávání zaměstnanců Policie ČR a přispívají tak i ke zvyšování kvality lidských zdrojů, kterými státní orgány disponují. Znalci jsou jmenováni Ministerstvem spravedlnosti a jejich seznam je možné nalézt, mimo jiné, na adrese www.justice.cz.

5.2 Business Software Alliance (BSA)

BSA vznikla v roce 1998 a působí ve více než 80 zemích světa. V současné době je asi nejaktivnější organizací působící v oblasti boje proti nelegálně šířeným počítačovým programům. V minulosti byla několikrát kritizována za nevhodný způsob „propagace“ své činnosti. Jednalo se například o „udavačskou“ internetovou stránku www.zatepla.cz nebo o videozáznamy ze zinscenované razie proti nelegálnímu SW rozesílané do schránek firem. Členy BSA jsou přední světoví výrobci a distributoři softwaru. Namátkou společnosti Adobe, Apple Computer, HP, IBM, Intel, Microsoft či Quark. Společnost BSA bojuje proti nelegálnímu použití a kopírování programů členských firem v 60 zemích světa. Internetové stránky organizace lze najít na www.bsa.org [3].

Obr. 10 – Logo BSA

5.3 Česká protipirátská unie (ČPU)

ČPU byla založena v roce 1992 za účelem ochrany autorského práva a práv souvisejících s právem autorským k audiovizuálním dílům a potírání všech forem pirátství v oblasti výroby, dovozu a šíření audiovizuálních děl [7]. Jak vidno z výše uvedeného, ČPU se zaměřuje hlavně na potírání nelegálního šíření děl audiovizuálních. Počítačový software není její doménou.

5.4 The Federation Against Software Theft (FAST)

Tato organizace vznikla jako vůbec první v této oblasti. V ČR přímo nepůsobí, je aktivní ve Velké Británii. Byla založena v roce 1984 a jejím prvotním úkolem bylo prosazení počítačového SW jako něčeho, co patří pod ochranu autorského zákona. V dnešní době FAST poskytuje hlavně školení, poradenskou službu a podporu. Důležitou součástí práce je pak osvěta a také snaha prosadit co nejlepší zákony v oblasti ochrany autorského práva. Na jejích stránkách najdou uživatelé řadu užitečných informací.

Obr. 11 – Logo FAST

Dalšími zahraničními „protipirátskými“ organizacemi jsou například The Software & Information Industry Association (SIIA), Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA)…

V podstatě v každé zemi existují specializované organizace, které se ochranou autorských práv zabývají. Často ovšem nemají SW mezi svými prioritami. Počítačovými programy se zabývají zejména první dvě zmiňované organizace, částečně pak ještě SIIA.

Pokud jde o další státní organizace zabývající se protipirátskou problematikou, nejde už zpravidla přímo o aktivní zasahování proti pirátům. Příslušná ministerstva a další vládní organizace působí spíše preventivně. To znamená, že podporují různé informační kampaně, které mají lidi upozornit na rizika spojená s užíváním a rozšiřováním nelegálního SW.

5.5 Odhalování nelegálního softwaru

5.5.1 Obecně

V dnešní době, kdy většina nelegálních programů je pořízena prostřednictvím internetu, musí se výše zmíněné organizace zaměřit na získávání potřebných informací zejména právě z internetu. Není to ovšem vždy úplně jednoduché. Jelikož uživatelé mají své právo na soukromí, které stojí nad právem autorským, nemají společnosti většinou právo nějak implementovat do svých programů mechanismus, který by upozorňoval na nelegální nakládání s programem. Šlo by totiž potom o nepřípustný zásah do soukromí osob. Je ovšem pravdou, že i v této oblasti se daří firmám potírajícím počítačovou kriminalitu stále více.

V roce 2007 se objevilo hned několik případů, které dokazují, že ani internet není anonymní médium a je možné dohledat, kdo se skrývá za stránkami nabízejícími nelegální SW nebo komu patří IP adresa, na které je SW dostupný. Mediálně známý je případ mladíka, který v roce 2007 opatřil v kině nelegální nahrávku filmu Simpsonovi a tu poté nabízel ke stažení na internetu. Mladíka policie vypátrala a dostala před soud. Vyvázl s peněžitým trestem

v řádu desítek tisíc korun. Samozřejmě se v tomto případě nejedná přímo o počítačový SW, ale na druhou stranu je to ukázka toho, že většinou existuje šance pachatele najít, i když se skrývá v anonymitě internetu. Ačkoliv je pravdou, že většinou jde v takovém případě o uživatele, kteří nejsou příliš zdatní, a jedná se u nich třeba jen o jednorázovou „akci“. Pokud je někdo v oboru počítačového pirátství „profesionálem“, je šance ho v internetu vypátrat velmi malá. I když jistě ne nulová.

Ve firemním sektoru slaví firmy potírající nelegální SW mnohem větší úspěchy. Na internetových stránkách BSA tak najdeme řadu případů, kdy se podařilo odhalit firmy podílející se na nelegálním šíření počítačových programů. Firmy, které se takto dostanou k soudu, většinou končí s finančním postihem. Jsou nuceny nahradit poškozeným firmám škodu. Majitelé takových firem jsou pak většinou obžalováni z nelegálního užívání počítačových programů a taktéž se dostanou před soud. Ten sice obvykle udělí pouze podmínečný trest, ale i zde se časy mění. V dubnu roku 2007 byl majitel společnosti zabývající se prodejem výpočetní techniky odsouzen k nepodmíněnému trestu v délce trvání 8 měsíců. Jeho firma se totiž dopustila nelegálního jednání při prodeji výpočetní techniky. Do některých počítačů byl před jejich prodejem nelegálně nainstalován SW společnosti Microsoft. Firma byla taktéž odsouzena k náhradě škody společnosti Microsoft [3]. Na tomto příkladu je vidět, že v potírání počítačového pirátství se obecně přitvrzuje a je možné, že v budoucnu budou nepodmíněné tresty s kratší dobou trvání víceméně běžnou záležitostí, pokud se někdo dopustí SW pirátství za účelem vlastního obohacení, jako tomu bylo v tomto případě.

5.5.2 Skrývání identity v síti

Pokud se uživatel chce v prostředí internetu skrývat, má řadu možností. K základním prostředkům, použitelným hlavně při běžném pohybu na internetu, jsou různé „anonymizéry“. To jsou programy nebo online služby, které uživateli dovolují skrývat svou IP adresu. Je tedy těžší takového uživatele v síti identifikovat, najít místo odkud se připojuje a kdo je jeho poskytovatelem připojení či jaká je jeho skutečná identita. Příkladem online služby poskytující takové služby je *The Cloak* (z angl. cloak – plášť). Službu je možné najít na internetové adrese http://www.the-cloak.com/. Služba v praxi funguje tak, že na této stránce uživatel zadá www adresu, kterou chce otevřít. Další prohlížení internetu už pak probíhá pod skrytou identitou. Počítač je díky využití proxy serverů schován pod jinou IP adresou. Není tak možné snadno zjistit, odkud se připojuje. Samozřejmě to není nemožné, ale už toto jednoduché skrýváni identity může při hledání pirátů znamenat potíž. Nicméně v praxi se takové služby uplatní spíše při prohlížení warez serverů či stahování přímo z internetu, kde je možné zadat konkrétní www adresu anonymizéru. Samozřejmě ani tyto služby nejsou určené k porušování autorských práv. V pravidlech pro užívání je toto zpravidla výslovně uvedeno. Poskytovatel této služby zná skutečnou IP adresu uživatele a v případě porušení autorských práv by mohl s vyšetřovateli spolupracovat – skrývání identity tak uživateli není příliš platné. Podobné je to i s programy sloužícími jako anonymizéry (*VPN Anonymizer*). Sice při pohybu v síti se počítač hlásí jinou IP adresou a tak není na první pohled zřejmé, kdo se za ní skrývá, nicméně při důkladnějším pátrání se skutečná identita uživatele zjistit dá. Anonymní surfování totiž probíhá za pomoci nástrojů třetích firem a ty jsou pro piráta samozřejmě slabým místem. Pokud by tedy došlo na vyšetřování, má policie prostředky, jak si zajistit, aby mu firma poskytla uživatelovu pravou identitu, a tak jej mohou vypátrat. Samozřejmě i sama firma bude mít v takovém případě zájem na spolupráci, aby si uchovala svou beztrestnost a zabránila případným problémům se zákonem.

Ovšem jsou i výjimky, jako například program TOR (z anglického ***T**he **O**nion **R**outer*). TOR je vyvíjen jako open source a je distribuován zdarma. Po jeho nainstalování a spuštění

má uživatel možnost surfovat zcela anonymně. Systém je technicky poměrně složitý, nicméně jedná se v podstatě o připojení prostřednictvím několika uzlů, které je navíc šifrováno. Odhalení pravé identity v případě použití tohoto programu, je-li vůbec možné, by mělo být daleko větším problémem než v předchozích případech. Připojení přes TOR je opět určeno hlavně pro běžný pohyb v síti.

Pokud jde o P2P sítě, má uživatel možnost použít skrývání prostřednictvím nějakého z programů pro anonymní surfování (např. již zmíněný VPN Anonymizer), nebo může využít některý z programů zaměřených na P2P sítě. Příkladem je program *PeerGuardian 2*. Ten má sice řadu funkcí, ale jeho hlavním úkolem je skrýt identitu uživatele v sítích P2P. Program blokuje odchozí IP adresu tak, že není možné poznat, kdo se v P2P síti pohybuje. Nicméně funguje i opačně, blokuje některé nebezpečné IP adresy a tím chrání uživatele před možnými riziky z těchto adres přicházejícími. Program je vyvíjen již více než 5 let a jeho obliba je na vzestupu. Obdobou výše zmíněného programu TOR v podmínkách P2P sítí je využívání systému I2P, který je postaven na podobném principu. Vysledování uživatelů v I2P sítích je takřka nemožné (k I2P sítím také v kap. 8). [21], [33]

Skrývání pravé identity v síti internet není trestným činem. Pokud je však skrytá identita použita k páchání trestné činnosti, je v moci státních orgánů pachatele vypátrat. Vzhledem k tomu, že řadu služeb anonymního surfování nabízí soukromé subjekty, nebude pro státní orgány obtížné si potřebné informace obstarat. Pokud však je anonymní surfování použito spíše k zajištění soukromí, lze jej doporučit. Při pohybu v internetu zanechává každý uživatel řadu stop a je v jeho zájmu omezit jejich množství na minimum a redukovat hrozby plynoucí ze zneužití těchto údajů. Koneckonců svoboda je zatím jedním z nejdůležitějších atributů internetu, a pokud by ze sítě sítí vymizela, ztratí internet část svého kouzla a své využitelnosti.

5.5.3 Pátrání po nelegálním softwaru

Pokud se týká principů, jak se nelegální SW odhaluje, existuje řada cest, jak je pirát možné vypátrat. Je to samozřejmě obtížné u domácích uživatelů. Pokud se ale jedná o organizovanou činnost, situaci to ulehčuje. Lze sledovat nabídky nelegálních programů na internetu, v tisku či jinde a různými cestami pak pachatele vypátrat. Ten, kdo nabízí nelegální SW k prodeji úplatně, je většinou nucen SW někde nabízet. Není-li při tom dost opatrný, může být touto cestou vypátrán. U firem se někdy jedná i o anonymní udání z řad zaměstnanců, bývalých zaměstnanců či jiných osob. K takovému účelu měla společnost BSA jeden čas zřízenu i speciální linku www.zatepla.cz, kde mohli lidé anonymně podat „udání“ na to, že někdo používá nelegální SW. U tohoto projektu je třeba zmínit poněkud rozporuplnou morální úroveň této aktivity. Pokud má podezření například konkurenční firma, která se domnívá, že konkurence pracuje s nelegálním SW a tím si snižuje náklady a zvyšuje konkurenceschopnost, je to v pořádku. Ovšem různá udání od nespokojených zákazníků či zaměstnanců jsou jistě problémem. Je totiž velmi snadné někoho falešně obvinit prostřednictvím takovéto informační linky. Jakmile se však začne jméno dotyčného propírat na stránkách protipirátské organizace, může ho to poškodit, i když nakonec v průběhu vyšetřování vyjde najevo, že firma či jednotlivec žádný nelegální SW nepoužívá. V současné době již doména www.zatepla.cz není funkční v podobě „udavačské“ stránky a funguje jen přesměrování na stránky BSA. Tam je však možné pirátství nahlásit.

5.5.4 Vyšetřování a trestní řízení

Pokud by někdo skutečně chtěl prostřednictvím BSA nahlásit podezření z používání nelegálních počítačových programů, má možnost tak učinit například na internetové adrese http://w3.bsa.org/czechrepublic/report/. Pirátství je také možné nahlásit prostřednictvím bezplatné telefonní linky nebo prostřednictvím e-mailové zprávy odeslané na adresu BSA. Společnost informaci po jejím obdržení posoudí a zváží, zda je natolik závažná, aby pokračovala ve vyšetřování. Pokud má pocit, že informace je závažná a dostatečně podložená, může na podezřelou osobu podat trestní oznámení. Další postup je poté již věcí Policie ČR a dalších státních orgánů. BSA může dále pouze nabídnout pomoc a součinnost při vyšetřování a shromažďování důkazů.

Po podání trestního oznámení následuje tzv. trestní řízení. Trestní řízení je upraveno tzv. **trestním řádem** (Zákon č. 141/1691 Sb., o trestním řízení soudním). Ten upravuje postup jednotlivých státních orgánů při vyšetřování a případném udílení trestů. Trestní řízení má několik fází:

- **Přípravné řízení –** v této fázi je úkolem státních orgánů opatřit si potřebné důkazy proti obviněnému. Už na samotné přípravné řízení dohlíží státní zástupce. Policie ČR v případě nelegálního softwaru nejprve prověří u výrobců či distributorů SW, zda vyšetřovaná osoba má zakoupeny legální instalace. Výrobci si totiž zpravidla vedou evidenci svých zákazníků a tak je možné odhalit případné falešně obvinění dříve, než dojde k dalším krokům. Pokud se nepodaří u výrobce a ani nikde jinde dohledat doklady o legálním nabytí SW u podezřelého, musí přijít na řadu jiné cesty, například i domovní prohlídka. Policie si také může zvát osoby k podání vysvětlení apod. Pokud Policie ČR nakonec zjistí, že podezření ze spáchání trestného činu se zakládá na pravdě a podaří se jí shromáždit dostatek důkazního materiálu, může případ putovat dále. Státní zástupce podává na vyšetřovanou osobu žalobu (zahájení trestního stíhání) a případ se dostává do rukou soudů. V případě, že by se potřebné důkazy opatřit nepodařilo, skončí přípravné řízení odložením případu. Pokud by orgány činné v trestním řízení došly k názoru, že nedošlo ke spáchání trestného činu, není trestní stíhání zahájeno.

- **Předběžné projednání žaloby** – výsledkem předběžného projednání je vrácení věci k došetření, postoupení případu jinému orgánu, zastavení trestního stíhání a nebo nařízení hlavního líčení.

- **Hlavní líčení** – představuje hlavní část trestního řízení. Soud rozhoduje o vině či nevině obžalovaného. Na konci hlavního líčení dojde k vynesení rozsudku. Rozsudek má v zásadě pouze dvě podoby: vinen nebo zproštěn obžaloby. Je-li obžalovaný shledán vinným, je mu v rozsudku sdělen také trest a případná povinnost k náhradě způsobené škody. Součástí rozsudku je i odůvodnění rozsudku a poučení o opravných prostředcích.

- **Odvolací řízení** – platí, že pokud rozhodnutí soudu prvního stupně ještě nenabylo právní moci, může se kterýkoli účastník řízení odvolat. Obecně lze říci, že pokud se některá ze stran odvolá, putuje případ k projednání

k odvolacímu soudu. Ten rozsudek potvrdí, změní či zruší. Je-li rozsudek zrušen, putuje případ znovu k soudu prvního stupně.

- **Výkon rozhodnutí** – účelem výkonu rozhodnutí je uskutečnit obsah rozhodnutí, tedy povinnosti udělené soudem.

- **Řízení o mimořádných prostředcích** – takové řízení je namířeno proti rozhodnutí soudu, které již nabylo právní moci. Patří sem obnova řízení, dovolání a stížnost pro porušení zákona. [34]

Je tedy zřejmé, že trestní řízení je velmi nepříjemnou procedurou a i z toho důvodu volí řada obviněných raději cestu mimosoudního vyrovnání, zejména pokud se jedná o porušení autorských práv ve firemním sektoru.

6 Postihy za nelegální šíření softwaru

V následující kapitole se krátce zmíním o postizích za nelegální šíření počítačových programů. Kapitola je poměrně stručná, jelikož, jak vyplyne z dalšího textu, průběhy a výsledky soudních řízení s počítačovými piráty bývají velmi podobné.

Podaří-li se protipirátským organizacím odhalit někoho, kdo porušuje autorský zákon, pokouší se shromáždit důkazy, které by byly dostačující k tomu, aby Policie ČR mohla zahájit vyšetřování. Pokud Policie ČR skutečně dojde k závěru, že dotyčná osoba autorský zákon porušuje a obstará dostatek důkazního materiálu, může být taková osoba obviněna z trestného činu. Stane-li se tak, pak případ putuje k soudu a zde se rozhoduje o vině či nevině obviněného a samozřejmě o případné výši trestu. Maximální výši trestu určuje Trestní zákon a činí u provinění menšího rozsahu dva roky odnětí svobody a u škod většího rozsahu šest měsíců až pět let odnětí svobody. To říká zákon. V realitě se k takto vysokým trestům většinou nesahá. Bohužel není možné nalézt nějaký kompletní veřejný přehled o trestních řízeních v této oblasti. Ovšem po prostudování zpráv, které zveřejňuje BSA, je třeba konstatovat, že naprostá většina soudních případů končí s mírnějšími tresty. Obvykle jsou tedy viníci odsouzeni k menším trestům v řádu měsíců s podmíněným odkladem. Dále bývá uložena povinnost nahradit vzniklou škodu či uhradit ušlý zisk.

Ve snaze vyhnout se trestnímu řízení i se všemi negativními důsledky (negativní publicita, ztráta zákazníků…) se firmy mnohdy snaží dosáhnout tzv. mimosoudního vyrovnání. To spočívá v tom, že společnost se zaváže uhradit vzniklou škodu a často i zakoupit legální licence programů, které užívala nelegálně. U soudu tak skončí pouze třetina případů. Ostatní jsou řešeny právě mimosoudně. Důležité je zdůraznit, že na takovou dohodu musí vždy přistoupit poškození a také státní zástupce [3].

Pokud jde o rozdíl mezi drobnými a většími piráty, bývá zejména ve způsobené škodě. Drobný pirát chce obvykle ušetřit finanční prostředky za SW, nebo se pirátství dopustí částečně i z neznalosti nebo nerozvážnosti. Soudy k takovéto skutečnosti přihlíží a tresty pro tyto drobné piráty jsou pak nižší. Naopak pokud někdo porušuje autorské právo ve velkém, není důvod pro zbytečnou shovívavost. V takovém případě pak také soudy sahají k přísnějším trestům. Mimo nutnosti nahradit škodu tak musí zaplatit i pokutu, a navíc jsou odsouzeni i k trestu odnětí svobody, ačkoliv většinou s podmíněným odkladem. Rozdíl v přístupu k drobným a velkým pirátům je způsoben faktem, že společenská nebezpečnost konání těchto dvou skupin se diametrálně odlišuje. Zatímco drobný pirát nebývá součástí žádné komunity a SW používá jen pro vlastní potřebu a aby ušetřil nějaké finanční prostředky, druhý typ pirátů hledá v této činnosti finanční prospěch. V takovém případě je tento trestný čin kvalifikován jako trestný čin s vyšší mírou společenské nebezpečnosti a soud může uložit vyšší trest. Ten potom může být, jak už bylo dříve uvedeno, až pět let odnětí svobody. Vzhledem k faktu, že tzv. velcí piráti mají z nelegálního šíření počítačových programů často nemalý finanční prospěch, je jejich dohledávání pro protipirátské organizace hlavním úkolem.

Srovnání stavu v ČR (většinou podmíněné tresty) se stavem v jiných částech světa ukazuje, že stav je ve většině zemí velmi podobný. K nepodmíněným trestům se sahá spíše zřídka. Nejčastěji jsou prohřešky řešeny v rovině finančního zadostiučinění.

7 Ochrana proti nelegálnímu používání softwaru

Zatím byly zmíněny zejména instituce, které se snaží vyhledávat a postihovat ty, jež autorské právo už porušili. Softwarové společnosti tak vystupují jako pasivní divák, který pouze utrpí ztráty a nemá šanci do procesu zasáhnout. Tak tomu ale není. Softwarové společnosti jsou naopak tím prvním, kdo má šanci s případným porušováním autorských práv něco udělat. Samozřejmě pomineme-li to, že stát a společnost by měly působit preventivně tak, aby nikoho ani nenapadlo si nelegální SW pořídit. Softwarové společnosti totiž mají možnost do svých programů implementovat různé nástroje, které potenciálním pirátům znemožní SW nelegálně šířit a užívat, či jim toto nelegální počínání alespoň zkomplikují. Tyto nástroje ochrany proti nelegálnímu užití jsou buď hardwarové, nebo softwarové.

7.1 Hardwarová ochrana

V tomto případě je funkčnost programu vázána na přítomnost nějaké HW součástky v počítači. Bez ní není program možné spustit. Nejčastěji se jedná o tzv. HW klíče. Ty se dříve připojovaly na paralelní port počítače (LPT), dnes je nejčastějším způsobem připojení port USB (Universal Serial Bus). Hardwarové klíče se používají hlavně k ochraně drahých nebo nepříliš rozšířených specializovaných SW produktů. V minulosti se jednalo například o produkty společnosti Autodesk (AutoCAD[8]) či Quark (QuarkXPress[9]). V praxi systém funguje velmi jednoduše. Současně s programem obdrží uživatel i HW klíč. Ten má dnes často podobu „klíčenky“ (USB flash disku) a není tak problém jej umístit do portu počítače (USB). V tomto portu musí být HW klíč přítomen, kdykoliv chce uživatel program použít. Není-li klíč fyzicky přítomen v počítači, nejde program vůbec spustit. Ochrana dokonce funguje tak, že pokud je klíč odpojen v průběhu práce, program to rozpozná a ukončí se, případně zablokuje až do momentu, kdy je HW klíč zapojen zpět do počítače. Z technického hlediska je HW klíč pouze druhem paměti, ve které je uloženo licenční číslo, které se při spuštění programu kontroluje. Pokud program nerozpozná odpovídající licenční číslo, program se nespustí. Taková kontrola pak probíhá i za běhu programu. Z hlediska uživatelského komfortu je tato metoda ochrany SW trochu nepohodlná. Uživatel je nucen stále HW klíč nosit u sebe, což samozřejmě není příjemné (riziko ztráty…), nebo jej nechávat v portu trvale a tak o tento port prakticky přijít. Navíc HW klíč také není samospasitelný. Cracker, který chce takovou ochranu programu odstranit, si obvykle poradí i s HW klíčem. Nejde o to, že by fyzicky přepisoval nebo crackoval HW klíč. Spíše zabrání programu, aby vykonával onu pravidelnou kontrolu přítomnosti HW klíče, případně mu ohlásí, že klíč je přítomen, i když tomu tak není. Pak je program tzv. crackován a přístupný i bez použití HW klíče. Jedná se tedy ve své podstatě také o SW ochranu, jelikož zásahem do zdrojového kódu programu je cracker schopen ochranu pomocí HW klíče odstranit.

7.2 Softwarová ochrana

Funkčnost programu je vázána na zadání licenčního programu při instalaci. Je-li tento zadán, program normálně funguje. Pokud jej nezadáme, nedovolí nám program dokončit instalaci. Ovšem to pouze v případě, že není crackován. Potom nám dovolí se nainstalovat s libovolným číslem. Nebo jinak – na internet se dostane několik licenčních čísel a piráti je pak použijí pro svou kopii programu. Je potom tedy možné, že velké množství

[8] AutoCAD je rozšířený a poměrně drahý SW, který se používá k projektování a konstruování na počítači. CAD = Computer-aided Design.
[9] QuarkXPress – velmi populární a také poměrně drahý sázecí program. Používá se v DTP studiích. DTP = DeskTop Publishing

uživatelů užívá program pod stejnou licencí. Nicméně ani pak nemusí mít pirát vyhráno. U kancelářského, grafického a podobného SW však většinou jiná ochrana nepadá v úvahu. Uživatelé chtějí program nainstalovat a pak jej používat bez zbytečných zdržení a omezení. Je pravdou, že některé programy se ještě zpětně dotazují na heslo přes internet (QuarkXPress), ale to samozřejmě uživatele omezuje a ani dnes nemají všichni přístup k internetu. Ochrana takového SW pak spočívá hlavně v tom, že se vývojáři snaží najít co nejdůmyslnější způsob, jak program napsat tak, aby cracker nebyl schopen odstranit ochranu, kterou do programu implementovali. Trochu výjimečné jsou v tomto ohledu počítačové hry. Ty nejen že vyžadují zadání licenčního čísla, ale navíc leckdy vyžadují i fyzickou přítomnost média v mechanice. Není tak možné spustit hru, dokud není originální DVD disk v DVD mechanice. Teprve potom program běží. Jedná se tak v podstatě o několikastupňovou ochranu. Nicméně i takováto ochrana se dá odstranit, takže je možno se setkat s hrami, které jsou distribuovány přes internet zdarma, v příloze je v souboru *.txt uložen licenční klíč ke spuštění instalace a v jedné ze složek „crackovaný“ EXE soubor. Ten je už od crackera připraven tak, aby nevyžadoval přítomnost disku v mechanice. Je tak možno používat hru i bez disku. Nebo hra kontroluje nejen přítomnost dat na disku, ale i jejich integritu a správnost. Pak program neběží, dokud není vložen originální disk do mechaniky. Ovšem i tyto ochrany jsou vždy oklamány a k programu je dodáván upravený EXE soubor, který programu zablokuje funkci kontroly originálního disku v mechanice. Existuje také řada SW produktů (DaemonTools), které se samy pokouší simulovat některé způsoby ochrany originálních CD/DVD disků a neoriginální pálené disky či obrazy disků se pak při spuštění programu tváří jako originální.

SW ochranou je také mechanismus, který zabraňuje použití více kopií programu než má uživatel legálně pořízeno. Tyto mechanismy pracují pouze tehdy, jsou-li počítače připojeny na síti. To je základní podmínkou fungování takového ochranného mechanismu. Ve chvíli, kdy počítač pracuje sólo a v síti není zapojen, nemá možnost se nějak chránit a kontrolovat přítomnost dalších kopií programu. Pokud počítače na síti jsou, pak program dovolí běh jen tolika kopií, kolik má uživatel zakoupeno. Pokud se pak pokusí použít například 2 stejná licenční čísla, program to pozná. Další kopie už se na jiném počítači prostě nespustí. Program také může hlídat počet spuštěných kopií a podobně. V současnosti se dá řada programů zakoupit a používat tak, že běží na serveru a jednotliví uživatelé mají možnost si program na přeskáčku pouštět. Pouze se nesmí přesáhnout maximální počet současně spuštěných kopií.

Příkladem neúspěšného boje proti nelegálnímu kopírování disků za pomoci SW ochrany mohou být poslední novinky z oblasti ochrany datových médií. Již dříve bylo vysvětleno, co jsou disky Blu-ray a HD DVD. Jelikož tyto disky představují třetí generaci optických médií, logicky si s sebou nesou také nejvyšší úroveň zabezpečení. Jedná se o ochranu proti kopírování. K ochraně disků se používaly ochrany AACS (Advanced Access Content System) a BD+. A jak to již bývá, ani tyto ochrany neměly dlouhého trvání. Poté co se na počátku roku 2007 podařilo prolomit ochranu AACS [27], podařilo se v listopadu 2007 firmě SlySoft prolomit i ochranu BD+. Funkci na odstranění ochrany pak implementovala do svého programu AnyDVD. V současné době tak již opět neexistuje ochrana, která by bránila kopírování HD DVD a Blu-ray disků [13].

7.3 Shrnutí

Na světě je, a vždy bude, mnoho metod, jak SW chránit. Vývojáři vymýšlejí stále nové a nové způsoby. Ukrývají kontrolní mechanismy do těch částí programu, kde by je nikdo nehledal. Snaží se všemi možnými způsoby vyzrát na piráty a crackery. Dá se však předpo-

kládat, že se jim to nikdy nepodaří. Jakákoli ochrana se dá obejít. Navíc jsem přesvědčen, že v řadách crackerů jsou mnohdy lidé s širšími znalostmi než vývojáři. Najít a odstranit pak tu část programu, která se stará o kontrolu originality SW je pro ně spíše otázkou minut či hodin. Zatímco vývojáři ztratí na tvorbě ochrany programu týdny či měsíce.

Do budoucna by se pro distributory, vývojáře a prodejce SW mohl stát trumfem internet. To médium, které tolik napomáhá k šíření nelegálních programů. Je totiž možné, že v budoucnu si uživatel nekoupí celý program, ale jen jakousi uživatelskou stanici. Část kódu programu poběží na serveru výrobce či distributora a piráti tak nebudou mít možnost se k němu dostat. Pokud by se toto stalo běžnou praxí, pirátům by to opět ztížilo život. Jenže dnes takováto ochrana není možná. Ne každý má přístup na internet, a vyčleňovat takové uživatele z práva na užívání programu by nebylo fér.

8 Metody rozšiřování nelegálního softwaru

V této kapitole si přiblížíme ty nejtradičnější cesty, kterými se může k uživateli nelegální SW dostat. Nepůjde o nějakou detailní analýzu, jelikož to není účelem této práce. Jde pouze o objasnění základních principů a získání přehledu o tom, které kanály hrají při šíření dominantní roli dnes a které tuto roli hrály dříve. Celá kapitola se zaměřuje na platformu IBM PC respektive operační systémy Windows. Je tomu tak záměrně. U konkurenčních platforem a systémů nedochází k nelegálnímu šíření SW v takové míře.

8.1 Trocha historie

Je třeba si uvědomit, že problematika nelegálního šíření softwaru je stará takřka stejně jako software sám. A stejně tak, jak se vyvíjel počítačový software, se vyvíjelo i počítačové pirátství, a stejně tak se vyvíjely i způsoby, jak tento software dále šířit. Je tedy třeba se zaměřit na způsoby šíření nelegálních programů od „dřevních dob“ počítačů až do dnešních dnů, kdy se stal fenoménem internet, nejlevnější a nejjednodušší cesta, jak dostat nelegální programy k jejich uživatelům. Popis metod šíření nelegálních programů bude uveden dle časového hlediska, tak jak se tyto metody vyvíjely a jak s rozvojem počítačů přicházely stále nové a nové způsoby, jak software šířit.

8.1.1 První kroky

Počítačové pirátství existuje v podstatě od doby, kdy se začaly první počítače dostávat do domácností a kdy se začaly masověji šířit. V té době se samozřejmě ještě nejednalo o počítače řady PC, které se významněji rozšířily až později. Na přelomu sedmdesátých a osmdesátých let se v domácnostech nacházely zejména tzv. ***8bitové počítače.*** Mezi ty nejvýznamnější pak patřily počítače firem Atari či Commodore. Do těchto počítačů se data načítala z kazet podobných audio kazetám. Jak užívání počítačů, tak i případné počítačové pirátství byly spíše záležitostí nadšenců než něčím masovým. 8bitové počítače se používaly často pouze ke hraní počítačových her.

zdroj: wikipedia

Obr. 12 - 8bitový počítač Commodore 64

8.1.2 Nástup PC

Spolu s masovějším nástupem počítačů se samozřejmě začíná rozvíjet i počítačové pirátství. Počítače už v 80. letech totiž obsahují disketovou mechaniku. První diskety se sice objevily již v roce 1967, kdy firma IBM představila 14“ disketu, ale masového rozšíření se dočkala až disketa 5,25“, která se montuje do osobních počítačů od roku 1981 [8].

Dalším aspektem, který je na místě zmínit, je to, že rozvoj počítačového pirátství je spojen také s nástupem fenoménu jménem Microsoft. Firma Microsoft totiž začala prodávat operační systémy, které nebyly přímo spjaté s počítačem. Existovalo více výrobců počítačů, na jejichž strojích takový systém mohl fungovat. To bylo v opozici k filozofii firmy Apple, která od svého počátku spojila pevně HW se SW. Programy firmy Apple budou jen velmi těžko fungovat na počítači jakéhokoliv jiného výrobce. Naproti tomu u programů od firmy Microsoft nezáleželo na tom, jestli počítač vyrobila firma A či B. Důležitá byla jen správná konfigurace HW, později podpora ovladačů.

V té době byla také dost nízká úroveň ochrany SW. Diskety do počítače, ať už 5,25“ či 3,5“, šlo jen těžko chránit, takže kopírovat programy z jedné diskety na druhou bylo pro zasvěcené poměrně snadné. Ochrana SW pak spočívala obvykle pouze v zadání sériového čísla, klíčového slova z manuálu a tak podobně. To byly problémy, se kterými se musely potýkat první pirátské skupiny. Pro uživatele byl komfort při používáni nelegálního softwaru na vysoké úrovni. Díky struktuře tehdejších operačních systémů často stačilo vzít celou složku s programem, zabalit komprimovacím programem (Arj, Rar…) a kopírovat na disketu. Pak již mohla putovat za dalším uživatelem. Ten archiv pouze zkopíroval na svůj disk, rozbalil a užíval si svou nelegální kopii.

Co se týče samotného rozšiřování SW, v té době šlo často hlavně o šíření bezúplatné, přes kamarády. Zpočátku se jednalo o velmi malé programy, které se vešly na jednu, případně několik málo disket. Obvykle to tedy fungovalo tak, že se lidé domluvili mezi sebou a diskety si půjčili, případně zkopírovali. Jelikož diskety byly dost pomalé, nefungovalo příliš často ani to, že by program kontroloval přítomnost diskety v mechanice. A tak stačilo nakopírovat jej na disk a to bylo vše. Opět se zpočátku jednalo hlavně o pirátství v oblasti počítačových her. Komunita uživatelů nebyla stále příliš rozšířená a programů se masově používalo jen malé množství. Snad jen MS-DOS se v té době dal najít na většině počítačů. Samozřejmě často v pirátské, neoprávněné kopii. Postupem času se zejména počítačové hry změnily do poměrně objemných programů. Zabíraly tak i několik disket a to pirátské šíření dost omezovalo. Často se totiž stávalo, že některá z disket byla poškozená, takže se program nedal nainstalovat či nakopírovat na počítač.

8.1.3 Windows 95

Nástup Windows 95 znamenal velký rozmach počítačů. Jednalo se totiž konečně o opravdu „user friendly“ (uživatelsky přívětivé) pracovní prostředí, které se se svými okénky a grafikou uživatelům zalíbilo. Co na tom, že stabilita a funkčnost nebyly jejich silnou stránkou? Kompatibilita s HW byla špatná, systém padal a konzumoval mnoho systémových prostředků. Přesto se velmi dobře prosadil a přiblížil počítače masám.

Z pohledu nelegálního šíření počítačových programů se toho moc nezměnilo. Snad kromě toho, že začal růst velmi slušný trh. S nástupem Windows se totiž začalo objevovat stále větší množství softwaru třetích stran, což jsou samozřejmě také objekty zájmu pirátů. Také samotný operační systém byl oblíbeným cílem. Bylo tomu tak proto, že nebyl v prvopočátcích příliš levný, a tak si jej řada uživatelů pořídila jinak. Systém Win95 byl distribuován buď na FDD či CD. Byl také jedním z prvních programů masově šířených na CD. S tím je spojen nástup CD jako standardních nosičů dat. Jak už bylo uvedeno dříve, oproti disketám mají CD daleko větší kapacitu. Také nejsou tak náchylná k poškození. V polovině 90. let byly zpočátku populární tzv. games packy. Jednalo se o lisované CD, na kterém se nacházelo několik crackovaných programů, které bylo možné bez problémů instalovat a používat. K dostání byla hlavně přes inzertní média, například v Annonci. Zájemce si našel v novinách nabídku, zavolal na uvedené číslo a domluvil si schůzku. Tam pak zaplatil požadovanou cenu (několik stokorun) a CD si nesl domů. Tam si pak mohl užívat her za zlomek ceny, kterou by ho stály v obchodě. V tomto případě šlo tedy o CD lisovaná. Také programy se šířily nejprve na lisovaných CD.

Bylo tomu tak z důvodu, že vypalovačky CD (CD-R) byly zpočátku velmi drahé, takže bylo zřejmě výhodnější mít kontakt v lisovně CD a CD zkrátka vyrobit standardní průmyslovou cestou.

8.1.4 CD-R

Masový nástup CD-R mechaniky do osobních počítačů byl dalším milníkem v počítačovém pirátství. S vypalovačkou se i velké programy staly jednoduchou kořistí pro kopírování a volné šíření. Dokud byly vypalovačky drahé, šíření příliš velkých programů (kromě půjčování originálních CD) bylo poněkud nepohodlné. Jak už bylo uvedeno, programy byly velké a jedinou alternativou byly diskety. Ovšem rozšiřovat SW na několika desítkách disket je hloupost. S nástupem CD-R se situace mění. Je možné kopírovat celá instalační CD (pochopitelně po odstranění příslušné ochrany) a šířit mezi piráty daleko větší objemy dat. Pirátství ve smyslu kopírování dat SW mezi uživateli se tak stává velmi jednoduchým a už není třeba nakupovat pirátský SW od distributora přes inzerát v novinách. To stačí udělat jen jednou a pak už se disk může kopírovat dle libosti.

CD disky obsahovaly ochranu proti kopírování. Ta spočívala například v tom, že se disk tvářil, že je na něm uloženo daleko víc dat, než by se na něj fyzicky mohlo vejít. Pokud chtěl někdo takový disk zkopírovat, nešlo mu to. Vypalovací program hlásil, že se na prázdné médium nevejde. Bylo tak třeba zásahu crackera, nebo někoho jiného, kdo se s tímto problémem popere. Bylo nutno z disku odstranit mechanismus, který simuloval nerealistický objem dat. Jakmile se to povedlo, mohl se disk libovolně kopírovat od uživatele k uživateli.

8.1.5 Internet

Rozmach internetu silně ovlivnil vývoj počítačového pirátství. Nikdy dříve nebylo možné nelegální SW šířit tak rychle do celého světa. Nikdy dříve nebylo možné, aby k obsahu uloženému kdesi na disku měl přístup kdokoliv, z kterékoliv části Země.

Jaká je dnes typická cesta počítačového programu na nějaký webový prostor, kde je možné si jej volně stáhnout? Na počátku jsou originální data od výrobce. Ta se nějakou cestou dostanou k pirátské skupině. Ta obsah analyzuje a zjistí, jaké ochrany jsou v programu použity proti nelegálnímu šíření. Poté použitou ochranu odstraní a upravený obsah umístí na internet. Odtud se pak data šíří do celého světa. Je paradox, že často jsou takováto nelegální data k dispozici dříve, než je originální program vůbec uveden na trh. Tak rychlé a spolehlivé jsou zdroje pirátských skupin. Tyto skupiny však ze své činnosti nemají žádný zisk. Jde v nich hlavně o prestiž. Obsah je na internetu umístěn zdarma.

Obrovská síla tohoto média je v tom, že nelegální obsah, ať už jde o SW, hudbu či programy, nenabízí jen zasvěceným. Dnes je v silách každého uživatele takový program na internetu objevit. A pokud má i nějaké minimální uživatelské znalosti, je takový program schopen nainstalovat a používat.

8.2 Kde lze nalézt nelegální software?

8.2.1 Klasické cesty

Klasickými cestami je v tomto případě myšleno cokoli jiného než internet. Pokud se nelegální programy nedostanou k uživateli po internetu, pak se k němu dostanou 2 až 3 možnými cestami. Tou první a možná nejčastější jsou známí, kamarádi, kolegové. Zkrátka se mezi řečí dohodnou, že jeden druhému donese DVD, nebo jiné médium, s pirátskou kopií programu. Takové pirátství není provozováno za účelem dosažení zisku. Spíše svědčí o tom, že komunita drží při sobě. Neznalým uživatelům se také může stát, že si program od kamaráda nainstalují a ani netuší, že dělají něco nedovoleného. Ovšem neznalost samozřejmě neomlouvá.

Druhým způsobem, který je dnes také na ústupu, je prodej přes inzerci. Jak již bylo uvedeno dříve, v 90. letech bylo dost běžné, že se PC hry a další software nabízely v inzertních novinách. V inzerátu bylo uvedeno pár titulů, které daný distributor nabízí, či poznámka, že seznam zašle na adresu. Z takového seznamu by si pak uživatel vybíral, o co má zájem. Pokud si vybere, kontaktuje zpět nabízejícího a domluví si podmínky obchodu. Dříve lidé nebyli příliš opatrní a bylo možné si disk po telefonické dohodě vyzvednout třeba u distributora před domem. Dnes už jsou takoví distributoři mnohem opatrnější, jelikož boj proti nelegálnímu softwaru je mnohem intenzivnější. Navíc právě takoví distributoři jsou často v hledáčku příslušných orgánů. Jde totiž o skupinu, která nelegální software šíří vyloženě za účelem zisku. Nejde tedy o nadšení či nějakou kolektivní vinu typu „když ostatní, tak proč ne já“. V tomto případě jde o obchod a distributor většího kalibru si může touto nelegální činností přijít na slušný balík peněz, i když dnes je možné naprostou většinu programů nalézt v nelegální kopii i na internetu.

Třetí cesta, kterou je třeba zmínit, je trochu netradiční. Jde o nákup nelegálního SW v zahraničí, na tržnicích a podobně. I v dnešní době je stále možné koupit nelegální SW na lisovaných discích. Mnoho takového SW se k nám dostává například z Ruska, ale také z dalších zemí, kde jsou na tom s nelegálním SW ještě daleko hůře než u nás. V některých státech je opravdu možné zakoupit nelegální SW na discích a v krabičkách, které se tváří jako pravé. V takovém případě by vina neměla být kladena přímo uživateli. Samozřejmě existují lidé, kteří nakupují takový SW záměrně, ovšem mohou existovat i uživatelé, kteří zkrátka nelegální balení SW od toho legálního nepoznají. Pomine-li se faktor hazardu spočívající v tom, že někdo nakupuje SW na tržnici, může v tom být uživatel i nevinně. V těchto případech by měla vina dopadat hlavně na prodávající. Ti se mohou těžko bránit s tím, že nevěděli co prodávají. Jako prodávající si měli původ zboží ověřit. Navíc prodává-li někdo počítačové programy, měl by mít přehled o cenových relacích. Dostanou-li se k němu velmi levná CD či DVD určená k prodeji, měl by zpozornět.

Ve firmě se také může stát, že některý zaměstnanec nainstaluje nelegální SW do firemního počítače, aniž by to někdo věděl. V takovém případě je za porušení zákona odpovědný i majitel či jednatel firmy. Každý vedoucí pracovník firmy by si tedy měl vždy dávat pozor na to, co jeho správce výpočetní techniky provádí. Za jeho konání je spoluodpovědný, i když hlavní odpovědnost leží na dotyčném správci. Správce počítačové sítě by také byl pravděpodobně tím prvním, na koho by se policie při vyšetřování zaměřila.

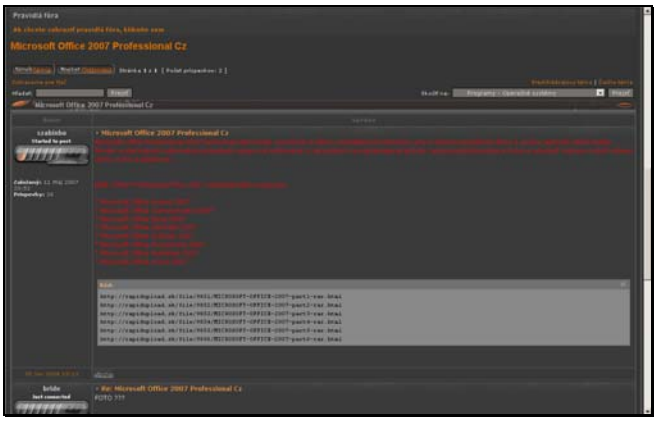
8.2.2 Internet

Internet, ten neustále omílaný fenomén. Je to nevyčerpatelná studnice softwaru, legálního i nelegálního. Na internetu sice není úplně vše, ale pokud je uživatel zkušený a má alespoň trochu představu kde hledat, s největší pravděpodobností dříve či později uspěje.

8.2.3 Warez servery

Na internetu se dá SW opatřit několika způsoby. Tím prvním a možná nejpohodlnějším jsou warezové servery. Jedná se o servery (často ve formě diskusních fór), kde uživatelé sdílí své poznatky o tom, kde se dá na internetu co najít. Ať už jde o hudbu, video, hry či plnohodnotné programy. Tohle všechno se na takovém diskusním fóru dá nalézt. Na obrázku níže je například screenshot z jednoho takového diskusního fóra. Na obrazovce jsou vidět adresy, na kterých je k nalezení pirátská kopie programu Microsoft Office 2007 Proffesional CZ. Pro zájemce z řad široké veřejnosti je postup už velmi jednoduchý. Linky,

které jsou uvedené na stránce, si postupně zkopíruje do svého webového prohlížeče, prokliká se k tlačítku download a postupně si nakopíruje do počítače všechny potřebné součásti. Pak si je na počítači spojí v jeden celek a instaluje. Licenční čísla jsou součástí archivu a nebo se obvykle dají nalézt někde poblíž www adres k downloadu. Jednoduché a funkční.



Obr. 14 – tak vypadá jeden z mnoha warez serverů

Pro uživatele může být pouze několik drobných překážek, které znepříjemňují život. První je nutnost registrace na některých serverech. Trochu to obtěžuje, ale jinak to vlastně ani taková překážka není. Co však překážkou je, je systém sdílení dat. Dnes už se obvykle nekopírují někam do webového prostoru, který se dá snadno zablokovat. Používají se tzv. úschovny. To jsou místa, kam si uživatelé mohou uložit svá data a někdo jiný si je vyzvedne. Je to výhodné zejména pokud mám data, která chci někomu doručit a jsou příliš objemná na e-mail. Bohužel tyto servery nejsou úplně nejrychlejší (pokud tedy dotyčný není placeným uživatelem). Také se stává, že některé ze serverů (oblíbený je www.RapidShare.de) nedovolují stahovat více částí programu najednou. Někdy se musí čekat před stahováním další části. Zkrátka znepříjemňují život. Pokud patří uživatel k platícím, má napůl vyhráno. Platícím uživatelům takové servery nabízí vysoký komfort. Pokud jsou však používány zdarma, je třeba očekávat obtíže, i když se jim dá předejít. Třeba používáním některého z programů, které byly přímo vyvinuty k tomu, aby usnadnily a zrychlily stahování (Universal Share Downloader…). Dalším problémem pak je to, že soubory nevydrží na „úschovnách“ věčně. To znamená, že je třeba hlídat si, aby linky, ze kterých se má stahovat, byly co nejnovější a tudíž nejaktuálnější. U starých linků se může stát, že už nebudou fungovat. Úschovna soubory po určité době zkrátka smaže.

Každopádně se tento způsob řadí k nejjednodušším, i když má svá úskalí. Je nejspíše dostupný i laikům. Není totiž nutné vlastnit nějaké speciální programové vybavení. Snad jen vyjma případů, kdy si chce uživatel stahování z úschoven usnadnit. Ovšem principielně to není nutnost.

8.2.4 P2P

Jak už bylo uvedeno v první kapitole, P2P neboli peer-to-peer je způsob spojení, při němž se jednotlivé počítače spojují přímo. Není tak třeba nějaký mezičlánek, na kterém je obsah uložen. Uživatelé sdílí data přímo ze svých počítačů a stejně tak druhá strana si data stáhne přímo z jejich disků. Takové připojení by bylo obtížné, pokud by se ke zjednodušení nepoužívaly programy, které práci usnadní. Takových programů je dnes celá řada. Jednotlivé programy si vlastně v oboru konkurují, ačkoliv mají všechny stejnou nebo podobnou funkci – výměnu jakéhokoli obsahu počítačů bez nutnosti používat nějaké další služby (Rapidshare…). Obecným principem takových programů je to, že po krátké registraci, či pouze nastavení programu (nutné pro identifikaci uživatele v síti), je možné program ihned používat. Pokud se uživateli podaří připojit, může vyhledávat, na co si vzpomene. Někdy stačí se jen připojit a program sám zajistí vyhledávání na správných místech, některé programy (DC++) ještě vyžadují připojit se k některému z jakýchsi „seznamů uživatelů“. Rozlišují se tedy centralizované (ty, které potřebují nějaký server) a decentralizované (bez centrálního serveru) sítě.

Na druhé straně musí být samozřejmě solidní partner. Může se totiž stát, že uživatelé nasdílí nekvalitní obsah (fake) a tím poškozují další uživatele. V tomto případě nejde jen o nelegální SW. Existuje také spousta dat, která jsou legální a uživatelé by si je také rádi nasdíleli. Uživatel sdílící nekvalitní obsah potom ztěžuje život všem ostatním, kteří se na síti pohybují. Někdy je totiž obtížné poznat kvalitní obsah od toho nekvalitního, i když v tomto směru již vývojáři také udělali velký kus práce.

Pro protipirátské autority je P2P jeden z nejnepříjemnějších způsobů šíření nelegálního obsahu. Je totiž obtížné uživatele odhalit a postihovat. Ze strany uživatelů se jedná také o velmi komfortní způsob získávání dat z internetu, i když vyžaduje nějaké minimální znalosti. Je třeba si nastavit správně připojení k síti a je třeba se umět zorientovat v jeho prostředí. Oproti stahování z úschoven na internetu, ke kterému stačí pouze webový prohlížeč, je to o dost složitější.

Existuje také systém I2P (Invisible Internet Project). Ten funguje na principech velmi podobných sítím P2P, ale jeho hlavní myšlenka je poněkud odlišná. Alfou a omegou tohoto projektu je vybudovat zcela anonymní síť. Na sítích P2P totiž uživatele vždy lze dříve či později dohledat. Sítě I2P naproti tomu dbají na udržení anonymity uživatelů. Data se tedy mezi uživateli vyměňují anonymně. Obsah, který je přenášen, je navíc šifrován a tak je obtížné rozeznat, zda je legální či nelegální. Bylo by ho nejprve nutné rozšifrovat.

8.2.5 FTP

FTP (**F**ile **T**ransfer **P**rotocol) servery jsou servery, které jsou primárně určeny k ukládání dat. Nejsou na nich tedy webové stránky k prohlížení, najdeme tam spíše data. FTP servery jsou tedy jednou z cest, jak se nelegální obsah šíří po internetu. Nutno říci, že nebývají přístupné široké veřejnosti. Někdy se na takový server běžný uživatel „proklikat“ může, ale není to příliš časté. FTP servery se používají spíše na sdílení obsahu mezi zasvěcenými. Na warez scéně jsou FTP servery jedním ze základních stavebních kamenů pro šíření nelegálního obsahu. Poté, co jsou programy úspěšně crackovány a je odstraněna ochrana proti kopírování, jsou data umístěna nejprve právě na FTP servery. Takové servery se někdy nazývají také Topsite FTP. Z těchto serverů, na které mají přístup jen zasvěcení, se pak nelegální obsah rychle šíří dále do internetu. Topsite FTP jsou tedy jedním z prvních článků. Podaří-li se policii náhodou takový server odhalit, pro warez scénu to může být velmi nepříjemné. Vzhledem k povaze těchto skupin však obvykle nebude trvat dlouho a nalezený, případně zabavený server bude brzy nahrazen jiným. Topsite FTP servery jsou nezřídka k nalezení ve vysokoškolském prostředí. Vysokoškolské koleje jsou dost možná jedním

zdroj: autor

Obr. 15 – K procházení FTP lze použít třeba i prohlížeč Firefox

z nejlepších a nejznámějších zdrojů nelegálního obsahu. Kvalitní připojení je dnes na vysokých školách běžné a pořídit kvalitní HW už dnes také není nedostupnou záležitostí. Koncem roku 2007 proběhl policejní zátah na vysokoškolských kolejích na pražském Strahově, kde byl údajně jeden takový Topsite FTP server objeven a zabaven. Je však otázkou, kolik jiných, neméně kvalitních FTP serverů už od té doby našlo na dotyčných kolejích své místo. Už dnes mohou být zaplněny minimálně stejným množstvím nelegálního obsahu jako onen zabavený server [32].

8.3 Programové prostředky používané při šíření nelegálního softwaru

V této kapitole si jen krátce přiblížíme některé z P2P programů, které se často používají právě při šíření nelegálních programů. Všechny sice pracují na podobném principu, ale každý z nich se odlišuje. Mezi programové prostředky k šíření nelegálních programů bychom mohli zařadit i webový prohlížeč nebo FTP klient, ale to jsou věci dost známé a také se k šíření nelegálního obsahu nepoužívají tak často.

8.3.1 BitTorrent klienti

BitTorrent je sice P2P program, nicméně je třeba jej odlišit od ostatních systémů. Rozdíl je v jejich zaměření. Zatímco většina P2P programů má jako hlavní náplň najít co nejširší spektrum obsahu u co největšího počtu uživatelů, BitTorrent je určen pro momentální využití. Výkonnost a rychlost stahování u tohoto systému sdílení dat roste se zájmem o dotyčná data. Pokud uživatel bude chtít stahovat například Windows 95, asi neuspěje tak výrazně. Windows 95 jsou již dávno za zenitem a poptávka po nich na P2P sítích nebude už největší. Naproti tomu lze postavit třeba nejaktuálnější snímky z kina, namátkou film *Michael Clayton*. Jelikož se v současnosti jedná o velmi aktuální snímek, dá se předpokládat, že o něj bude mít zájem velké množství lidí. A právě pro takové účely je BitTorrent ideální.

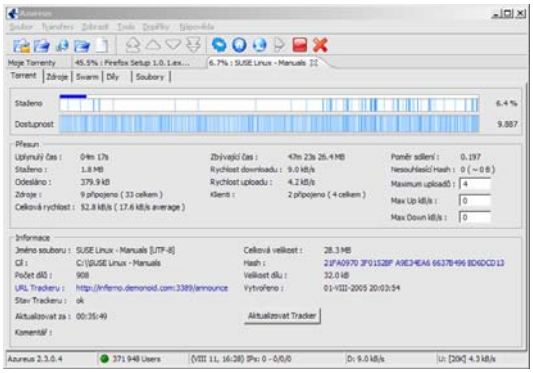
Funguje to asi tak, že ten, kdo je původním vlastníkem dat, vytvoří torrent. To je malý soubor, který obsahuje kompletní informace o datech i kde je hledat, jak je soubor velký a tak dále. Od tohoto prvního uživatele se pak data rozdělená na části rozšíří mezi další uživatele. Ti už je pak sdílí mezi sebou sami a původce dat nepotřebují.

Jakmile se .torrent soubor dostane k uživateli, ten se jeho pomocí připojí na tzv. tracker server. Zde se scházejí informace o všech uživatelích, kteří mají alespoň část potřebných dat k dispozici. Od těch si pak může pirát data stáhnout. Jakmile si stáhne nějakou část těchto dat, stává se součástí tohoto podniku. Jeho části programu si můžou stahovat další uživatelé. Čím aktuálnější je soubor, tím víc uživatelů jej momentálně nabízí či stahuje. Je potom velmi snadné potřebné části programu najít a složit z nich celek. Problémy nastanou ve chvíli, kdy už program není tak úplně aktuální. Pak se může stát, že se sice pomocí tracker serveru najde dost uživatelů, aby bylo možno pohodlně stahovat, ale nikdo z nich nemá některou část. Může se totiž stát, že určitou část dat momentálně nikdo nesdílí. V takovém případě si uživatel sice může stáhnout 90% dat, ale jsou mu k ničemu, protože část chybí. V takovém případě je pak jedinou možností, aby se připojil někdo, kdo potřebná data (celý soubor) má a může je nasdílet. Potřebná část dat se pak rozšíří dále a opět je od koho stahovat. Opatřit si *.torrent* soubory není žádný problém. Na internetu existuje řada serverů a webových stránek, které se přímo tomuto věnují. Celou řadu jich lze nalézt například na adrese http://www.torrentblog.net/.

Programy, které se na počítač instalují, se nazývají klienti. Zde jen výčet a krátký popis těch asi nejoblíbenějších a nejpoužívanějších. Programů je samozřejmě celá řada, ale není

cílem této práce o nich referovat. Zájemce si vše potřebné může dohledat na internetu.

Azureus – patří mezi ty neoblíbenější BitTorrent klienty. Je napsán v jazyce Java a díky tomu funguje nejenom pod operačním systémem Windows, ale má i své verze pro alternativní systémy jako Linux či Mac OS. Je šířen jako Open Source pod licencí GPL, to znamená, že jej lze volně užívat i dále modifikovat. Obsahuje všechny základní funkce, které by měl takový program podporovat. Podporuje dokonce také anonymní komunikační sítě I2P.



zdroj: wikipedia

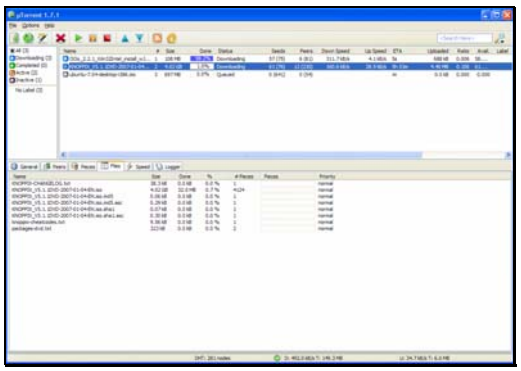
Obr. 16 – pracovní prostředí programu Azureus

BitSpirit – také tento klient je zdařilý, i když není mezi uživateli tak oblíbený jako zbývající dva uvedené. Obsahuje všechny základní funkce, které uživatel takového programu chce a očekává. Jeho výhodou je to, že je schopen nejen stahovat data, ale také uživateli pomoci s vytvářením torrentů, pokud chce nasdílet nějaká nová data.

zdroj: www.bitspirit.cz

Obr. 17 – Logo programu BitSpirit

µTorrent – tento klient má být jakousi odlehčenou verzí. Je proto velmi nenáročný na systémové zdroje, které spotřebovává ke svému běhu. Pokud však jde o funkčnost tohoto programu, nepostrádá nic potřebného. Program sice nebyl vyvinut v ČR, ale na internetu se dají najít jeho CZ i SK verze.



zdroj: www.utorrent.com

Obr. 18 – Pracovní prostředí klienta µTorrent

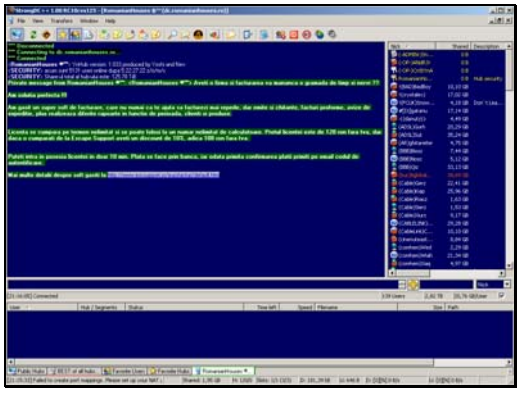
8.3.2 Klienti Direct Connect

Direct Connect je centralizovaná síť fungující na poněkud jiném principu než BitTorrent. Jejím principem je připojování k uzlovým bodům, tzv. HUBům. Na ty je současně připojeno i několik tisíc uživatelů. Každý uživatel může snadno procházet obsah nasdílených složek všech uživatelů, kteří jsou k HUBu aktuálně připojeni. Uživatel má na svém počítači nainstalován některý z klientů a po jeho spuštění a připojení k některému ze serverů může začít vyhledávat a stahovat data. Stahování není tolik citlivé na aktuální popularitu souborů.

Aktuální popularita souborů má samozřejmě vliv na množství dostupných zdrojů ke stahování, ale rychlost stahování neovlivňuje tak výrazně jako u sítě BitTorrent. Navíc je na síti Direct Connect snadnější najít méně obvyklá data. Také jsou HUBy někdy „specializované“, takže zájemce o konkrétní data může snadněji odhadnout, kde je asi najde. Existují HUBy zaměřené na video, mp3 a tak dále. Jedinou podmínkou pro připojení k serverům bývá množství nasdílených dat. Program ověřuje, kolik dat má uživatel ve sdílené složce, a podle toho mu dovolí či nedovolí se k HUBu připojit. Jedná se zpravidla o limity v řádech několika GB až několika desítek GB. Vzhledem k velké oblibě této sítě se také na internetu pohybuje velké množství klientů, které lze k připojení na DC použít. V krátkosti přehled několika nejznámějších:

DC++ – jedná se o originální klient pro Direct Connect. Obsahuje všechny nejnutnější funkce. Jako většina programů z této kategorie je i tento šířen zdarma. Jelikož síť Direct Connect je stále ještě aktivní, i klient DC++ prochází neustálým vývojem. Funkční je pouze pod systémy Windows. Aktuálně jej lze na internetu najít ve verzi 0.704.

StrongDC – možná nejkvalitnější klient pro Direct Connect. Vzhledově se nevymyká ze skupiny DC klientů. Ovládání je vcelku jednoduché a přehledné. Tento klient disponuje vlastností, kterou nemají jeho dva zde uvedení konkurenti. Jde o podporu segmentového stahování, což je vlastně principem BitTorrentu. Soubory jsou rozděleny na segmenty a ty se mohou stahovat zároveň a na konci stahování se spojí zpět do jednoho celku. Každý segment je možné stahovat od jiného uživatele. Tato funkce může velmi výrazně urychlit stahování dat ve srovnání s konkurenčními programy. Program je šířen zdarma jako freeware. [31]



zdroj: autor

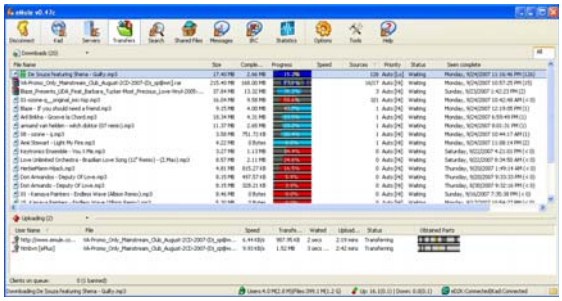
Obr. 19 – Pracovní prostředí klienta StrongDC

CZDC – jde vlastně jen o modifikaci originálního programu DC++. Obsahuje opravy některých chyb původního klienta a přidává některá vylepšení. Vzhledově se nijak nevymyká, podobá se oběma již zmíněným klientům. Mezi DC klienty patří také ke špičce. Je distribuován jako freeware. [6]

8.3.3 Další sítě

Ostatní sítě jsou založeny vždy na podobném principu a liší se spíše v detailech a v tom, zda jsou spíše centralizované či decentralizované. Některé vznikaly jako odpověď na nedokonalosti zmíněných dvou sítí, některé tu byly ještě dávno před nimi. Stejně tak oblíbenost těchto sítí je různá. Někdy se jedná o spíše chvilkovou záležitost, některé sítě si udržují solidní provoz dlouhodobě. Klienti pro tyto sítě jsou vesměs dost podobné a jsou podobné i klientům pro předcházející dvě sítě. Mezi nejznámější klienty patří:

eDonkey 2000 – jedná se o centralizovanou síť. V současné době má na miliony uživatelů. Slouží k výměně jakéhokoli obsahu, zejména pak filmů či hudby. Bohužel, jak je u podobných sítí obvyklé, řada sdílených souborů je nelegálních. Celou síť tvoří několik větších serverů, ke kterým se uživatelé připojují. Ty zprostředkovávají komunikaci mezi jednotlivými uživateli. V tom se podobá síti Direct Connect. Rozdíl je v tom, že servery v síti eDonkey dokážou ko-munikovat mezi sebou a uživatelům by mělo být teoreticky jedno, na kterém serveru jsou zrovna připojeni. Měli by vidět obsah všech aktuálně připojených uživatelů, i když zrovna nejsou na stejném serveru. Pro síť eDonkey se používá řada klientů. Jsou si zpravidla dost podobné a šíří se jako open source. Jako příklad poslouží eMule, Morpheus, Shareaza, eDonkey a řada dalších. Jsou snadno k nalezení a stažení na internetu. Je možné si klienty opatřit jak pro systémy Windows, tak pro alternativní Linux či MacOS [19].



Zdroj: wikipedia

Obr. 20 – Pracovní prostředí klienta eMule

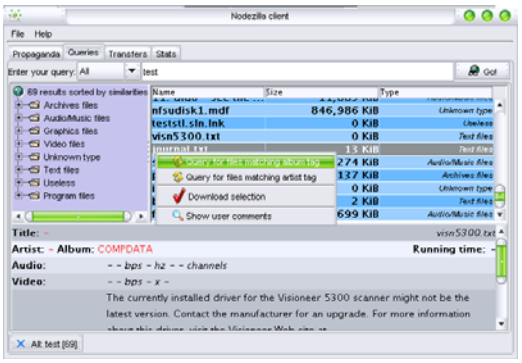
FastTrack – jeden čas byl FastTrack nejpopulárnější sítí vůbec. V dnešní době trochu ustoupil do pozadí a už se o něm tolik nemluví. Dovoluje stahovat data všech možných typů. Síť bývá často kritizována za poskytování prostředků k šíření nelegálního obsahu, to je ovšem obecně problém většiny P2P sítí. Nicméně FastTrack byl jednu dobu hlavním cílem protipirátských organizací jako je RIIA. Ta se snažila uživatelům znepříjemnit život tím, že na síť umísťovala řadu fake souborů a pro uživatele tak bylo velmi obtížné si stáhnout skutečně to, co chtěl. Často si stáhl bezcenný balík dat. V této síti je možné stahovat data po segmentech a tak může být download poměrně rychlý. Existuje několik různých klientů, které se na tuto síť umí připojit. Zpravidla jsou také šířeny zdarma. Z těch nejznámějších jsou to Kazaa, Grokster či iMesh. Kazaa měla svého času problémy s tím, že její klienti obsahují spyware[10], což jí trochu ublížilo v oblíbenosti.

Gnutella – v červnu roku 2005 patřilo této síti třetí místo v oblíbenosti P2P sítí. Předstihly ji pouze předchozí dvě jmenované. V současné době je také už spíše v pozadí. Je příkladem decentralizovaného systému. Uživatelé se k sobě připojují přímo, proto je Gnutella systém, který lze v rámci protipirátských aktivit jen těžko zlikvidovat. V podstatě se nedá vypnout. Jeho provoz závisí na počítačích jednotlivých uživatelů, nikoli na nějakém centrálním bodu, který by bylo možno odříznout. Klienti pro Gnutellu jsou různí a lze je opatřit pro všemožné operační

[10] 1Spyware jsou skryté drobné programky, které se nepozorovaně spouští na pozadí operačního systému a pak provádí nějakou činnost o které uživatel nemá často ani potuchy. Jedná se zejména o odesílání citlivých informací z počítače do sítě internet. Může jít třeba o přehled o navštěvovaných www adresách, které pak příjemce informací použije k zacílení rozesílané reklamy na správné uživatele. Některé druhy Spyware mohou být velmi nebezpečné povahou odesílaných dat (hesla,…).

systémy. Z těch nejoblíbenějších bych jmenoval LimeWire či BearShare. [11]

Nodezilla – Je to jeden z novějších počinů v oblasti sdílení dat. Jde o zcela decentralizovanou síť, která funguje na principu I2P což jsou sítě sázející hlavně na anonymitu. Také Nodezilla se snaží být anonymní sítí. Komunikace na této síti je šifrována. Nikdo tedy neví ani od koho stahuje, ani komu data poskytuje. Síť se snaží být co nejrychlejší a zabránit svému přetížení. Proto je možné stahovat data po segmentech. Velmi se tímto podobá síti BitTorrent, ze které si bere to lepší a přidává k tomu mnoho vylepšení. Jako program pro tuto síť se používá klient stejného jména [20].



Zdroj: www.nodezilla.net

Obr. 21 – Pracovní prostředí klienta Nodezilla

8.3.4 Vývoj do budoucna

Je dost obtížné odhadovat vývoj do budoucna. Technologie se ženou kupředu a těžko předvídat, s čím kdo zítra přijde, nebo jaká novinka se nenadále objeví. Těžko také odhadovat, která z cest si získá podporu širší veřejnosti. I v této oblasti totiž platí, že sebelepší nápad a sebelepší síť jsou k ničemu, pokud je lidé nevezmou za své. U sítí pro sdílení dat to platí dvojnásob. Jen velmi těžko se dá vybudovat úspěšná síť, pokud si k ní lidé nenajdou cestu. Sebekvalitnější síť totiž nebude skutečně funkční, pokud se na ní nenajde dost obsahu, který bude sdílen.

Dá se předpokládat, že budoucnost mají sítě typu I2P. Již existují technologie (Onion routing), které velmi ztěžují odhalení toho, kdo skutečně stahuje, i toho, co stahuje. Je to odpověď P2P scény na snahy protipirátských organizací omezit provoz na P2P sítích a zabránit sdílení nelegálních dat. Organizace jako například RIIA (Recording Industry Association of America) se snaží již dlouhá léta bojovat proti P2P sítím. V některých případech i celkem úspěšně. Například síť Napster byla nucena svůj princip zcela přetransformovat, pokud chtěla dále fungovat. Problémy měly také sítě jako FastTrack či WinMX. Obvykle protipirátské organizace dosáhly vypnutí centrálních serverů těchto sítí, nebo alespoň jejich omezení. Sítě nakonec obvykle opět ožijí, ale rozhodně jim taková aktivita znepříjemňuje život. A to by mohlo napovědět i vývoj do budoucnosti.

Věřím, že P2P scéna bude směřovat cestou anonymních sítí a šifrování. Jelikož je totiž v právním státě nutno piráta nejdřív usvědčit, je cílem zabránit získání potřebných důkazů. K tomu mohou sloužit sítě, kde budou uživatelé vystupovat maximálně anonymně, aby bylo jen velmi obtížné, ne-li nemožné, vypátrat jejich IP adresu a konkrétního uživatele, který se za ní skrývá. Dnes je velmi snadné od poskytovatele internetového připojení získat potřebná data. Ve chvíli kdy uživatel na síti nevystupuje pod skutečnou IP adresou, či svou identitu různě zakrývá a falšuje, je jeho odhalení značně ztíženo. Nejnovější systémy fungují například tak, že se nepřipojují přímo k původci dat, ale data cestují přes další uživatele a jejich původce je tak obtížné vypátrat. Cesta kterou data putují, se pak může dynamicky měnit, což opět ztěžuje odhalení zdroje.

Dalším trumfem pro P2P scénu se stane šifrování obsahu. To již dnes v některých sítích funguje a pro protipirátské organizace a policii bude představovat i v budoucnu velký oříšek. Pirátů je totiž obrovské množství, a pokud se budou přenášená data intenzivně šifrovat, je téměř mimo lidské možnosti veškerý přenášený obsah rozšifrovávat a zpětně zjišťovat, co který uživatel sdílí a stahuje. Dnešní šifrovací algoritmy jsou totiž poměrně kvalitní a rozlousknutí některých z nich je hodně složité. Ne že by to bylo nemožné, ale i s velmi jednoduchými nástroji se dá obsah šifrovat tak, že jejich rozšifrování se stává otázkou mnoha hodin i na vysoce výkonných počítačích.

Praxe v šíření nelegálních programů se tak může svým způsobem otočit. Piráti prolamují ochranu počítačových programů dnes a denně. V budoucnu možná tato práce bude čekat policii a protipirátské organizace, které budou nuceny prolamovat ochranu sítí pro sdílení dat, jejich šifrování a strukturu. Pro protipirátské organizace to je bohužel v podstatě marný boj. Těch ktěří chtějí stahovat, je daleko víc než těch, kdo nim tomu bojují. A tak i vývoj sítí pro sdílení bude nejspíš daleko rychlejší, než vývoj systémů jak jim čelit. Může to znamenat i to, že strana, na které stojí zákon, může tento boj zcela ztratit. Ukazuje se totiž, že vývoj zastavit nelze a zastavit sítě pro sdílení dat je asi nemožné. Technologie je dnes spíše na straně pirátů a ochránci autorských práv budou muset hledat jiné cesty, jak nelegálnímu šíření obsahu zabránit.

9 Vliv prostředků použitých k šíření nelegálních programů a rozsahu činnosti na případný právní postih

Každý způsob šíření nelegálních programů je trochu jiný a stejně tak je třeba jinak přistupovat i ke každému, kdo se porušením autorského práva provinil. Ne vždy platí, že porušení je motivováno dosažením majetkového prospěchu. Stejně tak rozsah činnosti se u různých metod šíření liší. Lišit by se tak měl i případný postih pachatele.

9.1 Prodej nelegálních disků

Jak už bylo uvedeno, jedná se o závažnější formu porušování autorského zákona. Je totiž velmi snadné v tomto případě prokázat úmysl způsobit škodu a obohatit se. Jen velmi těžko může prodejce či výrobce nelegálních kopií tvrdit, že neměl tušení o nelegálnosti svého počínání. Pak je také samozřejmě dost obtížné popřít, že šlo o úmyslný trestný čin. Je to velmi podobné jako s řadou jiných podvodů. Taková činnost je zjevně vědomá a má jasné cíle ve smyslu získání neoprávněného majetkového prospěchu. Navíc je tato činnost doménou organizovaných skupin. Jedná se tedy o organizovaný zločin.

Na takovýto způsob pirátství se samozřejmě vztahují příslušná ustanovení Trestního zákona (§150 a §152). Jelikož se pak jedná o činnost zpravidla velkého rozsahu, tresty by se měly pohybovat na horní hranici trestní sazby, tedy v rozmezí 6 měsíců až 5 let. Součástí trestu pak může být i trest propadnutí věci, tedy nelegálních kopií [28]. Ze soudních případů, které jsou citovány na internetových stránkách BSA, však vidíme, že zpravidla se sahá k podmíněným trestům. Jako součást trestu pak pravidelně figuruje i zmíněný trest propadnutí věc, tedy inkriminovaných datových nosičů a případně i prostředků, s jejichž pomocí byl SW neoprávněně kopírován. Někdy je pachatel nucen také nahradit škodu. Toto může být pro piráta největší rána. Ve chvíli, kdy někteří takoví distributoři vlastní i několik tisíc kopií programů, šplhá náhrada škody do statisícových částek.

Pokud jde o zjišťování takové nelegální činnosti pak lze říci, že z oblasti počítačového pirátství patří k nejsnáze dokazatelným. SW je totiž prodáván za úplatu a na fyzickém médiu. To potom může sloužit jako důkazní materiál. Pachatel také musí SW někde prodávat, ať už v kamenném obchodě, nebo prostřednictvím pošty. V obou případech však je v silách policie dotyčného hříšníka vypátrat a začít ho vyšetřovat. Pokud se jednou ocitne v hledáčku policie, už obvykle dojde i na domovní prohlídku, případně prohlídku nebytových prostor. A tam už bývá policie úspěšná v nacházení dalšího důkazního materiálu – dalších nelegálních disků.

9.2 Prodejci hardwaru

Velmi podobný druh kriminality, jako předchozí forma. Pachatelé se jen těžko mohou omlouvat tím, že nevěděli, že činí něco nelegálního. Pokud podnikají v oblasti IT, měli by znát i právní rámec takového podnikání. Autorské právo a trestní zákon do takového rámce bezpochyby patří. Druhým aspektem pak je opět cíl se obohatit. I když v tomto případě je možné, že prodejce programy na počítač jen nelegálně nainstaluje a nic si za to neúčtuje. Ovšem i v takovém případě jde o nezákonnou činnost. Prodejce totiž tímto získává neoprávněnou konkurenční výhodu. Jiný prodejce, který SW na počítače instaluje z legálních disků, si za programy samozřejmě nechá zaplatit. Pokud promítne náklady v řádech tisícikorun do ceny počítače, může být jen obtížně konkurenceschopný. A tak mu vznikla škoda.

Postihy za takovou trestnou činnost jsou velmi podobné předchozím případům. Zpravidla se jedná o tresty podmínečné ve spojení s trestem propadnutí věci a náhrady škody. Záleží však na rozsahu činnosti a způsobené škody. Obvykle platí, že nepodmíněné tresty se v takových soudních případech neobjevují.

Pokud jde o odhalování takovéto činnosti, což je samozřejmě první krok k postihu, má policie šanci uspět. Stejně jako v předchozím případě i tentokrát je nutné činnost někde fyzicky provádět. Pokud firma prodává HW s nelegálním programovým vybavením, je nucena jej nabízet na konkrétním místě. Jestliže tak činí, mají příslušné instituce šanci se k firmě dostat. A jakmile se na ni zaměří, není opatření důkazního materiálu tak náročné. V takové firmě je vždy někdo zodpovědný (jednatel), kdo ponese za takové konání důsledky. A to je v pořádku, jelikož si lze jen velmi těžko představit, že nejvyšší představitel firmy nemá tušení o tom, co se nachází v počítačích, které jeho firma prodává, i když se to vyloučit nedá. Svůj díl odpovědnosti bude mít i správce počítačového vybavení. Důkazním materiálem pak mohou být samotné počítače s nelegálními programy, datová média a podobně.

Firmy, které se takovouto trestnou činností proviní, bývají menší, často začínající. Nejsou totiž na trhu zavedené a tak zkouší najít jinou cestu, jak se zákazníkům zalíbit. Je to ovšem cesta špatná a může se stát, že taková začínající firma také brzy skončí.

9.3 Nadužívání softwaru

Nadužívání počítačových programů se vyskytuje zejména ve firemním sektoru a osobně bych jej nehodnotil tak přísně. Zde se nedá vyloučit, že půjde o trestný čin neúmyslný. Může se poměrně snadno stát, že dojde k omylu a SW je nainstalován na počítač, na kterém by být neměl. Nikdo není neomylný.

Ovšem i tak se jedná o trestný čin porušování autorského práva (§152 trestního zákona). Ten může být potrestán ve výjimečných případech odnětím svobody až na 5 let, peněžitým trestem a trestem propadnutí věci. To samozřejmě může být pro firmu velmi nepříjemné. Zejména dva aspekty jsou pro firmy velkým strašákem. Tím prvním je nepopiratelné poškození jména firmy. Pokud je firma usvědčena, může se její jméno objevit v tisku ve spojení s případem a negativní publicita jistě neprospěje. Druhým aspektem pak je výše zmíněný trest propadnutí věci. Často se totiž může jednat o citlivá data či „nepostradatelný“ prostředek pro přežití firmy. Pokud je firmě takový pracovní prostředek zabaven, riskuje vyzrazení citlivých firemních dat a také možné finanční ztráty. Pokud si představíme, že na počítači, který je zabaven, jsou uložena nějaká data potřebná k výrobě či dokončení zakázky, může takové soudní rozhodnutí ohrozit celou zakázku. Následná finanční ztráta pak může převýšit i obohacení způsobené nadužíváním SW. Proto se domnívám, že drobné prohřešky tohoto charakteru (jedna či dvě kopie navíc) by měly být řešeny spíše domluvou či peněžitým trestem. Satisfakce z tvrdého trestu by totiž mohla být daleko menší než způsobené škody.

Pokud jde o odhalování takové trestné činnosti, jde o složitější situaci. Nadužívání SW totiž není navenek vidět. V předchozích případech lze někde nalézt inzerát s podivně nízkou cenou SW či přeinstalovaného SW. Ale v tomto případě? Firma přece navenek nevytrubuje, že si nainstalovala o jednu či dvě kopie navíc. Cestou jsou v tomto případě buď ohlášení na policii (z řad bývalých či současných zaměstnanců, konkurentů, správců výpočetní techniky…) a nebo náhoda. Náhodou je myšleno například vyšetřování jiné povahy, v rámci něhož se náhodou přijde i na SW pirátství. Nebo konkurent firmu udá, aniž by měl konkrétní podezření a sází na to, že se najde něco, co není v pořádku. Jakmile se objeví nějaké důvodné podezření, má už policie nástroje, jak si důkazy opatřit. Může ve firmě vykonat prohlídku nebytových prostor a provést skeny (uloží přesnou kopii obsahu) na discích počítačů. Z nich pak, po porovnání s předloženou dokumentací, může zjistit zda nedochází k nadužívání SW, a pokud ano, tak v jaké míře.

Zde je třeba oddělovat neúmyslné a úmyslné porušení zákona. Může se skutečně stát, že se ve firemní síti najde nějaká nelegální kopie. Případně že si zaměstnanec sám nainstaluje, co nemá. Ale úmysl v tom být nemusí. Pokud však firma s 60 počítači zakoupila jen 2 instalace, avšak program má nainstalován na každém počítači, o chybě může být řeč jen velmi těžko.

9.4 Internetové pirátství

Internetové pirátství je již z povahy věci trochu obtížnější postihovat. Především, jak bylo v této práci již několikrát zmíněno, není úplně jednoduché piráta vypátrat. Ten, kdo se o to pokouší, musí vlastně zjistit 3 základní věci. Za prvé, jaký obsah dotyčný stahuje. Ne vše co se na internetu dá stáhnout, a to se týká i programů, je nelegální. Ba naopak, legální obsah převažuje. Je tedy třeba nejprve zjistit, zda jsou data skutečně chráněna autorským zákonem. Pokud ano a je s nimi nakládáno tak, jak autorským právům odporuje, je potřeba zjistit, kdo data nabízí/stahuje. Je tedy třeba adresu počítače, který byl k přenosu nelegálních dat použit, vypátrat. Počítače se v síti identifikují pomocí IP adresy. Je tedy třeba IP adresu piráta zjistit. Posledním krokem pak je zjistit, kdo se za danou IP adresou skrývá. To už však ve spolupráci s poskytovatelem internetového připojení patří k té lehčí činnosti. Toto vše je vlastně fáze získávání důkazů. Jakmile jich je dostatek, může policie přistoupit k tomu, že udělá u onoho uživatele domovní prohlídku, která se zaměří především na výpočetní techniku. Policie provede analýzu programů v počítači a porovná nainstalované s předloženými licencemi a doklady o koupi programu. Pokud zjistí nesrovnalosti, má dostatek podkladů k tomu, aby uživatele obvinila z porušování autorských práv.

Tresty za internetové pirátství jsou zatím spíše mírné, převládají podmínečné tresty. Ty jsou doplněny tresty peněžními a tresty propadnutí věci. Při dnešních pořizovacích nákladech na nové počítačové vybavení o příliš vážný trest nejde. Nápravný účel tak plní buď uložené pokuty nebo hrozba ztráty leckdy cenných dat. Shovívavost v těchto případech je vcelku pochopitelná. Málokterý uživatel s nelegálními daty prostřednictvím internetu skutečně obchoduje a jde tedy převážně o soukromou aktivitu. Jejím cílem není finanční prospěch, ale pouze úspora finančních prostředků. Samozřejmě i to je finanční prospěch, ale jistě všichni cítíme, že zde je rozdíl oproti tomu, kdyby SW nabízel za úplatu dále.

Warez servery – Pokud jde o warez servery, je třeba zmínit, že řada poskytovatelů serverového prostoru pracuje za protipirátské organizace. Zkrátka mají v podmínkách užívání dáno, že je zakázáno v jejich www prostoru zřizovat stránky odkazující na warez. Nicméně nejsou takoví všichni a vždy se najde možnost, jak takové stránky někam umístit. Potom je třeba rozlišit stranu nabídky a poptávky. V případě warez serverů je na straně nabídky někdo, kdo do fóra uloží link odkazující na soubor s nelegálními daty. Taková činnost je považována za nelegální. Vlastník autorských práv má pak podle §40 odst. 1 písm. f) autorského zákona právo se domáhat odstranění takových stránek..

Pro poptávku, tedy stahující stranu, není nelegální, pokud si **video či hudbu** stahuje a použije jen pro vlastní potřebu. I když se to bude týkat díla autorsky chráněného. Autorský zákon §30 odst. 1 a 2 totiž říkají, že:

*„Za užití díla podle tohoto zákona se **nepovažuje** užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.“* [28]

„Do práva autorského tak nezasahuje ten, kdo pro svou vlastní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.“ [28]

Ovšem pozor, v §30 odst. 3 je z možnosti tzv. volného užití vyjmut počítačový software. Znamená to tedy, že se zde měří jiným metrem u stahování audiovizuálních souborů a jiným u stahování softwaru. Stahování autorsky chráněných programů, třeba ze serveru Rapidshare, tak je možné kvalifikovat jako trestný čin. Platí, že i pokud si uživatel data pouze stáhne na disk a dále s nimi nijak nenakládá, tedy například z ISO[11] souboru program nenainstaluje, dopouští se trestného činu. Jedinou výjimkou by bylo, pokud by k takovém programu současně vlastnil legálně zakoupenou instalaci.

Na opačné straně barikády pak stojí ten, kdo obsah na server umístil. Ten se trestného činu dopouští, ať už na server uploaduje jakákoliv autorsky chráněná data. Rozdíl mezi oběma stranami je v tom, že stahující obsah dále nenabízí, ovšem uploadující strana už SW nabízí tím, že jej poskytne na stahování. Stává se tak distributorem nelegálního SW se všemi důsledky z toho plynoucími. Bude však poněkud problematické dokázat případně dotyčnému další nelegální SW, který někam uploadoval. To by si vyžádalo rozsáhlejší pátrání a dohledávání. Navíc se může lehce stát, že řada jeho uploadovaných dat je už ze serverů opět odstraněna. Proto se bude zpravidla jednat o porušování autorského práva v malém rozsahu a dotyčnému tak hrozí trest až do 2 let odnětí svobody, peněžitý trest a trest propadnutí věci. Horším dopadem pro takového hříšníka může být, že případné policejní vyšetřování a policejní prohlídka hrozí tím, že se u něj nalezne množství dalšího nelegálního materiálu.

FTP – Zde je situace velmi podobná warez serverům. Nelegálního jednání se dopouští jak ten, kdo data nabízí, tak i ten, kdo je stahuje (jedná-li se o počítačové programy). Rozdíl je třeba spatřovat v tom, že FTP servery nemusí být umístěny u nějakého třetího poskytovatele. Mohou se nacházet třeba na vysokoškolských kolejích, a pokud pak dojde na vyšetřování, je vina i na vlastníkovi serveru, jelikož povolil jeho využití k šíření nelegálního SW. Také se dá odhadnout, že na FTP serverech jsou obrovské objemy nelegálních dat. Dalo by se tedy asi s úspěchem tvrdit, že se jedná o činnost většího rozsahu. Ostatní aspekty zůstávají stejné. Odhalování takových FTP serverů bude trochu problematičtější, jelikož FTP servery nejsou věc veřejně prezentovaná, ale jsou záležitostí zasvěcených. Půjde tak spíše o úniky informací, které povedou k tomu, že se policie dostane na stopu.

P2P sítě – Na rozdíl od předchozích případů se v P2P sítích může do problémů dostat i nezkušený naivní uživatel. U warez servetů a FTP serverů se předpokládá jistá míra znalostí a úmyslu. V případě P2P sítě může dojít k porušení zákona i z důvodu nepozornosti, naivity či hlouposti. Jak už bylo uvedeno dříve, P2P sítě jsou založeny na principu nabídky a poptávky, tedy někdo stahuje a někdo nabízí. Například systém DC++ dokonce nedovolí připojení na některé z HUBů, pokud uživatel nenasdílí potřebné datové objemy. A zde může nastat problém pro nezkušeného a neznalého uživatele. Může tak přijít situace, kdy dotyčný slyší od kamaráda či známého o systému DC++, kde si může stáhnout co chce. Nemusí přitom jít o nelegální obsah. Může se jednat o demoverze nějakých programů. Dotyčný si DC nainstaluje, pokusí se připojit na některý HUB, ale to se mu nepodaří. Musí nejprve nasdílet nějaká data. Nasdílí tedy třeba svou hudební složku. Tu může mít velmi rozsáhlou a legální (MP3 zakoupené na iTunes[12]…). V tu chvíli se stane pachatelem trestného činu. I když si to možná ani neuvědomí a nebylo to jeho úmyslem. Prostě nasdílel, co neměl. Ovšem z pohledu autorského zákona už porušuje zákon, jelikož nabízí obsah chráněný autorským právem. Nicméně je velmi pravděpodobné, že takový uživatel by se do hledáčku protipirát-

[11] ISO soubor – jedná se o přesnou kopii CD/DVD disku uloženou na pevném disku počítače. Lze s ní dále pracovat. Buď je možno ji později opět vypálit na CD/DVD aniž by byla data nějak modifikována. ISO soubor je též možné připojit jako virtuální disk a pracovat s ním jako se skutečným originálním diskem.

[12] iTunes –internetový obchod firmy Apple Computer. Dovoluje z internetu legálně stahovat hudbu ve formátu MP3 a další obsah.

ských organizací dostal spíše náhodou. Naproti tomu někdo, kdo už půl roku soustavně nabízí na P2P síti svou „shared“ složku o objemu 500 GB, se může do hledáčku policie dostat dost snadno. I když dnes už se datové objemy na domácích počítačích mohou pohybovat ve stovkách GB, stále je někdo s 500 GB sdílených dat podezřelý. Zkrátka vyčnívá z řady. Pro rekapitulaci: mít P2P program nainstalován a stahovat audiovizuální data není podle českého práva problémem. Nabízet však jakýkoliv nelegální obsah už je trestným činem a jako takový může být potrestán.

Co se týče postihu, půjde spíše o tresty na spodní hranici trestní sazby. Společenská nebezpečnost takového uživatele není příliš vysoká a navíc jeho cílem nemusí být se nějak obohatit.

9.5 Drobní piráti vs. velké ryby

I když policie a protipirátské organizace jsou v odhalování nelegálního SW stále úspěšnější, jejich hlavním cílem budou organizace. Rozdíl je zřejmý. Z drobného piráta si toho poškozený mnoho nevezme. Jeho společenská nebezpečnost je nízká a tak i postihy jsou spíše mírnější. Jiné je to u větších organizací a firem. Taková firma má spoustu peněz. Má zavedené jméno a na starosti jiné věci, než se zaobírat problémy s pár nelegálními kopiemi Windows. Firmy jsou tedy daleko náchylnější k tomu sklonit hlavu, přiznat chybu a jít cestou mimosoudního vyrovnání. Vyhnou se tak ostudě, poškození obchodního jména i zbytečným průtahům. Nápravný efekt v takovém případě zůstane zachován. Jsem přesvědčen, že taková firma si dá pro příště daleko větší pozor.

Navíc k odhalení drobného piráta je třeba vynaložit stejné, ne-li větší, úsilí. Drobní piráti a domácí uživatelé tak jsou spíše na okraji zájmu. Když se některý z nich dostane před soud, je to tak trochu obětní beránek. Někdo, kdo má sloužit jako odstrašující případ a odradit alespoň na chvíli potenciální piráty od jejich jednání.

Trochu mimo pak stojí distributoři nelegálního SW, prodejci padělků a podobně. Ti jsou jinou skupinou a určitě si zaslouží ten nejtvrdší postih. V jejich případě by nepodmíněné tresty mohly padat mnohem častěji, protože v se bezpochyby jedná o krádež. Chtějí se obohatit na úkor někoho jiného, získat neoprávněný majetkový prospěch. Takové jednání neprospívá vůbec nikomu kromě jich samotných. Výrobci a distribuční články přijdou o peníze z prodeje, stát o příjmy z daní a koncový uživatel, který si program koupí, dostává velmi často nekvalitní produkt bez náležité podpory a příslušenství. Poškozeni tak jsou v podstatě všichni vyjma distributora nelegálních programů. Mají-li tedy v oblasti nelegálního šíření počítačových programů padat nepodmíněné tresty, mělo by to být právě v těchto případech.

10 Závěr

Ve své práci jsem se pokusil poměrně zeširoka obsáhnout problematiku nelegálního šíření počítačových programů. Dotýká se jak právních aspektů problematiky, tak oblastí ryze praktických. Snad se mi podařilo narazit i na oblasti, které nejsou běžnému uživateli známy a jsou pro něj tak trochu skryty. Jsem přesvědčen, že v dnešní informační společnosti by každý měl mít alespoň základní povědomí o této problematice. Když už pro nic jiného, tak jako prevenci, aby sám neudělal něco, co by mohlo být později za porušení autorských práv považováno. S počítači pracuje většina z nás dnes a denně a tak i problematika legálnosti používaného softwaru se dotýká nás všech.

Oblast nelegálního šíření počítačových programů a souvisejícího porušování autorských práv k programům je v současnosti velmi diskutovaným problémem. V minulosti byla právní úprava v této oblasti často nedostatečná a mohlo být obtížné aplikovat autorská práva na oblast informačních technologií zcela korektně. V poslední úpravě autorského zákona z roku 2006 se však objevila některá ustanovení, která se týkají výhradně počítačových programů a databází. Zdá se, že pro stranu poškozených v tomto věčném boji se objevují další nástroje a cesty, jak svůj software před zneužitím ochránit. Používání a šíření počítačových programů se tak pomalu stává poměrně dobře regulovanou oblastí. Také Policii ČR a dalším orgánům zabývajícím se odhalováním porušování autorského zákona v oblasti IT se daří v některých případech dopadnout i významnější piráty. Mohlo by se zdát, že se softwarovým společnostem a vývojářům může blýskat na lepší časy.

Na druhou stranu je třeba si uvědomit, že tak jak se vyvíjí ochrana počítačových programů z pohledu práva, vyvíjí se i techniky k obcházení zákonů. Velkým problémem je porušování autorských zákonů prostřednictvím internetu. Dnešní šifrované sítě, ve kterých může pirát dovedně skrývat svou identitu, představují pro stanu zákona opět komplikaci. Navíc do budoucna se nedá čekat, že piráti od svého jednání upustí. Je třeba si uvědomit, že pro mnoho pirátů je porušování autorských práv vlastně koníčkem. Je to hra na kočku a myš, ve které myš zatím stále vítězí.

I do budoucna tak budou převládat spíše případy odhalování nelegálního SW u firem a velkých pirátských skupin. Námaha k vypátrání běžného uživatele používajícího nelegální programy totiž může převýšit následnou satisfakci. Ve sféře pirátů jednotlivců povede cesta pravděpodobně jedině zpřísněním legislativy. Jednoduše prosadit takovou legislativu, která by nepostihovala jen ty usvědčené stahovače nelegálního obsahu, ale bojovala by už proti samotnému systému, tedy proti sítím pro sdílení dat. Pokud by se takové systémy postavily úplně mimo zákon, mohlo by být trestné nabízení jakéhokoli obsahu. Třeba i vlastních vytvořených dat nebo dat, která se z podstaty věci šířit mají a jsou k tomu určena (freeware, shareware, demoverze…). Je tedy dost pravděpodobné, že něčeho takového se v právním systému asi jen tak nedočkáme. Může se však stát, že se v zákonech objeví něco jako zákaz se na internetu ukrývat a vystupovat anonymně. Takový občanský průkaz nebo pas na internetu. Ovšem ruku na srdce. Je vůbec možné očekávat něco podobného? V dnešní době, kdy je svoboda pro lidi velmi důležitým atributem? V době, kdy se v Evropě boří hranice a kdy je možné svobodně cestovat bez toho, abychom byli obtěžování neustálými kontrolami? Těžko říci. Co nám tato oblast do budoucna přinese, ukáže jen čas.

11 Literatura

[1] Adware - Wikipedie, otevřená encyklopedie [online]. 2007 , 27. 12. 2007 [cit. 2008-01-06]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Adware>.

[2] BOHÁČEK Martin., Licenční smlouvy ve vztahu ke knihovnám [online]. [cit. 2008-01-06]. Dostupný z WWW: < http://knihovna.nkp.cz/NKKR0104/0104242.html>.

[3] BSA – Business Software Alliance [online].[cit. 2008-01-06]. Dostupný z WWW: <http://w3.bsa.org/czechrepublic/>.

[4] BSA – typy pirátství [online]. 2008 [cit. 2008-01-18]. Dostupný z WWW: < http://w3.bsa.org/czechrepublic/antipiracy/Types-of-Piracy.cfm >

[5e] BSD Licence - Wikipedie, otevřená encyklopedie [online]. 2007 , 03. 01. 2008 [cit. 2008-01-06]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/BSD_licence>.

[6] CZDC++ - český stahovací speciál [online]. 2008 , 13. 10. 2007 [cit. 2008-01-18]. Dostupný z WWW: < http://magazin.slunecnice.cz/clanky/czdc-cesky-stahovaci-special/ >.

[7] Česká protipirátská unie [online]. 2007 [cit. 2008-01-12]. Dostupný z WWW: <http://www.cpufilm.cz/kdo_jsme.html>

[8] Disketa - Wikipedie, otevřená encyklopedie [online]. 2007 , 01. 01. 2008 [cit. 2008-01-14]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Disketa >.

[9] Donationware - Wikipedia, the free encyclopedia [online]. 2007 , 17. 11. 2007 [cit. 2008-01-06]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Donationware>.

[10] GNU General Public Licence - Wikipedie, otevřená encyklopedie [online]. 2007 , 03. 01. 2008 [cit. 2008-01-06]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/GNU_General_Public_License>.

[11] Gnutella - Wikipedie, the free encyclopedia [online]. 2008 , 13. 01. 2008 [cit. 2008-01-18]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Gnutella >

[12] Graphisoft - Piracy in general [online]. 2008 [cit. 2008-01-20]. Dostupný z WWW: < http://www.graphisoft.com/company/about_graphisoft/piracy/piracy1.html >

[13] HOLČÍK, Tomáš. Ochrana BD+ prolomena. Computer 22/07. 2007, č. 22, s. 78.

[14] ITprávo – server o internetovém a počítačovém právu [online].[cit. 2008-01-20]. Dostupný z WWW: < http://www.itpravo.cz/ >

[15] KLÁŠTERECKÝ Jan D., Autorské právo: Vývoj a souvislosti - Měšec.cz [online]. 2007 , 6. 2. 2007 [cit. 2008-01-06]. Dostupný z WWW: < http://www.mesec.cz/clanky/autorske-pravo-vyvoj-a-souvislosti/ >

[16] Licenční smlouva [online]. [cit. 2008-01-06]. Dostupný z WWW: < http://www.microsoft.com/cze/licence/ZakladniInformace/LicencniSmlouva.mspx>.

[17] Míra softwarového pirátství v Česku a ve světě – tisková zpráva [online]. 2007 , 15. 05. 2007 [cit. 2008-01-06]. Dostupný z WWW: <http://w3.bsa.org/czechrepublic/upload/2006_studiebsa_tz-2.pdf>.

[18] Open source software - Wikipedie, otevřená encyklopedie [online]. 2007 , 20. 03. 2008 [cit. 2008-03-22]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Open_source >.

[19] P2P eXPerience : eDonkey 2000 [online]. 2008 [cit. 2008-01-18]. Dostupný z WWW: < http://www.p2pxp.info/index.php?page=edonkey&lng=cs >

[20] P2P eXPerience : Nodezilla [online]. 2008 [cit. 2008-01-18].
Dostupný z WWW: < http://www.p2pxp.info/index.php?page=nodezilla&lng=cs >

[21] Phoenix Labs > PeerGuardian 2 [online].[cit. 2008-03-02].
Dostupný z WWW: < http://phoenixlabs.org/pg2/ >

[22] Počítačový program - Wikipedie, otevřená encyklopedie [online]. 2007 , 13. 9. 2007 [cit. 2008-01-06].
Dostupný z WWW: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_program>.

[23] Policii scházejí lidé pro boj s internetovou kriminalitou [online], 2007, 28. 12. 2008 [cit. 03-03-2008].
Dostupný z WWW: <http://zpravy.idnes.cz/policii-schazeji-lide-pro-boj-s-internetovou-kriminalitou-pa2-/krimi..asp?=A071227_140808_krimi_pei>

[24] Portál veřejné správy České Republiky [online]. [cit. 2008-03-01]. Dostupný z WWW:
<http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=82/1998&PC_8411_li=0&PC_8411_ps=10&#10821 >

[25] Právo IT § [online].[cit. 2008-01-20]. Dostupný z WWW: < http://www.pravoit.cz >

[26] Proprietární software - Wikipedie, otevřená encyklopedie [online]. 2007 , 29. 12. 2007 [cit. 2008-01-06].
Dostupný z WWW: < http://cs.wikipedia.org/wiki/Propriet%C3%A1rn%C3%AD_software>.

[27] Protipirátská ochrana Blu-ray disků prolomena. Filmy budou zase zadarmo [online]. 2007, 23. 1. 2007 [cit. 2008-01-12]. Dostupný z WWW: < http://technet.idnes.cz/protipiratska-ochrana-blu-ray-disku-prolomena-filmy-budou-zase-zadarmo-1nv-/tec_denik.asp?c=A070123_115013_tec_video_NYV >

[28] SAGIT, Autorské právo, Průmyslová práva. Ostrava : [s.n.], 2007. 224 s. ÚZ. ISBN 80-7208-573-5.

[29] Softwarové licence - Wikipedie, otevřená encyklopedie [online]. 2007 , 3. 11. 2007 [cit. 2008-01-06].
Dostupný z WWW: < http://cs.wikipedia.org/wiki/Softwarov%C3%A9_licence>.

[30] Software zadarmo [online]. [cit. 2008-01-06].
Dostupný z WWW: < http://www.asw.cz/cze/free_software.html>.

[31] Stahujte pohodlně díky Strong DC ++ [online]. 2008 , 30. 9. 2007 [cit. 2008-01-18].
Dostupný z WWW: < http://magazin.slunecnice.cz/clanky/stahujte-pohodlne-diky-strong-dc/ >.

[32] Topsite_(warez) - Wikipedie, the free encyclopedia [online]. 2008 , 08. 01. 2008 [cit. 2008-01-18].
Dostupný z WWW: < http://en.wikipedia.org/wiki/Topsite_(warez) >.

[33] Tor: anonymity online [online].[cit. 2008-03-02]. Dostupný z WWW: < http://www.torproject.org/ >

[34] Trestní řád (Zákon o trestním řízení soudním) 2008 , 11. 3. 2008 [cit. 2008-03-11].
Dostupný z WWW: < http://business.center.cz/business/pravo/zakony/trestni_rad/ >.

[35] Volné dílo - Wikipedie, otevřená encyklopedie [online]. 2007 , 3. 11. 2007 [cit. 2008-01-06].
Dostupný z WWW: < http://cs.wikipedia.org/wiki/Public_Domain#Public_domain>.