UNIVERZITA KARLOVA V PRAZE

Právnická fakulta

Ústav práva autorského, práv průmyslových a práva soutěžního

Softwarové pirátství

Diplomová práce

Jan Pfeffer

Vedoucí diplomové práce:
JUDr. Petra Malá Žikovská

Praha, srpen 2009

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a že jsem v ní vyznačil všechny prameny, z nichž jsem čerpal, způsobem ve vědecké práci obvyklým.

V Praze 30.8.2009 Jan Pfeffer

Poděkování

Děkuji paní doktorce JUDr. Petře Malé Žikovské, vedoucí mé diplomové práce, za cenné připomínky, poskytnuté materiály a účinnou pomoc při zpracování.

Dále děkuji své přítelkyni a rodině za podporu, trpělivost a starostlivost.

V Praze 30.8.2009 Jan Pfeffer

Obsah

1. Úvod

Důvodem sepsání této práce pro mne byl zvyšující se počet zpráv o softwarovém pirátství a jeho potírání. Na základě vlastních zkušeností s prováděním softwarových auditů jsem se rozhodl získat více znalostí, ponořit se hlouběji do problematiky nelegálního užívání počítačových programů, jejich šíření v souvislosti s rozvojem informačních technologií, ale především také právní úpravy tohoto oboru včetně otázek doposud přehlížených, právem neupravených či soudy neřešených.

Pokusím se vymezit pojem počítačového programu, jeho vznik, nejdůležitější způsoby šíření a v neposlední řadě také soukromoprávní i veřejnoprávní ochranu.

Důležitým aspektem mé práce bude rozdělení počítačových programů do několika skupin, jejich definice a následné odlišení těch, které budou chráněny právem a které nikoli. Následovat bude uvedení nejčastějších případů softwarového pirátství včetně domněnek, mýtů a faktů pojících se s tímto tématem.

Základním tématem mé práce však bude dynamický rozvoj informačních technologií, především internetové sítí v posledních letech. Tento trend poskytuje poměrně snadnou cestu i pro začínajícího uživatele, jak nelegálně získat téměř jakýkoli počítačový program. Takových způsobů získání je mnoho a ve své práci se je pokusím popsat ať již ze stránky technologické, tak ze stránky právní a zároveň se pokusím nastínit možnosti postihu jednotlivých osob za jejich jednání ve vztahu k počítačovým programům, ale i ostatním právem chráněným dílům.

Hlavní pozornost věnuji dvěma fenoménům současné doby, které dle mého názoru způsobují v největším měřítku porušování veškerých autorských práv v soudobé společnosti. Prvním bude tzv. warez scéna, kterou lze považovat za počátek veškerého protiprávního šíření počítačových programů i dalších autorsky chráněných děl. Pokusím se tento pojem vysvětlit, popsat důvody i období jeho vzniku, vymezit jeho cíle a odlišit ho od ostatních způsobů šíření počítačových programů a porušování autorských práv. Druhým fenoménem budou tzv. P2P (peer-to-peer) sítě, které sice začaly vznikat až o několik let později, ale momentálně se s jejich pomocí protiprávně šíří naprostá většina autorsky chráněných děl po internetu. Pokusím se popsat principy fungování těchto sítí, jejich základní rozlišení, právní úpravu a především také vyvodit odpovědnost jednotlivých osob v rámci těchto sítí.

Vzhledem k velice rychlému vývoji této oblasti si dovolím vynechat starší literaturu a odborné články týkající se právě počítačových programů, jelikož jejich absolutní ochranu přinesla až současná právní úprava. Snahou bude zaměřit se zejména na otázky řešené v praxi s ohledem na vývoj různých případů momentálně řešených českými či zahraničními soudy. Nelze opomenout světovou legislativu, která taktéž v posledních letech prochází významnými změnami ve vztahu nejen k počítačovým programům, ale zejména ve vztahu ke všem autorsky chráněným dílům.

Nebude snadné se s těmito otázkami vypořádat, jelikož většina z nich doposud nebyla řešena světovými soudy, natož pak soudy České republiky. Účelem práce je tedy poukázat na některé aktuální otázky, nastínit přístup české právní úpravy ve vztahu k těmto otázkám a zároveň se pokusit de lege ferenda nastínit možný vývoj legislativy i soudní praxe v rámci České republiky.

V práci se také budu průběžně věnovat možnostem autora v případě porušení jeho práv, zejména občanskoprávním institutům náhrady škody, bezdůvodného obohacení, opomenutí obecné povinnosti předcházet škodám, ale i jiným možnostem ochrany autorského práva, jakými jsou například různé druhy trestněprávní a správněprávní ochrany.

2. Právní úprava, definice pojmů

Z počátku bude třeba nastínit právní úpravu v České republice a vyjasnit si definice základních pojmů, se kterými se budeme nadále setkávat. Základním pramenem úpravy je zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen AutZ). Autorské právo náleží do oblasti práv duševního vlastnictví. Takové právo můžeme v objektivním smyslu chápat jako „soubor právních norem, které upravují společenské vztahy vznikající při tvorbě a společenském uplatnění děl literárních, vědeckých a uměleckých“[1]. V subjektivním smyslu jej pak chápeme jako „souhrn oprávnění, která autorovi vznikají, a která může na základě tohoto zákona uplatňovat ve vztahu jeho díla jako výsledku duševní tvůrčí činnosti“[2]. Autorské právo se považuje za právo přirozeně vznikající spolu s výtvorem a z toho důvodu není potřeba žádného dalšího úkonu, aby dílo bylo autorským právem chráněno. Stát toto právo nikomu nepřiznává, nýbrž je jakožto právo nezadatelné pouze chrání a vedle toho též stanoví způsob výkonu tohoto nezadatelného, přirozeného práva. Autorské právo je právem absolutním, působí erga omnes (má tedy univerzální povahu), z čehož vyplývá povinnost individuálně neurčených cizích osob zdržet se jakýchkoli neoprávněných zásahů do oprávnění nositele autorského práva.

Pro snazší orientaci si bude třeba vymezit několik základních pojmů. Nejprve si je třeba uvědomit, co znamená pojem software, případně počítačový program. Tyto jsou běžně užívány jako synonyma a tudíž jsou velice často volně zaměňovány. Software můžeme definovat jako programové vybavení, tedy sadu všech počítačových programů v počítači (na rozdíl od hardware, který zahrnuje všechny fyzické součásti počítače)[3]. Počítačový program je postup operací, který popisuje realizaci dané úlohy. Počítačový program může být vytvořen programátorem zápisem algoritmu v nějakém programovacím jazyce. S pojmem počítačový program, jakožto s fiktivním dílem, pracuje již zmiňovaný AutZ, přestože jej nedefinuje. Pro účely této práce můžeme

[1] Kříž, J. Ochrana autorských práv v informační společnosti, Praha, Linde 1999, 1. Vydání, str. 3

[2] tamtéž

[3] http://cs.wikipedia.org/wiki/Software

pojmy software a počítačový program brát jako synonyma a v textu s nimi budeme tímto způsobem zacházet.

V českém právním řádů byla ochrana počítačových programů jako specifických duševních výtvorů výslovně zakotvena až novelou předchozího autorského zákona č. 35/1965 Sb., z roku 1990 (zákon č. 80/1990 Sb.), která odstranila pochybnosti o věcném rozsahu autorského zákona ve vztahu k počítačovým programům. Ani v této úpravě však nebyla ochrana počítačových programů komplexní, jelikož ochranu neposkytovala jakémukoliv původnímu počítačovému programu. Ochranu bylo možno přiznat pouze tehdy, jestliže obdobně jako kterékoli jiné statky vytvořené tvůrčí činností fyzických osob splnily legálně požadované pojmové znaky autorského díla. Změna této koncepce se nepodařila ani novele autorského zákona z roku 1996 a tedy až do přijetí současného AutZ byla ochrana počítačových programů poskytována pouze na základě znaku tvůrčí individuality, což bylo v případě počítačových programů poměrně obtížně splnitelné. Ze současného AutZ již vyplývá, že počítačové programy mohou být na území České republiky předmětem absolutní ochrany právem autorským. To vše ale za předpokladu, že splní, podobně jako jiná autorská díla pojmové znaky děl uvedených v AutZ. To nás jednoznačně vede k rozdělení počítačových programů do několika skupin.

a) V prvém případě se bude jednat o počítačové programy, které splňují pojmové znaky děl podle AutZ, tedy zejména kritérium jedinečnosti výsledku tvůrčí činnosti. Tyto počítačové programy jsou chráněny v totožném rozsahu, jako jsou chráněna díla literární, aniž by se ve skutečnosti muselo o díla literární jednat. Platí pro ně tedy plně autorskoprávní režim, byť s určitými zvláštnostmi.

b) Do druhé skupiny můžeme zařadit díla, které sice nesplňují pojmové znaky autorského díla, které vyžaduje autorský zákon, ale splňují požadavek původnosti[4] ve smyslu původního duševního výtvoru. Žádná další kritéria pro určení, zda počítačový program je původní a může být autorskoprávně chráněn, se nepoužijí.

[4] §2 odst. 2 AutZ

Autorský zákon je tudíž hlavním pramenem ochrany počítačových programů v českém právním řádu. Lze však chránit i počítačové programy, které nesplňují pojmové znaky děl, ani kritérium původnosti duševní tvůrčí činnosti a které v důsledku toho nejsou ani předmětem ochrany absolutního práva autorského. V těchto případech však není vyloučena ochrana jinými právy duševního vlastnictví, zejména pomocí obchodního tajemství, know-how či nekalé soutěže. Existuje tedy možnost chránit počítačové programy jako předměty obchodního tajemství na základě zákona č. 513/1993 Sb., obchodního zákoníku (ObchZ), za předpokladu že splňují pojmové znaky podle tohoto zákona. V úvahu přichází jejich ochrana jako předmětů obchodního tajemství mimo ochranu před nekalým soutěžním jednáním dle §17 a násl. ObchZ, či v rámci zvláštní skutkové podstaty nekalého soutěžního jednání podle §51 ObchZ. Pokud by počítačové programy tyto pojmové znaky nesplňovaly, bylo by třeba zvážit možnost jejich ochrany pomocí generální klauzule nekalého soutěžního jednání ve smyslu §44 ObchZ.

Kdy vlastně počítačový program vzniká? AutZ uvádí, že dílo vzniká okamžikem, kdy je vyjádřeno v jakékoli objektivně vnímatelné podobě. V případě počítačových programů je situace trochu složitější. Ke vzniku díla postačí zachycení programu v podobě zdrojového kódu, tzn. není tedy nutné, aby byl program spustitelný na počítači[5].

[5] Telec, I., Tůma, P. Autorský zákon: komentář, Praha, C.H. Beck 2007, 1. vydání, str. 127

3. Druhy softwaru a způsob jeho užití

Autorský zákon vymezuje způsoby užití počítačových programů. Takové právo lze, kromě výjimky u děl volných, nabýt pouze smlouvou. Jedná se o smlouvu licenční, jejíž uzavírání upravuje §46 a násl. AutZ. V této kapitole bych rád nastínil rozdělení počítačových programů do určitých skupin, podle kterých lze následně odvodit způsoby jejich možného užití, aniž by bylo porušováno autorské právo.

3.1 Freeware

V tomto případě se jedná o volně dostupný a šiřitelný software, bez nároku autora na honorář. Autor si ponechává svá autorská práva a dovoluje užití zdarma pouze pro osobní potřebu nebo pro nekomerční účely. Vývoj takového programu je plně v rukou autora a není ani možné, aby v něm kdokoli cizí dělal různé úpravy a modifikace. Autor nezveřejňuje zdrojový kód a není dovoleno tento zdrojový kód zpětným způsobem z programu získávat. Pojem freeware však nesmíme zaměňovat za „volný software“. Volný software je program, ke kterému již nikdo nemá autorská práva, která zanikly uplynutím 70 let od smrti autora.

3.2 Shareware

Shareware je software chráněný autorským právem, který je možné volně distribuovat (zejména po internetu, formou CD/DVD atd.). Uživatel je má možnost takový software po určitou dobu zdarma zkoušet a přesvědčit se, zda mu vyhovuje. Po uplynutí určité autorem stanové lhůty je ovšem uživatel povinen řídit se licenčním ujednáním, tedy zpravidla za program zaplatit, nebo se například někde zaregistrovat. Pokud uživatel nemá o program nadále zájem, musí jej odinstalovat. Autorem stanovená zkušební lhůta („trial“) je obvykla stanovena v rozmezí 30-60 dnů.

3.3 Adaware (advertising-supported software)

V případě těchto programů se opět jedná o volně šiřitelný software, který je ovšem limitován v užívání například zobrazováním reklam či jiných podobných nepříjemností. Ani tento druh softwaru nesmí být volně měněn, ani nesmí být zabráněno zobrazování reklamy. V běžné veřejnosti se často setkáváme se zaměňováním pojmů adaware a spyware. Základní rozdíl mezi těmito je ve vědomí uživatele. Spyware se do počítače instaluje sám, tedy bez vědomí uživatele a obvykle má za účel sbírat různá

citlivá data, případně ohrozit stabilitu a funkčnost počítače. Adaware se instaluje v souladu s licenčními podmínkami a jeho funkce je čistě reklamní, nikoli škodlivá.

3.4 Open source software

Jedná se o software s otevřeným zdrojovým kódem. Otevřenost zde znamená jak technickou dostupnost kódu, tak legální dostupnost - licenci software, která umožňuje, při dodržení jistých podmínek, uživatelům zdrojový kód využívat, například prohlížet a upravovat.

3.5 OEM software

OEM licence (tzv. „Original Equipment Manufacture) je způsob užití počítačového programu vázaný na konkrétní kus hardwaru. Takový program může být užíván pouze s hardware, ke kterému byl dodán a nelze jej užívat samostatně.OEM software nelze nainstalovat na jiný počítač a při ztrátě nebo zničení takového počítače dochází k zániku OEM licence. Výhoda OEM softwaru je v jeho nižší pořizovací ceně tzv. krabicové verze. Funkčnost OEM i krabicové verze je stejná, cena však někdy může být až třetinová.

3.6 Komerční (krabicový, retail) software

Na závěr musíme zmínit to nejdůležitější – tedy plnohodnotný, krabicový, plně funkční a neomezený software. Autor poskytuje užívání takového softwaru na základě licenční smlouvy a to za úplatu. Není možné takový program modifikovat, vyjma zákonných výjimek. Jedná se obvykle o nejkvalitnější, cenově velmi nákladný a uživateli vyhledávaný software. Komerční software je oním „lukrativním“ zbožím, k jehož šíření dochází všemi možnými způsoby porušování autorského práva. O způsobech porušování autorského práva bude pojednáno dále.

4. Rozmnoženina pro osobní potřebu, záložní rozmnoženina a vlastnictví média jako mýty a fakta ve společnosti

4.1 Rozmnoženina pro osobní potřebu

Jedním z mnoha diskutovaných témat je tvorba rozmnoženiny pro osobní potřebu. AutZ tento pojem upravuje ve svém §30 jako tzv. volné užití díla. Takovému užití je třeba rozumět jako užití díla v soukromí uživatele. Účelem může být sebevzdělání, samostudium, ale i zábava a to vše za předpokladu, že je prováděno v rámci domácnosti[6], jakož i v rámci okruhu osob jemu blízkých[7]. Účelem takového užití nesmí být dosažení přímého či nepřímého hospodářského nebo obchodního prospěchu. Obecně tedy lze vytvářet záznam, rozmnoženinu nebo napodobeninu pro osobní potřebu. V případě počítačových programů však AutZ v souladu se směrnicí Rady 91/250/EHS o právní ochraně počítačových programů vyloučil tvorbu kopie pro osobní potřebu. Tato výjimka je absolutní – týká se veškerých počítačových programů, včetně her. V důsledku to tedy znamená, že i v soukromí je možno užití jakéhokoliv počítačového programu pouze se svolením autora, případně se svolením jiného vykonavatele autorských majetkových práv. Důvodem tohoto absolutního zákazu zjevně byla potenciální hrozba nekontrolovatelného a masového šíření počítačových programů a s tím spojené narušení majetkových zájmů autorů počítačových programů.

4.2 Záložní rozmnoženina

Mnoho uživatelů, ale i odborníků často zmiňuje pojem „záložní rozmnoženina“, který nesprávně zaměňují s tvorbou rozmnoženiny pro osobní potřebu. Záložní rozmnoženinu definuje AutZ ve svém §66, který stanovuje omezení autorských práv ve vztahu k počítačovému programu.

Tato úprava má ovšem zcela odlišný režim. Takovou záložní rozmnoženinu si může vytvořit pouze oprávněný uživatel a to pouze za podmínky, že je taková rozmnoženina nezbytná pro užívání počítačového programu. Takovou potřebou se rozumí například možnost oprávněného uživatele nově zavést (instalovat) počítačový

[6] §115 zákona 40/1964 Sb., občanského zákoníku

[7] §116 tamtéž

program při nahrazení starého hardware za nový či při změně operačního systému apod. Je zcela nerozhodné, zda je záložní rozmnoženina pořizována pro osobní potřebu či nikoli, neboť omezení autorského práva pro rozmnožování děl pro osobní potřebu se na počítačové programy nevztahuje, jak jsem již uvedl výše. Pojem oprávněného uživatele definuje například směrnice 91/250/EHS o právní ochraně počítačových programů, podle níž je takovým uživatelem kupující, nabyvatel licence, nájemce nebo osoba oprávněná užít program ve prospěch těchto osob.

Dle AutZ je oprávněným uživatelem rozmnoženiny počítačového programu oprávněný nabyvatel rozmnoženiny počítačového programu, který má vlastnické či jiné právo k rozmnoženině počítačového programu, a to za účelem jejího využití, nikoli za účelem jejího dalšího převodu, dále oprávněný nabyvatel licence nebo jiná osoba oprávněná užívat rozmnoženinu počítačového programu. Současné zákonné vymezení oprávněného uživatele počítačového programu není zcela v souladu s komunitárním právem a je poněkud nezřetelné a zavádějící. Interpretace tohoto pojmu ze strany Evropského soudního dvora je pro definitivní vyjasnění této záležitosti zřejmě nezbytná. Závěrem můžeme říci, že oprávněný uživatel musí mít, na rozdíl od tvorby rozmnoženiny pro osobní potřebu běžným uživatelem, specifické oprávnění k užití počítačového programu, aby mohl zhotovit záložní rozmnoženinu.

4.3 Vlastnictví média jako hmotného substrátu

Mezi další mýtus, který koluje mezi uživateli, lze zařadit vlastnictví prostředku, na kterém je počítačový program uložen – rozuměno tedy např. CD, DVD či jiný datový nosič. Mnoho uživatelů se domnívá, že koupí hmotného nosiče, tedy nabytím vlastnického práva k tomuto nosiči, se automaticky stávají oprávněnými uživateli a mohou tudíž takové dílo užívat všemi povolenými způsoby. Ve skutečnosti to tak není. AutZ rozlišuje právo vlastnické k nosiči dat (hmotnému statku) a právo autorské k dílu (nehmotnému statku). Každé z těchto práv se řídí vlastním režimem. K legálnímu užití počítačového programu je tedy třeba mít uzavřenou licenční smlouvu.

5. Softwarové pirátství a jeho nejčastější případy

Co je vlastně softwarové pirátství? Existuje mnoho různých definic, se kterými se běžně setkáváme. Například se jedná o „neoprávněné užívání softwaru, které je chráněného autorskými právy“[8]. Jiná definice zase pojem softwarového pirátství označuje jako útoky proti autorskému právu související s počítačovými programy k získání prospěchu pro sebe nebo jiného tj. s komerčním využitím[9]. Tím se zároveň vymezuje rozdíl mezi softwarovým pirátstvím a warezem či P2P, kde se zpravidla o žádné komerční užití nejedná. Pro mou práci jsem se softwarové pirátství rozhodl vymezit jako jakékoliv nakládání s autorsky chráněným dílem, tedy konkrétněji s počítačovým programem, které je v rozporu s AutZ. Dále se budeme zabývat jednotlivými případy. Kdy tedy k porušování autorsky chráněných děl dochází?

5.1 Používání počítačového programu bez licence

Jak již bylo uvedeno výše v kapitole o komerčním softwaru, je k legálnímu užití těchto programů potřeba souhlasu autora, nejčastěji tedy ve formě licence k danému počítačovému programu. Pokud je počítačový program užíván bez licence, jedná se o porušení AutZ. K takovému porušování dochází zejména mezi koncovými uživateli, tedy v domácnostech a ve firmách. Autor se proti těmto osobám může domáhat ochrany na základě §40 AutZ, ale také může požadovat náhradu škody či vydání bezdůvodného obohacení podle obecných právních předpisů – zejména podle zákona č. 40/1964 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen ObčZ).

5.2 Překročení licencí

Tento případ porušování autorsko právně chráněných děl se vyskytuje zejména ve společnostech. Jedná se o případy, kdy společnost má sice určitý počítačový program legálně zakoupený, má tedy licenci k jeho užití, ale následně překročí meze této licence. Běžně je taková licence určena k užití na jednom počítači. Porušení spočívá v současném užití tohoto programu na více počítačích. Snahou bývá úspora peněz a

[8] BSA (Business Software Alliance), http://www.bsa.org/country.aspx?sc_lang=cs-CZ

[9] Smejkal, V. a kol. Právo informačních a telekomunikačních systémů. 2., aktualizované a rozšířené vydání. Praha, C.H. Beck 2004, str.723

jakási falešná domněnka, že je vlastně vše v pořádku a k žádnému porušování práv nedochází. Opak je ovšem pravdou a takové jednání bezpochyby odporuje licenčním ujednáním a autor se může opět domáhat ochrany jak již bylo uvedeno výše. Odpovědnost za takto vzniklou škodu ponese společnost, tedy buďto její statutární orgány, případně jiné osoby v zaměstnaneckém poměru, které jsou vzhledem ke své pozici odpovědné za řádný provoz počítačových programů a jejich licencování.

5.3 Předinstalovaný software výrobci počítačů

Existuje mnoho společností zabývající se prodejem nových počítačů. Prodej počítače bez programového vybavení, tedy pouze ve formě hardware, již v dnešní době téměř neexistuje a tak se prodejci snaží na počítač již v době prodeje umístit značné množství počítačových programů. Pokud k umístění těchto programů nemají povolení autora nebo osoby vykonávající správu autorských práv k redistribuci, prodeji, instalování daného počítačového programu, dopouští se opět porušování AutZ. Získávají tím jakousi výhodu oproti konkurenci, jelikož v případě oprávněné instalace těchto programů se zvyšují náklady a cena logicky musí být vyšší. Autor se opět může domáhat ochrany podle AutZ i podle ObčZ. Stejně tak by se pravděpodobně mohla ochrany domoci společnost, která takovýmto porušováním autorských práv přichází o zisky z již výše uvedené konkurenční nevýhody.

5.4 Pronájem bez souhlasu autora

Pronájmem originálu nebo rozmnoženiny díla se rozumí zpřístupnění díla za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu poskytnutím originálu nebo rozmnoženiny díla na dobu určitou[10]. Takové jednání bývá opět v rozporu s licenčním ujednáním a tudíž zde opět nastupuje možnost autora domáhat se ochrany dle AutZ a ObčZ.

[10] §15 AutZ

6. Rozmnožování a sdílení pomocí internetu

Internet je v současné době nejmocnější médium. Ať chceme či nechceme, obklopuje nás a setkáváme se s ním v každodenním životě. Přináší mnoho pozitiv, které můžeme spatřovat například v rychlém přístupu k jakýmkoli informacím. Obecně lze říci, že internet náš život zjednodušil a zrychlil. Skýtá ovšem i značné množství negativních stránek. Za zmínku stojí například neomezené možnosti dětí dostat se k obsahu, který by se jim do rukou dostat neměl. A právě internet je prostředí, ve kterém se zrodily dva nejvýznamnější fenomény současné doby, jimiž bezpochyby jsou výměnné P2P (peer-to-peer) sítě, ale také tzv. warez scéna.

Co to vlastně warez znamená? Co to jsou P2P sítě a jaký je jejich vztah k warez scéně? Co bylo dřív a jaké jsou hodnoty a cíle? Jakým způsobem jsou v rámci těchto sítí porušovány práva k autorsky chráněným dílům a jakou odpovědnost můžeme vyvodit u osob spojených s těmito sítěmi? Na tyto a mnoho dalších otázek se pokusím odpovědět v následujících kapitolách. V současné době, kdy dostupnost a rychlost internetového připojení prožívá nebývalého rozkvětu, můžeme tyto dva fenomény řadit k základním a nejčastějším způsobům, jakými se nelegální software dostává k běžným uživatelům. Dříve se autorská práva k počítačovým programům porušovaly vypalováním datových nosičů, zejména CD a DVD.

Ještě před několika málo lety bylo internetové připojení poměrně vzácnou záležitostí. Poskytovatelů služeb tohoto druhu nebylo mnoho a pokud se již někdo rozhodl takovou službu objednat, musel vynaložit poměrně velké množství finančních prostředků. Takto draze zaplacená služba byla navíc na velice slabé úrovni. Rychlost připojení byla pomalá a v případě domácích uživatelů se tak často používala pouze k příjmu e-mailů, případně prohlížení webových stránek. To byly časy tzv. dial-up modemů, kdy připojení k internetu umožňoval pouze modem přímo připojený k telefonické přípojce, která v té době ještě navíc byla pouze analogová a připojení tak velice často nebylo stabilní. Přístup k rychlému internetu tak mělo jen pár vybraných jedinců pracujících ve velkých firmách, případně u poskytovatelů služeb připojení k internetu, nebo i těch, kteří se k rychlému internetu dostali na akademické půdě – tedy v prostorách a budovách vysokých škol. Zájem o autorsky chráněná díla byl v té době obrovský, ať už se jednalo o počítačové programy, či hudební a filmové nahrávky. Není

tedy divu, že se v této době objevilo mnoho jedinců, kteří si z této poptávky udělali jistý druh „podnikání“.

Stačilo mít tedy přístup k rychlému internetu a CD vypalovací mechaniku, kterých v té době taktéž nebylo mnoho, jelikož jejich cena se v počátcích pohybovala i okolo 200 000,- Kč za kus, což v porovnání se současností, kdy kombinovaná vypalovací i přepisovací CD/DVD mechanika lze pořídit za cca 500,- Kč, je opravdu nepředstavitelná částka. Pak už jen bylo třeba mít nějaký ten přístup k oněm autorsky chráněným dílům, dát si inzerát do novin či na různá jiná místa, případně rozhlásit nabídku mezi svými kamarády a mohlo se začít prodávat. V této době ještě počítačové programy nedosahovaly větších velikostí a tak bylo možno na jedno CD médium vypálit i větší množství programů, někdy se mohlo jednat i o desítky až stovky takových děl. Takto vypálené médium mělo pochopitelně poměrně vysokou cenu a bylo možné ho bez problémů prodat i ve větším množství. Cena jednoho takového CD média se pohybovala v rozmezí 500-5000,- Kč a vezmeme-li v potaz cenu prázdného CD média, která se pohybovala cca v rozmezí 200-300,- Kč, mohlo se jednat o poměrně slušný přivýdělek, samozřejmě nelegální. V této době ovšem ještě počítačové pirátství nebylo takovým problémem a tak mnoho lidem poměrně snadno procházely i výše zmiňované inzeráty v novinách nabízející autorsky chráněná díla.

S postupem času se situace začala výrazně měnit. Objevilo se mnoho nových poskytovatelů služeb připojení k internetu, tyto služby se stávaly kvalitnější, rychlejší, dostupnější a samozřejmě i levnější. To vše zejména proto, že se dramaticky zvyšovala konkurence na trhu a to logicky zapříčinilo především pokles cen, ale i obecné zkvalitnění služeb. Pro koncového zákazníka se tedy situace ubírala správným směrem, ne už tak pro autory počítačových programů a jiných chráněných děl. V dnešní době již připojení k internetu nabízejí poskytovatelé téměř na každém rohu, ceny jsou na velmi nízké úrovni a dostupnost a pokrytí se blíží 100%.

Současní uživatelé se již ani nenamáhají praktikovat něco takového, co bylo zmíněno výše. Rychlost a možnosti současného internetu jim umožnili šíření nelegálního softwaru mnohem rychleji, snadněji, efektivněji a především anonymněji.

6.1 P2P sítě

Na úvod je vhodné nastínit fungování a principy P2P sítí, které dramaticky zefektivnily sdílení nelegálního softwaru, ale i veškerých dalších děl chráněných AutZ a spolu se vzrůstajícím počtem uživatelů internetu umožnily doslova „komukoliv“ přístup k „čemukoliv“. P2P je označení architektury počítačové sítě, ve které spolu komunikují klienti (uživatelé) doslova jako rovný s rovným. Čistý pojem P2P vůbec nezná pojem server, jak se někteří mohou domnívat. Všichni klienti jsou na stejné úrovni a každý plní zároveň funkci klienta i serveru pro ostatní. Zjednodušeně se tedy jedná o výměnné sítě, prostřednictví kterých si uživatelé mezi sebou vyměňují data. Ať se nám to líbí nebo ne, slouží tyto sítě zejména pro šíření nelegálního obsahu, ať už se jedná o počítačové programy, hry, filmy, ale i hudební nahrávky a mnoho dalšího. Samozřejmě existují i uživatelé, kteří tyto technologie využívají k přenosu legálního obsahu, těch je ovšem minimum.

V rámci těchto sítí tedy dochází ke zpřístupňování rozmnoženin autorskoprávně chráněných děl. Nespornou otázkou je vznik autorskoprávní odpovědnosti osob, které rozmnoženiny děl veřejnosti takto zpřístupňují. Zejména se bude jednat o koncové uživatele o jejichž odpovědnosti je pojednáno níže. AutZ ve svém §18 odst. 1 definuje pojem sdělování díla veřejnosti. Takovým sdělováním díla se rozumí zpřístupňování díla v nehmotné podobě, živě nebo ze záznamu, po drátě nebo bezdrátově. Odst. 2 tohoto ustanovení dále stanoví, že sdělováním díla je taktéž zpřístupňování díla veřejnosti způsobem, že kdokoli může mít k němu přístup na místě a v čase podle své vlastní volby zejména počítačovou nebo obdobnou sítí. Uživatelé těchto sítí jednoznačně zpřístupňují autorsky chráněná díla veřejnosti bez souhlasu autora, či bez jakékoli platné licence.

Velmi složitým faktem ovšem bude selekce uživatelů porušujících právo výše uvedeným způsobem – tedy zpřístupňováním díla veřejnosti bez souhlasu autora. V prvé řadě budou v rámci výměnné sítě existovat uživatelé, kteří budou stahovat a šířit pouze obsah nechráněný autorským právem. Jak již bylo výše uvedeno, tyto sítě slouží jako velice efektivní nástroj pro šíření objemných souborů s minimálními nároky na hardware i připojení k internetu. Pro zajímavost lze uvést, že i společnost Microsoft poskytuje službu Live Update (v rámci této služby jsou Microsoftem zdarma

poskytovány aktualizace pro jeho počítačové programy) na bázi velice podobné P2P sítím, zejména torrentům. Další skupinu mohou tvořit uživatelé, kteří budou poskytovat obsah právně nezávadný – například volně přístupné hudební nahrávky, fotky z dovolené, či jakýkoliv jiný volně šiřitelný obsah a zároveň budou na svůj domácí počítač stahovat (ukládat) díla audiovizuální (hudební soubory ve formátu MP3, filmová díla ve formátu XviD[11] či x264[12]). Ani takové uživatele nelze postihnout, jelikož AutZ tyto díla řadí pod výjimku rozmnoženiny pro osobní potřebu (viz. kapitola 4.1).

Neoprávněného sdělování díla veřejnosti dle výše uvedeného §18 AutZ se budou dopouštět uživatelé, kteří budou buďto stahovat počítačové programy, jelikož na ty se nevztahuje výjimka pro osobní rozmnoženinu, případně budou sdílet (nabízet) jakákoli autorsky chráněná díla široké veřejnosti (v tomto případě postačí i nasdílení hudebního či filmového díla).

Další otázkou zůstává role a odpovědnost třetích osob, které provozují či uvádějí do oběhu zařízení, s jejichž pomocí k výše uvedenému zpřístupňování děl veřejnosti dochází. Tito provozovatelé či výrobci a tvůrci P2P systémů nefigurují jako sdělovatelé díla. Jejich úloha tedy spočívá v usnadnění sdělování děl veřejnosti třetími osobami. Běžně tak tyto osoby nenesou odpovědnost dle AutZ za sdělování děl veřejnosti, mohou však být za určitých okolností označení za tzv. prostředníky – tedy poskytovatele služeb, které třetí osoby využívají k porušování nebo ohrožování autorského práva. K jejich odpovědnosti bude pojednáno dále v kapitole o odpovědnosti provozovatelů P2P sítí.

Důsledkem porušování autorských práv v rámci těchto sítí jsou mnohé žaloby na provozovatele těchto sítí (převážně v USA), podávaných zástupci autorů a organizacemi jako je RIAA či MPAA. Často se poukazuje na to, že prostřednictvím těchto sítí se může šířit i obsah mnohem závažnější, jako je například dětská pornografie. Zastánci

[11] www.xvid.org, MPEG-4 kompatibilní kodek s otevřeným kódem užívaný ke kompresi videa

[12] http://www.videolan.org/developers/x264.html, kodek pro kompresi videa ve vysokém rozlišení

však argumentují tím, že možnost zneužití takových sítí k nezákonným účelům nesmí bránit jejímu legálnímu využívání.

Současné výměnné sítě lze podle typu protokolu, který využívají, rozdělit na tři základní velké skupiny. První z nich je zcela decentralizovaná. Každý klient může být současně serverem, který se pro ostatní klienty stará o řízení seznamu souborů, tedy indexu. Právě ten je totiž při výměně klíčový. Mezi tyto protokoly patří Fastrack, nesprávně zcela ztotožňovaný se sítí KaZaA, Gnutella, Gnutella G2 a některé další. Výhodou těchto systémů je především jejich mohutnost a naprostá autonomie.

Druhý typ systémů sází na jiný princip. Jsou v nich jak počítače (klienty), které sdílejí informace, tak i servery, které se starají o udržení indexu, přičemž servery jsou dedikované, k žádnému jinému účelu neslouží. Servery jsou mezi sebou pro zvýšení efektivity propojeny, komunikují spolu a existuje jejich centrální evidence. Výhodou těchto sítí (e-Donkey) je především rychlost hledání informací a spolehlivost alokace jejich zdrojů (v případě Gnutelly máme jen malou šanci, že při stahování určitého souboru využijeme všechny dostupné zdroje, respektive je využijeme efektivně). Nedostatkem je naopak poměrně snadná možnost radikálně snížit kvalitu sítě odpojením několika nejvýkonnějších serverů, protože bez nich výměnný systém neexistuje.

Posledním typem jsou systémy založené na jediném centrálním serveru a klientech, kteří si jeho prostřednictvím vyměňují soubory. Tyto sítě (OpenNap, DirectConnect) v současné době nepředstavují žádné celistvé globální řešení sdílení, ačkoliv v minulosti tomu tak bylo. Jejich výhody i nedostatky jsou jasné: vysoká kvalita, žádná redundance.

Mezi nejznámější P2P sítě patří Napster, BitTorrent, Kazaa, Gnutella, Direct Connect, Akamai, Applejuice, CAKE, ed2k, FileTopia, Freenet, Hypercast, PeerCast a mnoho dalších. Níže jsou popsány ty nejdůležitější, zlomové či nejpoužívanější.

6.1.1 Napster

Napster byla síť vytvořená Shawnem Fanningem a fungující v letech 1999-2001. Umožňovala uživatelům jednoduše kopírovat a distribuovat hudbu ve formátu MP3. V únoru 2001 měla síť již přes 25 milionů uživatelů, což způsobilo rychlý a citelný pokles prodeje hudebních nosičů. Na tento pokles zareagovali producenti hudby

sdružení v RIAA a již v prosinci 1999 byla podána první žaloba. Během roku 2000 se připojilo několik hudebních skupin v čele s Metallicou. Napster se hájil tím, že pouze poskytuje službu spojení uživatelů internetu. Bylo však prokázáno, že Napster měl kontrolu nad sdíleným obsahem sítě (díky svému vlastnímu serveru, který indexoval soubory) a dále že měl z provozování majetkový prospěch z prodeje reklamního prostoru. Tím byly dny Napsteru sečteny, soud uznal žalované vinnými z tzv. sekundární odpovědnosti a v červenci 2001 nařídil zastavení této sítě.

6.1.2 Kazaa

Další z výměnných sítí, kterou vytvořili Niklas Zennström a Janus Friis (kteří později vytvořili populární program pro internetové telefonování Skype). Tato síť byla založena na protokolu FastTrack.

6.1.3 BitTorrent

BitTorrent původně nevzniknul jako další ze systémů ke sdílení dat, ale jako distribuční mechanismus pro velké soubory. Pokud chcete velký soubor rozšířit mezi co největší počet uživatelů, musím být vybaven velmi silným serverem, odkud si jej budou moci stahovat. Tato skutečnost jednak zvyšuje náklady na distribuci a jednak při enormním zájmu o soubor snižuje jeho dostupnost, například pokud je webový server přetížen nebo vlivem velkého množství požadavků dokonce vyřazen z provozu. Alternativou je nabídnout možnost stahovat soubor nejen z mého serveru, ale současně z počítačů těch, kteří si jej již stáhli. Aby bylo možné stahovat jediný soubor z více zdrojů současně, je třeba jej virtuálně rozdělit na množství menších částí. Každá tato část je kouskem skládačky, která se nakonec složí do původní podoby celku. Každá část může pocházet z jiného místa. Jediné, co je k tomu třeba, je přesný popis celku a výchozí zdroj – místo s původní kopií daného souboru.

Tento popis je u technologie BitTorrent uložen v samostatném souboru s příponou .torrent. Jakmile je (pomocí ovladače integrovaného do webového prohlížeče nebo jiného klientu - aplikace) zahájeno stahování souboru, stává se tento klient zároveň prvkem, který již stažené součásti nabízí dál. Tím pádem stoupá dostupnost těch kusů celku, které již byly staženy, a pokud stahuje (a zároveň uploaduje) dostatečný počet

uživatelů, i celku jako takového. Jediné, co je kromě původní kopie souboru třeba distribuovat, je popis (.torrent) nebo alespoň odkaz na něj.

Jak vyplývá z předchozího, BitTorrent je a není výměnnou sítí. Využívá výhod P2P technologií a distribuovaných přenosů, avšak neumožňuje vyhledávání. Každý soubor si vytváří jakoby vlastní výměnnou síť (prostřednictvím souboru popisu), avšak o žádné malé ani globální „torrent“ síti nelze hovořit. BT je tak vlastně jakýmsi hybridem.

V případě torrentových výměnných sítí dochází k zajímavé právní situaci. Jak již bylo výše naznačena, stává se jakýkoli uživatel, který začne ukládat dílo do svého počítače, zároveň serverem pro ostatní uživatele – začne jim tedy automaticky již stažené části díla nabízet. Jak se k tomuto staví naše právní úprava? Základem bude úprava §2 odst. 3 AutZ, který stanoví, že právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav. V případě této skupiny předmětů tedy může běžně nastat situace, že i část díla obecně autorskoprávně nechráněná, bude v tvůrčí oblasti počítačových programů požívat autorskoprávní ochrany, pokud bude vykazovat znak tvůrčí původnosti. Jak můžeme toto pojetí aplikovat v praxi? Opět se bude jednat o velice složitou otázku, která v praxi zatím nebyla řešena. Počítačový program je jako takový zapsán ve formě zdrojového kódu, který následně přeložit a zobrazit umí až počítač. Lze si teoreticky představit, že část tohoto zdrojového kódu bude představovat určitou část autorského díla, kterou lze chránit samostatně. Vezměme pro příklad počítačovou hru, která bude mít svého hlavního hrdinu – tedy autorem vymyšlenou, vytvořenou (naprogramovanou) postavu, která bude zapsána ve formě zdrojového kódu. Bude tedy tvořit část zdrojového kódu celé hry a bude požívat ochrany AutZ za předpokladu splnění podmínky původnosti.

V případě torrentového protokolu dochází k nabízení již stažených částí díla. Z mého pohledu však vidím problém v neuspořádanosti a náhodnosti stahovaných a zároveň již poskytovaných částí díla. Pokud začne uživatel stahovat autorsky chráněné dílo, neprobíhá toto stahování od začátku zdrojového kódu až do jeho konce, nýbrž probíhá zcela náhodně. Navíc toto stahování probíhá v tak malých částech, kdy jedna taková část ani zdaleka nemusí představovat výše zmiňovanou postavu ve hře, ale může se jednat o nepatrný zlomek této postavy, tedy část kódu, která sama o sobě nedává

žádný srozumitelný smysl a nemá žádnou hodnotu ani použitelnost. Prakticky tedy lze dosáhnout situace, kdy bude uživatel mít staženu polovinu autorsky chráněného díla, ale žádná z již stažených částí nebude přímo souviset s ostatními částmi.

Z pohledu trestního práva pravděpodobně lze nalézt řešení v podobě pokusu trestného činu dle §152 TZ. V takovém případě bude vyžadováno úmyslné jednání pachatele bezprostředně směřující k dokonání individuálně určeného trestného činu (alespoň v základních znacích), které se bude vyznačovat tím, že nebylo dokonáno. Uživatel, který by sdílel jednotlivé, byť nesamostatné části autorsky chráněného díla, by s největší pravděpodobností tyto podmínky splňoval a mohl by tedy být trestně stíhán. To vše ovšem za předpokladu, že by se dopustil škody v určitém rozsahu, aby svým jednáním naplnil znaky trestného činu.

Otázkou zůstává, zdali je prakticky možné, účelné a efektivní každého takového jednotlivého uživatele sdílejícího chráněná díla trestně stíhat. Takovým postupem by zřejmě došlo k zahlcení justice, pokud by zároveň nebyly zřízeny specializované soudy (samosoudci), kteří by na tuto činnost byli vyškoleni a byli by schopni zpracovat a rozhodnout v krátkém časovém úseku velké množství podobných případů.

Jakým způsobem se tedy k tomuto problému postavit? Nebo jak se k němu postaví naše justice, bude-li někdy v budoucnu takový problém řešit? Lze odpovědnost za sdílení dovodit až v případě nabízení díla jako celku, nebo i jeho jednotlivých součástí? Nebo judikatura dovodí hranici, od které se bude již sdílení částí díla považovat za dílo celé? Uživatelé těchto výměnných sítí se zcela jistě budou bránit argumenty, že neposkytli dílo celé, případně že ta část zdrojového kódu, kterou poskytli, nedává sama o sobě žádný smysl a nesplňuje tak znaky zákona potřebné pro ochranu díla.

6.1.4 DirectConnect

Velice oblíbený systém v České republice. Má střední míru decentralizace. Peer klienti nekomunikují přímo, ale připojují se na jednotlivé huby. Hub je server poskytující klientům služby, informace o klientech, vyhledávání a chat. Nevýhodou je malý počet uživatelů na jednom hubu a tudíž i malý objem sdílených dat. Huby mezi sebou vzájemně nekomunikují.

6.2 Warez

Warez je kategorie sama pro sebe. Vznikla daleko dřív, než jakákoli jiná P2P síť. Pokusím se v této kapitole warez komplexně popsat a rozebrat. Pojem warez však obsahuje mnoho dalších pojmů, které v českém jazyce nemají svůj vlastní ekvivalent. Uživatelé je používají v původním výrazu, tedy v angličtině. Některé z nich se dále pokusím vysvětlit.

Pod pojmem warez se nám vybaví pirátský software, tak to ovšem není. Warez je především komunita, skupina lidí, kteří mají něco společného. Této komunitě se říká „scéna“. Warez scéna je tedy skupina lidí, mající přesně danou hierarchii, v níž každý člen má své místo, svou úlohu a která je přísně uzavřená. Jak říká jedno staré přísloví warez scény: „warez není právo, je to výsada a privilegium“. Z tohoto přísloví můžeme usuzovat, že scéna není pro každého a dostat se do ní není zcela jednoduchá záležitost. Historie warez scény sahá do počátků PC, kdy se první členové začali adaptovat na stále více populární a rozšířenější PC z již skomírající Amigy, Commodore 64, Atari či ZX Spectrumu. V té době se jednalo převážně o hry, jejichž velikost byla v porovnání s dnešními produkty směšná. Nesmíme ovšem zapomenout, že v té době veškerá komunikace probíhala na soukromých BBS (Bulletin Board System), což byly komunikační počítače, ke kterým se uživatelé přímo připojovali komutovanou telefonní linkou. Rychlost těchto telefonních linek byla velmi pomalá. Později byly BBS nahrazeny FTP (File Transfer Protocol) servery, po kterých se produkty warez scény šíří dodnes. Technologie zůstala stejná, změnila se však rychlost internetu a kvalita FTP serverů. Komunikace mezi členy scény nyní probíhá pomocí protokolu IRC (Internet Relay Chat), který se především díky své rychlosti a bezpečnosti stal oblíbeným a vydržel až do dnešní doby. Další z prvků zvyšující bezpečnost komunikace mezi členy warez scény jsou tzv. bouncery a proxy servery. Jedná se o počítače umístěné na bezpečném místě, na které se daný člen připojí a teprve z nich se připojí například na již zmíněný FTP server, nebo na IRC server. Tím do řetězce vloží další článek a zvyšuje svou bezpečnost, minimálně tím, že na FTP serveru není přímo vidět IP adresa jeho počítače (každý počítač v internetu má přidělenou unikátní adresu, podle které ho lze přesně vyhledat a identifikovat – IP adresu).

Warez scéna tedy funguje ve dvou úrovních. První je komunikační – tedy pomocí IRC, převážně na Efnet a Linknet serverech. Druhá úroveň je datová, tedy FTP servery. Každý takový FTP server má své unikátní jméno, svou IP adresu (obvykle schovanou za bouncerem) a své specifické datové složení. Zároveň má každý FTP server svůj unikátní kanál (channel, chann – tedy chatovací místnost na IRC), na který se člen dostane pouze pomocí speciálního příkazu po přihlášení na FTP server. Tento příkaz se nazývá „invite“ a jde o jakousi formu pozvánky na IRC kanál, bez které se uživatel na kanál nemá možnost dostat. Dalším ochranným prvkem IRC kanálu je jeho specifické heslo a posledním prvkem je tzv. „blow-key“, což je ve své podstatě šifrovací klíč pro komunikaci na samotném kanálu. Bez něj uživatel vidí pouze nesmyslnou směs znaků, ze které nic nerozluští. Po zadání všech klíčů a pozvánky může konečně číst a psát na daném kanále.

Samotný přístup na FTP server je chráněn uživatelským jménem, heslem a navíc se vyžaduje od uživatele fixní IP adresa, která bude na FTP serveru uložena a pouze z této adresy se bude možné připojit. Na fungování kanálu dohlíží bot, což je naprogramovaný skript, který je velice snadno programovatelný a dá se prakticky neomezeně rozšiřovat a vylepšovat. Tento bot plní na daném kanále mnoho funkcí. Dohlíží zejména na pořádek a na chování uživatelů. Kromě toho funguje jako informační skript o tom, co se zrovna děje na daném FTP serveru. Když se například na FTP server začne něco nového nahrávat, bot to ihned oznámí na kanále. Obvykle bot vypíše i takové detaily, jako který uživatel začal danou věc nahrávat, do jakého adresáře, jakou rychlostí atd. Tím jsme si popsali obě sféry fungování warez scény a nyní se můžeme zabývat tím, co vlastně taková scéna produkuje.

6.2.1 K čemu slouží a co produkuje?

Hned ze začátku bude třeba seznámit se s dalším základním pojmem, kterým je „release“. Release je vlastně výsledný produkt warez scény. Jedná se o hotový datový balík, který je po stažení plně funkční. Cesta k takovému produktu je poměrně zdlouhavá a k pochopení fungování celé warez scény je potřeba si tento proces popsat.

O co tedy vlastně jde? V rámci warez scény funguje mnoho tzv. release groups (vydávajících skupin), které mezi sebou soupeří o to, kdo daný film, hudbu, program či hru vydá jako první. Z toho tedy plyne, že skupina, která jako první vytvoří release

daného produktu, vítězí. To je jeden z pilířů warez scény. Z takového vítězství plyne prestiž, respekt a uznání ostatních skupin a členů warez scény. Leckdy se jedná doslova o vteřiny, které rozhodují o vítězství té či oné skupiny, protože na daném releasu jich často pracuje zároveň několik.

Tím se dostáváme k prvnímu článku tvorby releasu a tím je „supplier“. Supplier může být člověk, který dané skupině dodává hardware na tvorbu FTP serverů, ale především je to člověk, který skupině dodává nové, nikým doposud nevydané produkty. Jako český ekvivalent pro takového člověka můžeme použít termín „zásobovač“. Tito lidé bývají z řad IT publicistů, oskarových kritiků, recenzentů v časopisech, beta-testerů či prodejců. Jde o základní kámen celé skupiny, protože bez něj by doslova nebylo co dělat a všichni ostatní členové skupiny by se stali zbytečnými.

Dalším členem skupiny je cracker/ripper. Takový člověk má na starosti daný produkt zbavit všech ochran, případně ho převést do formátu použitelném v rámci warez scény. Crackují se zejména počítačové programy, hry a ripují se hudební a filmová CD/DVD/Bluray disky. Ripnutí hudebního CD znamené jeho převedení do formátu .mp3, v případě filmu se jedná o převedení do formátu XViD či dnes již modernějšího x264. Crackování znamená zbavení produktu všech ochran proti kopírování, případně vytvoření drobného upraveného souboru (cracku), který nahradí původní soubor po instalaci, čímž eliminuje veškeré ochrany a umožní bezproblémové spuštění daného počítačového programu či hry.

Dalším článkem je tzv. „packager“, což je člověk, který produkt již zbavený o veškeré ochrany upraví do formátu, ve kterém se může podle pravidel šířit v rámci warez scény. V praxi to znamená, že data zkomprimuje do přijatelné podoby (v současnosti jde o 15/50/100/150MB veliké soubory), přidá k nim tzv. sfv soubor (kontrolní soubor obsahující jednotlivé CRC součty všech archivů, sloužící pro kontrolu, zda byly všechny archivy nahrané/stažené v pořádku) a v neposlední řadě k releasu přidá tzv. nfo soubor. Funkce nfo souboru je, jak již samotný název napovídá, čistě informativní. Jde o soubor v textovém, případně grafickém (ASCII, ANSI) vyhotovení, ve kterém skupina uvádí informace o svém releasu. Zejména o jeho názvu, velikosti, datu vydání, způsobu instalace atd. Mnoho skupin zde také uvádí informace týkající se skupiny samotné a skupin, ke kterým chovají respekt a úctu.

V tomto momentu přichází další část řetězce – nahrání již hotového releasu na vybrané FTP servery. Těmito vybranými FTP servery jsou tzv. affil FTP servery. Co to vlastně znamená? Každá release skupina má vybraných několik FTP serverů, na nichž je domluvena s majitelem (případně správcem) na exkluzivitě. Výhoda této exkluzivity spočívá v tom, že tam daná skupina vždy umístí svůj release jako první ze všech ostatních serverů po celém světě.

Pro takové případy má skupina svůj vlastní adresář, do kterého release nahraje a posléze jednoduchým skriptem spustí tzv. PRE. To spočívá ve zobrazení daného releasu všem ostatním členům scény. Výhodou tedy je, že při PRE je release kompletní na všech affil FTP serverech a na ty ostatní se už jen šíří pomocí kurýrů, o nichž však pojednáme dále. Na oplátku mají skupiny na svých affil FTP serverech mnoho výhod, ze kterých mohou čerpat. Čím lepší a známější skupiny mají svůj affil na daném FTP serveru, tím větší prestiž daný FTP server získává. Existují i různé druhy žebříčků, kde jsou FTP servery hodnoceny. Hodnotí se zejména rychlost daného FTP serveru, jeho kvalita hardwaru, stabilita, doba po kterou server již funguje a v neposlední řadě také počet a kvalita affilů.

FTP serverů existuje mnoho. Od běžných a pomalých, kterých je většina, až po velice rychlé. Elitní servery se vyznačují malým počtem uživatelů (obvykle okolo 50) a vysokou přenosovou rychlostí, která je ceněna zejména skupinou kurýrů. V současné době není výjimkou ani FTP server na internetové lince dosahující rychlosti až 10GBit, ani FTP server o velikosti 100TB a více.

Abychom uzavřeli výčet členů warez skupiny, musíme ještě zmínit ty nejvyšší, kteří obvykle skupinu či server řídí. V případě skupiny se jedná o leadera (vůdce), který obvykle shání nové lidi, řídí a organizuje činnost skupiny a také dbá o čistotu a prestiž skupiny. Jeho pomocníky bývají councils, což jsou většinou spoluzakladatelé skupiny, kteří pomáhají leaderovi, zastupují ho v době jeho nepřítomnosti a tvoří pravidla pro skupinu. Ze strany vedení FTP serverů musíme zmínit siteopy, což jsou lidé, kteří spravují a dohlíží na daný FTP server. Na takovém serveru pak mají na rozdíl od běžných uživatelů veškerá práva a na nich závisí bezproblémový chod celého serveru, včetně všech skriptů. Časté jsou případy, kdy siteop je zároveň owner (majitel, kterému

server fyzicky patří a který se o něj obvykle lokálně stará). Stává se ovšem, že jde o dvě rozdílné osoby.

Poslední zmínka o členech skupin bude patřit coderovi, což bývá schopný programátor, který v dané skupině má na starosti skripty a různé drobné pomůcky usnadňující práci skupiny. Tester zase zkouší funkčnost releasů dané skupiny, aby byla jistota, že jejich práce je kvalitní a nikdo je nebude do budoucna opravovat.

6.2.2 Jak se warez šíří?

Jak jsme si již výše popsali, každý release z počátku objeví jen na pár vybraných FTP serverech. Jak se ale dostane na ostatní? Část warez scény tvoří uživatelé, kteří si takto vytvořený release pouze stáhnou na svůj domácí počítač a nic dalšího s ním nedělají.

Uvnitř scény ovšem existuje podstatná skupina uživatelů, která se nazývá „curry groups“ (tzv. kurýrské skupiny, tradeři). Jde o členy, jejichž práce spočívá v šíření releasů mezi FTP servery. Ihned po zveřejnění releasu na oněch pár vybraných FTP serverech začíná nelítostný boj o body. Ano, podstata šíření spočívá opět v prestiži a bodech, které za rychlé přesunutí kurýři získávají. Opět zde existují různé druhy žebříčků, kde lze kurýry porovnávat a sledovat, kolik dat a na jak hodnocené servery přenesli. Nejlepší kurýři tráví mnoho hodin denně u svých počítačů a čekají, až budou moci něco rozšířit. Tito lidé se obvykle sdružují v těch nejlepších kurýrských skupinách, což jim opět přidává na prestiži. Objeví-li se totiž nový release, jde o pouhé vteřiny, než se objeví na ostatních FTP serverech. Ano, vteřiny, tak rychlé jsou současné přenosy a reakce těch nejlepších kurýrů. Vše samozřejmě probíhá v rámci warez scény a kterýkoli kurýr by byl přichycen při šíření těchto releasů například na P2P sítě, byl by nemilosrdně smazán a vyhozen ze scény. Stejně tak pokud by byl kterýkoli člen warez scény přichycen při prodeji, nebo jakémkoli jiném zisku z těchto produktů, čeká ho opět stejná sankce.

6.2.3 Má warez pravidla?

Jak jsem již zmínil několikrát výše, warez scéna má mnoho pravidel, ať už psaných, tak nepsaných. Mezi základní pravidla patří například „non profit“, která všem členům zakazuje jakýkoli zisk z této činnosti. Dalším pravidlem může být zákaz šíření

releasů mimo scénu, protože vše by mělo být přístupné jen mezi členy uvnitř, nikoli každému. Z toho samozřejmě plyne další pravidlo, že warez není právo, ale je to výsada či privilegium, není tedy pro každého.

Mimo tyto základní pravidla existují ještě další dvě skupiny pravidel, o kterých se zmíním pouze všeobecně. První skupinu tvoří tzv. scene-rules, což jsou obecná pravidla scény pro tvorbu veškerých releasů. Jde tedy o jakési obecné standardy a technické specifikace, které daná skupina musí při tvorbě releasu dodržet, aby je nikdo další nemohl v budoucnu opravit či zesměšnit. Druhá sada pravidel se nazývá site-rules. V tomto případě se jedná o pravidla daného FTP serveru. Každý FTP server v rámci scény mívá odlišná pravidla a zásady. To obvykle plyne z požadavků majitelů těchto serverů, případně jejich správců. Na každý FTP server tak může být šířen je určitý druh releasů, například pouze filmy, hudba, nebo jen hry a počítačové programy. Některé povolují vše, jiné jsou o něco ochuzené. Těmito pravidly se řídí zejména kurýři, aby nešířili něco, co zrovna není dovoleno. Scene-rules vznikají souhlasnou dohodou všech či většiny vydávajících skupin uvnitř scény, site-rules vznikají pouze na základě rozhodnutí daného majitele nebo správce serveru.

6.3 Odpovědnost za warez

Tato problematika je sama o sobě velice složitá a rozsáhlá a pro komplexní analýzu by vyžadovala mnohem širší prostor, než tato práce poskytuje. U všech článků řetězce této komunity by odpovědnost byla jiná a velice těžko prokazatelná v rámci naší legislativy. Jako praktický příklad je v kapitole 7.4.1 uveden rozbor možné odpovědnosti provozovatelů FTP serveru, který sloužil výlučně pro potřeby warezové komunity.

6.4 Warez a P2P?

Mnoho lidí tyto pojmy nesprávně považuje za jedno a to samé. Jak jsme si již výše popsali, warez je především komunita, skupina lidí, kteří něco tvoří. Na druhou stranu P2P se také vyvíjí. Od počátku je velký boj mezi warez scénou a P2P sítěmi. Scéna se snaží hlídat své produkty, aby se nedostávaly na P2P sítě, kde k nim mají přístup běžní uživatelé.

To ovšem není zcela reálné, protože scéna už není to, co dřív bývala. Je v ní mnoho neznámých lidí, kteří se chovají proti základním pravidlům. A tak stačí jeden takový člověk, který release scény nahraje na některou z P2P sítí a tím vše pokazí. Takový release se během několika málo minut rozšíří na všechny ostatní P2P sítě a během velice krátké doby k němu má přístup v podstatě kdokoli. To ovšem není, nebyl a nikdy nebude cíl a účel warez scény. Pokud je někdo při takové či podobné činnosti přichycen, na warez scéně skončil.

Můžeme tedy říci, že ještě donedávna P2P pouze parazitovala a žila z warez scény, ale v poslední době se situace začíná měnit. Komunita kolem P2P sítí se začala značně diferencovat a začala vytvářet své vlastní releasy, které se šíří pouze prostřednictvím P2P sítí. Postupně tedy vznikají dva rozdílné systémy (komunity), které dělají v podstatě totéž. Rozdíl je v tom, že warez scéna má dlouhou historii, je uzavřená a její účel není zpřístupnit „všechno a všem“, nýbrž se jedná o soutěžení skupin mezi sebou.

Zatímco P2P slouží k uspokojování potřeb kohokoli, kdo se přihlásí, vytvoří si na dané síti svůj účet (některé P2P sítě přijímají uživatele pouze na pozvání) a může začít stahovat. Princip těchto sítí je ovšem založen na současném sdílení dat. Uživatel, který si chce něco stáhnout a uložit na svůj domácí počítač, zároveň stahovaná data sdílí a nabízí je tak široké veřejnosti, což je v rozporu s AutZ. Warez scéna funguje trochu odlišně, nemá princip sdílení a mnoho jejích členů si data pouze stahuje k sobě.

Dovolil bych si tvrdit, že warez scéna a P2P tvoří v současné době až 90% a více nelegálního šíření počítačových programů, ale i všech ostatních autorskoprávně chráněných děl. Umožnil to velmi rychlý nástup informačních technologií, zejména internetu, se kterým nestačí zákony držet krok.

Po celém světě probíhá mnoho soudních sporů, jejichž výsledky jsou ne vždy zcela přesvědčivé. V evropském parlamentu proběhl pokus o přijetí návrhu „třikrát a dost“, který spočíval v odpojení uživatele od internetu, pokud byl 3x přichycen při sdílení autorsky chráněného obsahu. Poslanci ovšem návrh neschválili s odůvodněním, že přístup uživatelů k internetu nesmí být omezen bez předchozího rozhodnutí soudních orgánů.

Přijímání podobné legislativy právě probíhá na území Francie. Do podvědomí široké veřejnosti se dostala pod názvem „HADOPI“[13]. Tento návrh zákona však zamítla francouzská Ústavní rada, která posuzuje soulad zákonů s ústavou. Zamítnut byl především hlavní bod tohoto zákona – tedy možnost odpojení uživatele od internetu a tím vlastně celý zákon ztratil smysl. Ústavní rada poukazovala na to, že odstřižení někoho od placené služby, jakou je internet, může být důsledkem jedině rozhodnutí soudu, ne administrativního orgánu. To je v podstatě totéž, co opakovaně hlásal na adresu „třikrát a dost“ Evropský parlament: „přístup uživatelů k internetu nesmí být omezen bez předchozího rozhodnutí soudních orgánů“.

V současné době byla umírající legislativa „HADOPI“ pozměněna patnácti dodatky, z nichž ten zásadní řeší problém, kvůli kterému byl původní návrh zákona zamítnut Ústavní radou. V novém návrhu může veškeré sankce může nařídit jen soud. Odpojování od internetu samozřejmě zůstává a aby však postihů a sankcí nebylo málo, přidává nový návrh na seznam trestů několik zajímavostí. Kupříkladu pokud se již odpojený hříšník bude snažit změnit svého poskytovatele internetového připojení, může mu být uložena pokuta až do výše 3,750 € (v přepočtu cca 100.000,- Kč). Co když ovšem s poskytovatelem internetového připojení uzavře smlouvu někdo z blízkého okolí hříšníka? Například někdo další z rodiny, s níž hříšník žije ve společné domácnosti? V takovém případě bude zřejmě hříšník opět připojen k internetu a vše začne nanovo. Velice zajímavá je též situace, kdy se hříšník pokouší vyhnout odpovědnosti tvrzením, že jeho počítač byl zneužit například tím, že se někdo cizí připojil na jeho nezabezpečenou či nedostatečně zabezpečenou bezdrátovou síť. I v takovém případě lze uložit pokutu až do výše 1,500 € (v přepočtu cca 40.000,- Kč). V případě samotného základního prohřešku porušování autorských práv může být kromě až ročního odpojení od internetu uložena pokuta až do výše 300,000 € (v přepočtu cca 7.800.000,- Kč) a nepodmíněný trest odnětí svobody až na tři roky.

Perličkou na závěr zůstává fakt, že poskytovatelé připojení k internetu budou nuceni do smluv o poskytování internetového připojení zahrnout informace o výši trestů za porušování autorských práv a nejspíše si budou také sami vést a udržovat seznamy

[13] High Authority for the Diffusion and Protection of Internet Creations

hříšníků, jelikož nebude existovat žádná centrální databáze. Zákon počítá se vznikem stejnojmenného národního úřadu (HADOPI), který bude v případě zjištění nelegálního stahování uživatelem postupovat následujícím způsobem. Nejprve zašle uživateli varovný e-mail oznamující, že stahovaný obsah je chráněn autorským právem a tudíž se jedná o nelegální stahování. Pokud uživatel nebude na e-mail reagovat a bude nadále pokračovat, zašle úřad uživateli formální dopis a pokud ani poté uživatel nepřestane se stahováním nelegálního obsahu, bude třetí krok již plně v rukou francouzských soudů, kteří budou oprávnění uživatele od internetu odpojit. Nový návrh zákona byl velmi rychle schválen senátem a nyní čeká na své hlasování v Národním shromáždění, které bylo odloženo až na září roku 2009.

Podobná legislativa je nyní zvažována či dokonce již přijímána v mnohých zemích, nejen v rámci Evropy. Jako příklad můžeme uvést Singapur či Nový Zéland. Právě v případě Nového Zélandu byl předložen již zrevidovaný návrh zákona, který přenáší důkazní břemeno na nositele autorských práv, kteří budou mít povinnost prokazovat u soudu porušování jejich autorských práv. V případě úspěchu při dokazování bude dotyčný viník pokutován, či následně odpojen od internetu.

Další podobný zákon již platí ve Švédsku, kde nositelé autorských práv možnost domáhat se soudně odhalení identity uživatelů sdílejících díla, jimž je poskytována autorskoprávní ochrana. To vše však opět za předpokladu, že u soudu toto sdílení budou schopni prokázat. Jako důkazní prostředek bude pravděpodobně dostačovat fakt, že z dané konkrétní IP adresy k porušování autorských práv docházelo a následný výpis z telekomunikačního provozu poskytnutý poskytovatelem služby internetového připojení.

Poslední z podobných zákonů byl přijat na Taiwanu. Nový dodatek k autorskému zákonu staví používání P2P technologií usnadňujících šíření autorsky chráněných děl na úroveň trestného činu. Zároveň jsou poskytovatelé internetu zbaveni odpovědnosti za to, co dělají uživatelé s jejich službami, ale na oplátku musejí zavést již výše zmiňované „třikrát a dost“ s jednou velice zvláštní úpravou: nemusejí předávat organizacím zastupujícím zábavní průmysl informace vedoucí k identifikace hříšníků. Pokud však takový hříšník bude protestovat (zejména bude-li tvrdit, že je nevinen), pak poskytovatel služby internetového připojení takové údaje poskytne.

7. Odpovědnost stran při zpřístupňování děl veřejnosti

Účelem této kapitoly je pokusit se vymezit rozsah a možnosti odpovědnosti, která by měla postihovat různé strany řetězce. Zejména se bude jednat o poskytovatele internetového připojení, provozovatele výměnné sítě a v neposlední řadě taktéž koncového uživatele.

7.1 Odpovědnost poskytovatele internetového připojení

Základním článkem řetězce bude tzv. „internet service provider“, tedy poskytovatel internetového připojení. Toho lze pravděpodobně k odpovědnosti hnát jen těžko. AutZ dokonce ve svém §18 odst. 3 výslovně určuje, že sdělování díla veřejnosti není pouhé provozování zařízení umožňujícího nebo zajišťujícího takové sdělování. Již z vymezení obsahu autorského práva k sdělování díla veřejnosti vyplývá, že výkonem tohoto práva je samotný akt zpřístupnění díla, nikoli jeho technické zajištění. Osoba provozující technickou transmisi sdělovaného díla se tedy sama o sobě nedopouští sdělování díla veřejnosti.

Tyto osoby, zejména tedy provozovatelé komunikačních sítí a zařízeních využívaných pro provoz těchto sítí, nenesou odpovědnost za obsahovou stránku přenášených informací, ale pouze za technickou kvalitu přenosu. Z právního hlediska nelze po poskytovateli internetového připojení, či provozovateli komunikační sítě požadovat, aby nesl jakoukoli odpovědnost za obsah přenášených dat. V takovém případě bysme po něm s postupem času mohli požadovat kontrolu celého obsahu se zaměřením na páchání veškeré trestné činnosti.

Na takovouto kontrolu by bylo třeba extrémního množství zdrojů, at již finančních, tak lidských. Zároveň by při takové kontrole mohlo docházet ke střetu s některými dalšími zákony. Jako příklad uveďme možné narušení osobních údajů dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění, ale v krajním případě by mohla být narušena i ochrana osobnosti, zejména soukromí dle ObčZ.

Na druhou stranu lze po těchto osobách spravedlivě vyžadovat určitý druh spolupráce, zejména na základě požadavků ze strany policie či justice. Tento druh spolupráce by měl spočívat například v monitorování přenosu dat na základě

konkrétního požadavku, či poskytnutí údajů o konkrétních osobách podílejících se na monitorovaných či kontrolovaných přenosech. Lze si taktéž představit požadavek, kdy bude osoba poskytující některou z výše uvedených služeb nucena podstoupit různé druhy omezení. Takový případ by mohl nastat, když by poskytovatel připojení k internetu byl nucen zablokovat přístup všech jeho zákazníků na určitou část internetu. Například zablokováním určitých IP adres, nebo dokonce celého rozsahu těchto IP adres, o kterých je všeobecně známo, či prokázáno, že je z nich šířen nelegální obsah – tedy autorskoprávně chráněná díla. Pokud byl poskytovatel služby internetového připojení na porušování autorských práv upozorněn, případně byl požádán o spolupráci a neprovedl žádná opatření, mohl by být odpovědný dle §415 ObčZ, který spočívá v uložení všeobecné povinnosti prevence – tedy předcházení hrozícím škodám. V případě že by poskytovatel neučinil vše potřebné v rámci svých možností, aby zabránil vzniku škod, bylo by reálné prokázat jeho zavinění a vyvodit odpovědnost.

Odpovědnost tvůrců protokolu a aplikací pro P2P je taktéž těžko dovoditelná. Každá z P2P sítí funguje na bázi některého konkrétního protokolu. Autorem protokolu může být osoba zcela odlišná od autora aplikace, která využití daného protokolu umožňuje. Otázkou tedy je, jak můžeme požadovat odpovědnost od tvůrců těchto protokolů či aplikací? Ani v jednom případě si nelze takovou odpovědnost představit. Dle mého názoru v tomto případě nelze dovodit ani odpovědnost za spolupachatelství. Současná právní teorie v případě spolupachatelství k trestnému činu vyžaduje již předchozí úmysl takový trestný čin spáchat. V rovině dokazování by tedy soud byl postaven do situace, kdy bude muset tvůrci P2P aplikace či protokolu prokázat úmysl ve vztahu k porušování autorských práv. Taková situace je sice teoreticky možná, ale prakticky ne zcela reálná. Takovému autorovi by se musel prokázat úmysl, že daný protokol či aplikaci vytvořil za účelem sdílení a přenosu nelegálního obsahu. Taková odpovědnost by musela být objektivní – tedy za výsledek a to by bylo velice přísné. Jen těžko lze najít takovou síť, která by k šíření nelegálního obsahu nesloužila a tak by již předem byl každý autor odpovědným viníkem. Stejně jako nelze přičítat odpovědnost výrobci zbraní za zabití konkrétního člověka, nelze předem přičítat autorovi protokolu či aplikace vinu za porušení daného konkrétního autorského práva.

7.2 Odpovědnost provozovatelů P2P sítí

Provozovatelé P2P sítí většinou nevystupují jako ti, kteří dané dílo sdělují, ale pouze sdělování díla usnadňují. V případě torrentů půjde o lokalizaci příslušného díla v počítačové síti. Právě proto tyto osoby nenesou odpovědnost dle AutZ za sdělování díla veřejnosti. Náš AutZ nezná delikt za poskytování pomoci či jiné asistence osobám, které autorská práva porušují.

Činnost těchto osob však za určitých podmínek může mít povahu tzv. „prostředníků“, tedy poskytovatelů služeb, které využívají třetí osoby k porušování nebo ohrožování autorských práv. Novela AutZ z roku 2006 zavedla vůči těmto osobám možnost uplatnění zvláštního negatorního nároku směřujícího k zákazu poskytování jejich služeb[14]. Autorský zákon tímto ustanovením specifikuje autorskoprávní odpovědnost osob za jednání odlišné od samotného porušování či ohrožování autorského práva.Vznik odpovědnosti za poskytování předmětných služeb je závislý na vzniku autorskoprávní odpovědnosti třetích osob, tedy porušitelů či ohrozitelů autorského práva. Jedná se tedy o závislou skutkovou podstatu autorského práva, ze které plyne i povinnost důkazu porušení či ohrožení autorského práva jako podmínky pro přiznání nároku vůči poskytovateli služby – provozovateli P2P sítě. Vždy však bude nutné zkoumat příčinnou souvislost mezi poskytováním služby a mezi porušením či ohrožením autorského práva ze strany třetích osob.

Tyto případy bude vždy nutné posuzovat podle konkrétních okolností, zejména zda se bude jednat o P2P systém založený na centralizovaném systému, tedy případ kdy bude existovat centrální server, tedy počítač který bude provádět určitou specifickou činnost (například indexaci záznamů o dílech, vyhledávač konkrétních děl), nebo zda se bude jednat o systém zcela necentralizovaný, kde každý koncový počítač bude fungovat jako server a tudíž jako vyhledávač. Další faktor může být například fakt, zda dochází ze strany provozovatele služby k přímému či nepřímému majetkovému prospěchu, či zda dochází k podněcování třetích osob k zásahu do autorského práva. Pokud by se provozovatele konkrétní sítě podařilo identifikovat, musel by se v každém konkrétním případě posuzovat jeho vliv na porušení práv chráněných AutZ.

[14] §40 odst 1 písm. f) AutZ

V úvahu by tak navíc přicházela obecná odpovědnost za škodu dle §420 a násl. ObčZ. Otázkou by nadále zůstavalo, jaká míra zavinění ve vztahu k porušování autorsky chráněných práv by se provozovateli podařila prokázat. Snadnější cestou se zdá být §415 ObčZ, který spočívá v uložení všeobecné povinnosti prevence – tedy předcházení hrozícím škodám. V takovém případě by se prokazovalo, že provozovatel dané sítě neučinil vše potřebné v rámci svých možností, aby zabránil vzniku škod. Této možnosti mohou využít například vlastníci či zástupci vlastníků autorskoprávně chráněných děl v podobě upozornění provozovatele dané výměnné sítě na nelegální obsah šířený v rámci dané sítě. Pokud by provozovatel tomuto upozornění nevěnoval pozornost, byla by mnohem snazší prokázat jeho zavinění a tím pádem i odpovědnost.

Ze současné praxe můžeme vycházet z poměrně čerstvého rozhodnutí nizozemského soudu týkajícího se jednoho z velice známých a oblíbených torrent vyhledávačů Mininova. Ten byl v nizozemí pronásledován tamní protipirátskou organizací BREIN za porušování autorských práv. Mininova sice dle soudce není přímo zodpovědná za porušování autorských práv, ale i tak jí bylo nařízeno odstranění všech torrentů odkazujících na autorsky chráněná díla. Lhůta k odstranění činí tři měsíce a pokud tak neučiní, riskuje pokutu v celkové výši až 5.000.000 €. Tato částka je maximální možná. Za každý torrent obsahující odkaz na chráněné dílo bude případně vymáháno 1.000 € a to až do celkové maximální výše. Soudce tak potvrdil tvrzení BREINu, že Mininova neučinila dostatečná opatření směřující k ochraně držitelů práv k dílům. Takové pojetí by se dalo v rámci našeho právního řádu přirovnat k obecné prevenční povinnosti dle §415 ObčZ, jak již bylo zmíněno výše. Lidé spojení s Mininovou navrhovali filtraci na bázi systému klíčových slov a digitálních otisků souborů, což by umožňovalo majitelům práv kontrolu, to však soudce shledal nedostatečným. Soudce také nesouhlasil s tvrzením Mininovy, že není možné kontrolovat všechny torrenty, které jsou na stránky uploadovány (nahrávány). Naopak se domnívá, že Mininova své uživatele ke stahování chráněných děl motivuje. Též bylo naznačeno, že Mininova z chráněného obsahu profituje díky ziskům z reklamních bannerů. Zakladatelé samozřejmě zvažují odvolání (lhůta činí taktéž tři měsíce).

Boj proti P2P sítím probíhá i na území Velké Británie. Tamní vláda vydala dokument, ve kterém vyzývá k diskuzi všechny, kterých se problematika nelegálního sdílení v P2P sítích týká. Výzva je součástí nové vládní politiky, která má urychlit

proces řešení problému nelegálního sdílení na internetu, kdy by se v příštích několika letech chtěla dostat na 30 % současné aktivity. Mezi návrhy se nachází již známé požadavky na poskytovale služeb připojení k internetu, aby v případě opakovaného porušování autorských práv zakročili a snížili uživateli rychlost, nebo ho i dočasně odpojili, případně aby blokovali některé internetové IP adresy či služby. Vláda sice projevuje snahu, ale i zde existuje řada nedořešených otázek. Není třeba ještě zcela určeno, jaký postih bude uplatněn na majitele autorského práva v případě neopodstatněného „udání“, dále není jasné, jak tento majitel bude dokazovat, že k předmětnému dílu opravdu tato práva vlastní. Doufejme, že se do debaty zapojí i poskytovatelé služeb připojení k internetu a majitelé autorských práv.

7.3 Odpovědnost koncových uživatelů

Koncové uživatele lze rozdělit na uživatele P2P sítí a konzumenty warez scény. V případě koncového uživatele warez scény by bylo velice těžké prokazovat odpovědnost. Takovýto uživatel má pouze přístup na daný FTP server a z něj si stahuje data na svůj soukromý počítač, která následně využívá (hudební a filmové nahrávky). Tyto data již ovšem není nucen šířit a tudíž ani nešíří dál. To je základní rozdíl oproti P2P sítím a jejich protokolům, které jsou velmi často založeny na vynuceném sdílení dat již při samotném stahování autorsky chráněného obsahu.

Takový uživatel se tedy již při příjmu dat dopouští porušování autorských práv tím, že zároveň tyto stažená data poskytuje všem ostatním uživatelům dané P2P sítě k dispozici. Na tomto principu funguje například v současnosti velmi rozšířený BitTorrent. Na podobném principu fungují například i DirectConnect huby, které sice okamžitě neposkytují ke stažení uživatelem právě stahovaná data, ale již předem musí být vymezen určitý rozsah dat, který uživatel ke stažení nabízí. Nasdílení určitého objemu dat bývá základní podmínkou pro vstup na DirectConnect huby. To ovšem ještě automaticky nezakládá odpovědnost za porušování autorských práv. Lze si představit konkrétního uživatele, který pro ostatní uživatele nasdílel (tedy zpřístupnil, umožnil stažení) nechráněný obsah, například své fotky z dovolené, či jiná volně přístupná data. Tento obsah sice není příliš atraktivní, ale ke splnění podmínky pro daný DirectConnect hub často dostačuje.

Odpovědnost daného koncového uživatele se tedy bude velmi lišit a bude záležet na konkrétním posouzení daných okolností, tedy zejména zda vůbec a jaký druh obsahu poskytl ostatním uživatelům dané výměnné sítě. Uživatel, který sdílí data a tedy sděluje dílo veřejnosti bez souhlasu jeho autora či bez platné licence, vznikne autorskoprávní odpovědnost. Taktéž v tomto případě je možné využít již zmíněný §40 AutZ, který například umožňuje domáhat se autorství, zákazu ohrožení autorských práv, sdělení údajů o původu a původcích nelegálních kopií díla a odstranění následků zásahu do autorského práva či poskytnutí přiměřeného zadostiučinění za způsobenou nemajetkovou újmu. V případě přiměřeného zadostiučinění se předpokládá v prvé řadě omluva, jinak peněžitá náhrada.

Ani v případě koncového uživatele však není vyloučena možnost poškozeného domáhat se náhrady škody a vydání bezdůvodného obohacení v na základě ObčZ. I v tomto případě by připadala v úvahu obecná občanskoprávní odpovědnost dle §420 a násl. ObčZ. V tomto případě by však odpadla potíž s určením míry zavinění na porušování autorských práv. Toto porušení by vyplývalo již ze samotného aktu zpřístupnění díla veřejnosti bez souhlasu autora či bez příslušné licence. V rámci zavinění postačuje nevědomá nedbalost, která je předpokládána zákonem. §415 ObčZ lze aplikovat i na koncového uživatele. Vzhledem k velmi obecné prevenční povinnosti a ke snazšímu dokazování odpovědnosti dle §420 ObčZ lze však předpokládat, že v praxi toto použití nebude časté.

Užití ustanovení o bezdůvodném obohacení dle §451 a násl. ObčZ se jeví přinejmenším jako problematické. V případě uživatele-podnikatele si lze představit situaci, kdy si takový uživatel nelegálně opatří program potřebný k jeho podnikání a s jeho pomocí následně dosahuje zisku. Takový zisk je poměrně snadno prokazatelný a vlastník autorských práv by mohl požadovat vydání bezdůvodného obohacení. V našem případě ovšem posuzujeme odpovědnost uživatelů P2P sítí, kteří jsou odpovědní za sdílení dat a ne za jejich stahování. Vlastní stažení ještě nezakládá odpovědnost, nýbrž až jeho další užití, jak již bylo uvedeno výše (viz. kapitola 5.1).

7.4 Aktuální vývoj vybraných případů ze současnosti

Pro lepší obrázek o současné praxi u nás i v zahraničí jsem se rozhodl rozebrat dvě právě probíhající trestní řízení. V prvém případě se jedná o případ warezového FTP

serveru v České republice nazvaný „Blind Alley“ a ve druhém o světově známý a proslavený vyhledávač torrentů - server the „Pirate Bay“ (Pirátská Zátoka).

7.4.1 Blind Alley

Tzv. „Slepá Ulička“, případ který v průběhu celého roku 2009 hýbe všemi médii a již několikrát byl zmiňován v denních zpravodajstvích české veřejnoprávní televize. Cílem mé snahy bude tento případ popsat a rozebrat příčiny a důsledky doposud neúspěšného trestního řízení ve vztahu k legislativě České republiky.

V případě Blind Alley se jedná o zabavení dvou počítačů - FTP serverů v prostorách Akademie Věd. Tyto servery sloužily jako tzv. TOP servery sloužící pro účely warez scény, jak jsme si ji již popsali výše. Jednalo se o úložiště nelegálního obsahu na té nejvyšší úrovni, které obsahovalo ohromné množství autorsky chráněných děl. Nebezpečnost těchto serverů lze nalézt zejména ve vztahu k jednotce času. Jen těžko si lze představit, že se autorská díla objevila někde jinde dříve, než právě na těchto serverech a právě z těchto serverů se šířila dál na různé podřadnější počítače, servery a P2P sítě, ale v konečném důsledku taktéž mezi běžné koncové uživatele.

Policie zabavila dva servery s daty, provedla domovní prohlídky potenciálních pachatelů a poté několik měsíců získaná data analyzovala. Taktéž byli zadrženi a vyslechnuti tři podezřelí. Na tyto osoby byla posléze podány státním zástupcem obžaloba pro porušování autorského práva, práv souvisejících s právem autorským a práv k databázi dle §152 odst. 1 zákona č. 140/1961 Sb., trestního zákona (dále jen TrZ), ve spolupachatelství dle §9 odst. 2 TrZ, s tím, že soudem bylo dáno podle §190 odst. 2 TrZ upozornění na možnost právní kvalifikace podle §152 odst. 1, 2 písm. b) TrZ. Nejprve byl soudem vydán trestní příkaz, kterým byl všem obžalovaným uložen trest odnětí svobody v délce 12 měsíců s podmíněným odkladem trestu na zkušební dobu 24 měsíců. Proti tomuto trestnímu příkazu byl však podán všemi obžalovanými odpor a soudce tedy ve věci nařídil hlavní líčení. V hlavním líčení soudce nakonec podle §226 písm. c) zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) zprostil všechny tři obžalované obžaloby.

V současné době podal státní zástupce odvolání a případ tak zřejmě bude pokračovat u Městského soudu v Praze. Soudce bude čelit velice složitému problému, tedy jak prokázat obžalovaným, že právě oni se dopouštěli porušování autorských práv?

Důkladným rozborem prvoinstančního rozhodnutí dojdeme k zajímavým a pro praxi velmi důležitým poznatkům. Policie po zajištění výše uvedených serverů přibrala k jejich posouzení znalce z oboru IT (tedy informačních technologií). Důkaz znaleckým posudkem bude v řízeních tohoto typu základním, často možná i jediným přímým důkazem umožňujícím důkladný rozbor a analýzu. Ať si to již chceme či nechceme přiznat, v soudním řízení se nelze odkazovat jen na nepřímé důkazy získané od třetích osob, případně na různé druhy udání či tvrzení. Je tedy nutnou podmínkou znalce přibrat a nechat ho zpracovat komplexní znalecký posudek. Takový posudek by v případě zabavení výpočetní techniky (počítačů – serverů) měl obsahovat celkový popis, obsahující zejména hardwarovou strukturu těchto počítačů, jejich softwarové vybavení a samozřejmě také případný seznam veškerých autorskoprávně chráněných děl, která na takovém počítači budou uložena.

Tím však práce znalce zdaleka není u konce. Další faktor, který bude znalec nucen posuzovat, bude spojení podezřelých, obviněných či obžalovaných osob k předmětným počítačům. V konkrétním případě bude nutné dokazovat přímou či nepřímou správu, manipulaci a konfiguraci těchto počítačů ze strany konkrétních osob.

Je tedy nanejvýš pravděpodobné, že identifikaci poškozených děl, rozsah tohoto poškození a spojitost s konkrétní fyzickou osobou nebude možné prokázat jinak, než důkladnou analýzou takových počítačů. Nad touto situací je ovšem nutno se zamyslet i z druhé strany. Počítačoví piráti jsou v naprosté většině případů lidé z IT, kteří mají znalosti na velmi vysoké úrovni a podle toho se také chovají. Pokud už takový počítač provozují, budou se chtít v co nejvyšší možné míře zabezpečit a vyhnout se tak potenciálním problémům s policií a orgány justice.

Pro takovou úroveň zabezpečení v současnosti postačují dva kroky. Prvním krokem je vypnutí veškerého druhu tzv. logování. Logování je vlastně jakási historie, která se v počítači ukládá a při podrobném zkoumání v ní znalec může například nalézt údaje o tom, kdo, kdy a jakým způsobem se k danému počítači připojoval, případně kdo a kdy na tento počítač nahrával autorsky chráněná díla. Z logů lze vyčíst mnoho informací, které by ve svém důsledku mohly vést k odhalení pachatele a jeho následnému odsouzení. Pokud je však takové logování vypnuté, žádné informace tohoto druhu v počítači znalec nenalezne.

Druhou a dle mého názoru stěžejní a naším právem nereflektovanou možností je možnost zašifrování dat na počítači. V dnešní době existuje mnoho volně dostupných počítačových programů sloužících k zašifrování celého obsahu pevných disků, i včetně disku, na kterém je uložen operační systém. Mezi nejznámější patří program TrueCrypt[15], který využívá více druhů šifrování a záleží tedy pouze na uživateli, jaký druh šifry s jakou sílou si zvolí. Patrně i ta nejslabší šifra je pro tento druh zabezpečení dostačující, jelikož v rámci současného stavu výpočetní techniky neexistuje možnost, jak byť tuto nejslabší šifru prolomit. Tím se dostáváme k otázce, jak je možné se k takto zašifrovaným datům a obsahu dostat?

První variantou je znát uživatelské heslo s jehož pomocí se k datům snadno dostane leckterý laik. Horší situace nastává, pokud heslo neznáme. V takovém případě přichází v úvahu pouze varianta použití hrubé síly (tzv. „bruteforce"), kdy se heslo snažíme získat prolomením šifry za použití dostupného výpočetního výkonu. Jednoduše řečeno se jedná o náhodné zkoušení různých kombinací, které by v případě použití dostatečného výpočetního výkonu vedlo k prolomení šifry, hesla a následnému již snadnému přístupu k datům. Tato metoda je ale víceméně pouze teoretická, jelikož dnešní počítače takovýmto výpočetním výkonem nedisponují. Lze si představit za několik desítek let, že dnešní šifry budou prolomitelné během několika málo minut či hodin, ale v té době již zcela jistě budou existovat šifry lepší, složitější a pro budoucí techniku opět neprolomitelné. A pokud se někdo bude zabývat prolamováním šifer starších, většinou již půjde o pouhý koníček, jelikož trestnost takto spáchaných trestných činů bude pravděpodobně již promlčena.

Jaké je tedy v takovém případě postavení znalce? Pokud znalec dostane za úkol vypracovat posudek na počítač, jehož datové úložiště je zašifrováno, je téměř bezmocný. Jak bylo zmíněno výše, není v jeho možnostech šifru prolomit. Varianta s heslem je taktéž pouze teoretická. Jen těžko si lze představit obžalovaného, který bude dobrovolně vypovídat proti sobě a heslo dobrovolně sdělí. Takové osobě náleží právo nevypovídat a neexistuje tedy možnost zákonného donucení, kdy by osoba byla povinna heslo sdělit.

[15] www.truecrypt.org

Bez možnosti přístupu k datům nebude znalec schopen činit kategorické závěry o tom, zda na daném počítači autorsky chráněná díla skutečně jsou, kdo a kdy k tomuto počítači přistupoval, kdo se dopustil porušování autorského práva nahráváním autorsky chráněných děl a tím automaticky porušování AutZ sdělováním díla veřejnosti bez souhlasu autora atd.

7.4.2 The Pirate Bay

Tento případ můžeme s jistotou označit za největší svého druhu v celé historii porušování autorských práv. Jedná se o torrentový server s jehož pomocí bylo každodenně přeneseno stovky terabajtů dat mezi uživateli po celém světě. I díky snaze obžalovaných se případ stal vyhledávaným zdrojem informací pro informační média i televizní stanice z mnoha zemí. Považuji za nutnost ho v mé práci podrobně rozebrat a nastínit jeho právní základy i přesto, že je celý založen na švédském právu a tak není zcela možné ho porovnávat s legislativou platnou na území České republiky.

Účelem tedy bude popsat od počátku vývoj a zdůraznit důvody na jejichž základě byli provozovatelé uznáni vinnými.

Historie tahu na piráty z The Pirate Bay (dále jen „TPB“) sahá až do roku 2007, kdy švédský prokurátor Håkan Roswall oznámil, že hodlá vyrazit proti pěti lidem z TPB a podat žalobu nejpozději do 31. ledna 2008. To však „kluky z pirátské zátoky“, jak bychom mohli Fredrika Neije, Gottfrida Svartholma, Petera Sundeho a Carla Lundströma nazvat, příliš nerozhodilo. Jak totiž sami tvrdili, na jejich serverech se žádný materiál chráněný autorským právem nenacházel. To, že se na serverech skutečně nenacházel žádný chráněný materiál, věděla i sama policie, která v roce 2006 udělala u provozovatelů hostingu TPB právě pod vedením Håkana Roswalla razii. Razie byla posléze označena za krajně neúspěšnou.

Roswall se však nevzdal, v lednu 2008 oznámil agentuře Revers, že žalobu chce skutečně podat a že se bude týkat aktivního napomáhání v páchání trestné činnosti porušování autorských práv. Prohlásil, že TPB není jen vyhledávač, ale aktivní součást činnosti, která je určena a také vede k poskytování materiálu chráněného autorským právem. Dle něj šlo o klasický případ spolupachatelství, kdy TPB operuje jako zprostředkovatel mezi lidmi, kteří danou kriminalitu provádějí.

TPB však neležela v žaludku jen jemu, již na začátku února 2008 v Dánsku tamní soud nařídil poskytovateli internetového připojení Tele2, aby zablokoval svým zákazníkům přístup na web TPB. Nešlo o první vyhovění soudu ze strany dánského Tele2 ohledně přístupu na stránky, o nichž zainteresované skupiny tvrdí, že jsou stvořeny téměř výhradně za účelem porušování autorských práv.

V květnu 2008 přichází organizace MPAA a požaduje po švédské TPB 15,4 miliónu dolarů jako kompenzaci škod na autorských právech ke čtyřem filmům a třinácti episodám jednoho seriálu.

V červnu 2008 nabrala kauza dalších zajímavých obrátek. Ukázalo se totiž, že policejní IT specialista Jim Keser, který měl na starosti vyšetřování obvinění vznesených proti TPB, byl zaměstnán společností Warner Bros a to i v době, kdy vyšetřování TPB ještě nebylo ukončeno. Tato skutečnost vrhla na případ podivné světlo hraničící s podezřením na podplácení policejních činitelů zainteresovanými osobami. Warner Bros museli s pravdou ven a státní zástupce to po rozhovoru s jejich právníkem potvrdil, že Keyzera zaměstnávali v době, kdy byl zaměstnancem policie, ale současně pracoval na kauze, ve které je Warner Bros žalující stranou.

V sprnu 2008 okresní soud ve Stockholmu, který má na svých bedrech celou slavnou kauzu vedenou proti tomuto serveru, resp. několika jeho hlavním představitelům, oznámil, že odkládá zahájení soudního přelíčení. Původně mělo začít právě koncem léta, nyní se vše odkládá nejdříve na konec roku, možná až na rok příští. V odůvodnění stálo, že zjišťování škod a také doručování obsílek zkrátka trvalo a trvá déle, než se předpokládalo. Každopádně po dvou letech vyšetřování bylo nakonec rozhodnuto o obžalování čtyř lidí kolem serveru z porušování autorských práv, konkrétně jak samotných „pirátů“ (Fredrik Neij, Gottfrid Svartholm a Peter Sunde), tak obchodníka Carla Lundströma. Žalobce požaduje 188 000 USD pokutu pro každého z nich a dále konfiskaci jejich počítačů.

V Itálii se mezitím tamní představitelé dohodli na zablokování TPB v rámci celé země. Zablokování serveru mělo však naprosto opačný účinek. Soud v Bergamu označil blokování za protiprávní a nařídil jeho zrušení. Námitky, že TPB žádná autorská práva neporušuje, protože skrze jejich servery neprotéká žádný autorsky chráněný obsah,

zřejmě padly na úrodnou půdu. Reklama, kterou tím však TPB poskytli, zvedla enormně návštěvnost tohoto webu.

Doby, kdy TPB byla malým místním serverem jsou pryč. Právě útoky hollywoodské mašinérie a policejní razie vedená zmiňovaným policejním důstojníkem udělaly ze serveru velice rychle hvězdu P2P světa a mnozí nyní odhadují, že zhruba 50% veškerých přenesených dat na internetu spojuje právě tracker TPB.

Soud začal 16.2.2009, byla to nejžhavější kauza v novodobých dějinách autorských práv. obžaloba hovořila 3 dny, nicméně žalující strany nebyly prozatím schopny předložit přesvědčivé důkazy. Nebyli schopni prokázat, že .torrent soubory, které mají být předmětem porušování autorských práv, skutečně prošly trackerem TPB. Spousta doložených screenshotů z různých programů není dostatečně průkazná, aby spojila konkrétní porušení práv právě s TPB. Fredrik posléze oznámil, že obžaloba nepochopila způsob fungování technologie a že předložené důkazy nemusejí znamenat, že byl v souvislosti s porušováním práv použit právě tracker TPB.

Prozatímní výsledek tedy byl, že žalovaná strana už druhý den stáhla polovinu obvinění. Z obžaloby se vytratila část pojednávající o „napomáhání porušování autorských práv“ a v tuto chvíli zbylo jen „napomáhání zpřístupňování děl“.

Avšak 17.4.2009 došlo k průlomovému rozhodnutí v jedné z nejsledovanějších kauz týkajících se používání P2P sítí a speciálně torrentů. Provozovatelé nejznámějšího torrentového trackeru / vyhledávače TPB byli uznáni vinnými z napomáhání zpřístupňování autorsky chráněných děl.

Všichni čtyři obvinění dostali každý jeden rok vězení. Soud uznal, že obžalovaní fungovali jako tým, že si byli vědomi, že prostřednictvím TPB si uživatelé vyměňují autorsky chráněný obsah a fungováním TPB jim to usnadňovali. Zamítl však vyčíslené horentní sumy přesahující miliardu dolarů, sám stanovil škodu ve výši 30 miliónů švédských korun (v přepočtu 3,62 miliónu dolarů / skoro 74 miliónů Kč / 2,7 miliónu €). Na tuto škodu by se měli všichni čtyři obvinění složit.

V květnu roku 2009 podala čtveřice odvolání, rozsudek nenabyl právní moci a TPB je čím dál tím více populární a hlavně stále funkční. Tato situace však nenechala hudební průmysl klidným a společnosti Universal, EMI, Sony a Warner rozhodly „vzít situaci do právních rukou Petera Danowskyho z IFPI“. Ten předložil okresnímu soudu

žádost o okamžité zajištění zastavení TPB coby „služby na porušování práv“. Zároveň chce nařídit poskytovateli připojení serverů TPB „Black Internet“, aby jim přestal poskytovat služby.

Odvolání však přerušily pochybnosti o zaujatosti soudce Tomase Norströma. Soudce byl totiž členem hned několika hned několika skupin hájících autorská práva. Jednalo se o SFU (Swedish Association of Copyright), SE (The Internet Infrastructure Foundation), SFIR (Swedish Association for the Protection of Intellectual Property).

Švédský odvolací soud však zamítl žádost obhájců chlapců z Pirátské zátoky a oznámil, že nové líčení se zahajovat nebude, soudce Tomas Norström zaujatý není. Sice mu vyčinil, že své aktivity v organizacích, kde také vystupují zástupci žalující strany, měl oznámit ještě před zahájením soudního řízení, mohlo se to vyřešit hned v samém úvodu, nicméně to prý neovlivní jeho rozhodování. Členství v těchto asociacích ukazuje na znalost problémů, které jsou do jisté míry v zájmu majitelů autorských práv. Je prý třeba brát v potaz, že práva majitelů autorských práv jsou zakotvena ve švédských zákonech. To, že soudce s těmito základními principy tohoto zákona souhlasí, nemohlo být samo o sobě bráno jako zaujatost, konstatoval odvolací soud.

Co lze říci závěrem? Viníci byly shledáni odpovědnými za napomáhání zpřístupňování autorsky chráněných děl. Toto rozhodnutí lze považovat za průlomové přinejmenším ve vztahu k provozovatelům torrentových serverů, jelikož většina z nich funguje na stejném principu a pokud byli uznáni vinnými jedni, je možné takto odsoudit i další.

8. Soukromoprávní odpovědnost obecně

V současnosti se autor může domáhat náhrady vzniklé škody[16], tj. škody skutečné a ušlého zisku, resp. náhrady ušlého zisku ve výši obvyklé autorské odměny namísto skutečně ušlého zisku. Dále má autor možnost domáhat se vydání bezdůvodného obohacení[17]. Pro případ bezdůvodného obohacení obsahuje autorský zákon v §40 odst. 4 věta druhá speciální ustanovení, které určuje výši bezdůvodného obohacení vzniklého na straně toho, kdo neoprávněně nakládal s dílem, aniž by k tomu získal potřebnou licenci, jako dvojnásobek odměny, která by byla na získání takové licence obvyklá v době neoprávněného nakládání s dílem.

8.1 Ochrana dle autorského zákona

Autorský zákon ve svém §40 odst.1 demonstrativně vyjmenovává možnosti, jakými se autor může bránit proti osobě, která neoprávněně zasáhla do jeho autorského práva nebo je ohrozila. Možnosti autora jsou následující:

a) určení autorství pomocí žaloby určovací

b) nárok zápůrčí či zdržovací (negatorní) – ten spočívá v zákazu jednání, které v dané době ohrožuje autorské právo, nebo do něj zasahuje, tj. možnost domoci se nečinnosti neoprávněně jednající osoby (rušitele). Z povahy věci vyplývá, že takový nárok lze uplatnit pouze tehdy, kdy škodlivý stav stále trvá.

c) sdělení informací, spočívající v povinnosti poskytnout zákonem stanovené informace

d) nárok odstraňovací (restituční), jehož účelem je odstranit na náklady ohrozitele či porušitele důsledky, které neoprávněný zásah do práva autorského (či jeho ohrožení) přivodil, a tak obnovit (restituovat) právní stav před tímto neoprávněným zásahem (ohrožením)

[16] §420 a násl. zákona 40/1964 Sb., občanského zákoníku

[17] §451 a násl. tamtéž

e) nárok na přiměřené zadostiučinění (satisfakční), zejména ve formě omluvy či zadostiučinění v penězích, které náleží pouze při vzniku nebo reálné hrozbě nemajetkové újmy

f) zvláštní zápůrčí nárok vůči poskytování služby, kterou využívají třetí osoby k porušování nebo ohrožování práva autora (tento nárok lze využít proti poskytovatelům služeb, například tedy provozovatelům P2P sítí, o nichž bylo pojednáno výše).

8.2 Ochrana dle ObčZ

Autorský zákon stanoví, že vznikem autorskoprávní odpovědnosti není dotčen možný vznik odpovědnosti za škodu a bezdůvodné obohacení související s porušením či ohrožením autorského práva[18]. Jedná se o odkazovací normu na ObčZ. Odpovědnost za škodu se bude uplatňovat na základě §420 a násl. ObčZ. Tato odpovědnost je založena na subjektivním principu, tzn. ke vzniku odpovědnosti bude potřeba zavinění škůdce, ať již nedbalostní, nebo úmyslné.

Jestliže někdo užije cizí dílo bez některého z právních důvodů stanovených v autorském zákoně, či bez platné licence, naplňuje tím skutkovou podstatu soukromoprávního deliktu bezdůvodného obohacení dle §451 a násl. ObčZ. Jednalo by se o plnění bez právního důvodu. Povinnost vydat bezdůvodné obohacení vzniká bez ohledu na zavinění bezdůvodně obohaceného. Podmínky pro vznik odpovědnosti za bezdůvodné obohacení nevyplývají z AutZ, nýbrž obecně z ustanovení ObčZ. Bezdůvodné obohacení může v konkrétním případě spočívat například v přímem zisku, který byl dosažen porušením autorského práva, či ušetření a zvětšení majetku bezdůvodně obohaceného. AutZ však odlišně od obecné právní úpravy stanoví výši odměny za nakládání s autorským dílem bez potřebného právního důvodu, a to jako dvojnásobek obvyklé smluvní licenční odměny. Tímto způsobem pojatá výše bezdůvodného obohacení se spíše již blíží sankčnímu nároku ve formě soukromé pokuty. Obecná úprava vydání bezdůvodného obohacení plní spíše funkci restituční.

[18] §40 odst. 4 AutZ

Dvojnásobná výše bezdůvodného obohacení v sobě tedy zahrnuje jak restituci, tak i jakousi formu pokuty náležející autorovi za neoprávněné užití díla.

9. Veřejnoprávní odpovědnost obecně

V souvislosti s rozvojem internetu a tedy velmi snadné dostupnosti autorsky chráněných děl široké veřejnosti je třeba posílit právní prostředky ochrany těchto děl. Vedle běžně dostupné soukromoprávní ochrany, kterou jsme popsali v předchozí kapitole, je třeba zmínit i odpovědnost trestní a postih pachatelů dle autorského zákona.

9.1 Trestněprávní ochrana

V současně platném trestním zákoníku je porušování autorského práva upraveno ve zvláštní části, hlavě druhé o trestných činech hospodářských, oddílu čtvrtém o trestných činech proti předpisům o nekalé soutěži, ochranných známkách, chráněných vzorech a vynálezech a proti autorskému právu, proti právům souvisejícím s právem autorským a proti právům k databázi. Konkrétně se jedná o §152 TrZ pojmenovaný „Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi.“ U tohoto trestného činu judikatura[19] upozorňuje na potřebu zjišťovat, zda je dán také potřebný (minimální) stupeň nebezpečnosti činu pro společnost. Vyžaduje se neoprávněný zásah do autorských práv, pachatelem může být kdokoli. Nutným znakem je úmysl, zákon tedy nepřipouští nedbalostní formu zavinění.[20] V prvním odstavci hrozí pachateli trest odnětí svobody až na 2 roky nebo peněžitý trest nebo propadnutí věci nebo jiné majetkové hodnoty. Kvalifikovaná skutková podstata uvedená v odst. 2 vyžaduje ke svému naplnění alternativně získání značného prospěchu (tedy nejméně 500.000,- Kč)[21] nebo spáchání činu ve značném rozsahu. V takovém případě pak hrozí nepodmíněný trest odnětí svobody na 6 měsíců až 5 let nebo peněžitý trest nebo propadnutí věci nebo jiné majetkové hodnoty. Pachatel však může být odpovědný i z jiných trestných činů, kromě výše uvedeného. Jedná se o trestný čin uvedený v §257a, nazvaný „Poškození a zneužití záznamu na nosiči informací“. V případě tohoto trestného činu se chrání zájem na ochraně dat uložených na nosiči informací proti neoprávněným změnám a jejich neoprávněnému použití. Předmětem útoku je tedy nosič informací, resp. jeho obsahové a technické vybavení. Zákonný termín „nosič informací“

[19] č. 33/2004 Sb. rozh. tr.

[20] č. 9/1997 Sb. rozh. tr.

[21] §89 odst. 11 zákona 140/1961 Sb., trestního zákona

použitý v §257a je třeba chápat jako nosič dat v informační technice. Může mít konkrétní podobu diskety, pevného disku, CD disku, čipu, operační paměti. Není to tedy např. pouhý záznam zvuku, záznam kinematografický ani videozáznam, i když jsou na magnetické pásce. Opět se zde vyžaduje úmysl pachatele orientovaný ke způsobení škody nebo jiné újmy jinému anebo získání neoprávněného prospěchu pro sebe nebo jiného. Konkrétní jednání pachatele pak záleží v získání přístupu k nosiči informací a zároveň ve splnění jednoho ze tří taxativně jmenovaných způsobů jednání, tedy:

a) v neoprávněném užití získaných informací

b) ve zničení, poškození, změně nebo učinění informací neupotřebitelnými

c) v zásahu do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení

V tomto trestném činu můžeme spatřovat jednu z činností, která se bezprostředně váže k páchaní softwarového pirátství – tedy cracking. Tvorba „cracků“ spočívá ve změně informace umístěné na nosiči informací, nejčastěji s úmyslem používat program bez platné licence. Není vůbec rozhodné, zda se informace nachází na pevném disku či CD/DVD nosiči.

Závěrem je nutné poznamenat, že ne každé jednání vykazující výše uvedené znaky můžeme kvalifikovat jako trestný čin. Zejména je nutné brát ohled na nebezpečnost činu pro společnost. Nelze shodně posuzovat jednání, kdy pachatel užívá doma jeden nelegálně získaný software, na rozdíl od společnosti, která používá nelegálně veškerý software na všech svých počítačích. Výše škody či majetkového prospěchu se posuzuje v případě počítačových programů jako výše odměny poskytované za získání skutečné licence k danému programu. Neužije se tedy vzorec pro výpočet bezdůvodného obohacení dle autorského zákona[22], tedy jako dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem. Pokud ovšem nebude stupeň nebezpečnosti pro společnost alespoň nepatrný, nelze jednání považovat za trestný čin, i když jinak znaky trestného činu

[22] §40 odst. 4 AutZ

vykazuje. V takovém případě je možné jednání kvalifikovat jako přestupek podle ustanovení §105a - §105c AutZ (např. při neúmyslném jednání).

9.2 Správněprávní ochrana dle autorského zákona

Základem je §105a - §105c AutZ. Tato úprava obsahuje přestupky fyzických osob, ale také správní delikty osob právnických a podnikajících fyzických osob. Skutkové podstaty spočívají v neoprávněném užití nehmotných předmětů chráněných autorským zákonem, neoprávněném obcházení účinných technických prostředků ochrany práv, nekalého pomůckářství, pozměňování elektronické informace o správě práv a nakládání s rozmnoženinou, na které byla elektronická informace pozměněna. Pokuty jsou stanoveny v rozmezí od 50.000,- Kč až do 150.000,- Kč.

10. Závěr a úvahy de lege ferenda

Neoprávněné užívání počítačových programů či jiných autorsky chráněných děl je zajisté jedním ze současných společenských problémů. Příčin můžeme identifikovat hned několik. Jako první se ukazuje velice snadná dostupnost technických prostředků pro běžného člověka. Jak bylo v práci zmíněno, je běžnou praxí mít v domácnosti počítač s připojením k internetu a zároveň CD/DVD vypalovací mechanikou. Takovéto vybavení lze již zakoupit za minimální náklady.

Druhým faktorem bude bezesporu snadná dostupnost prostředků pro šíření chráněných děl, zejména pomocí výměnných sítí v rámci sítě internet, ke kterému se bez potíží dostane i laický uživatel. Autorská práva jsou porušována v masivním měřítku, tresty a exemplární potrestání neexistují téměř žádná a tak má většina pachatelů pocit falešného bezpečí. Tento pocit částečně způsobuje anonymní prostředí internetu. Domnívám se, že kdyby českými médii proběhlo několik případů potrestání koncového uživatele za sdílení či stahování autorsky chráněných děl, dostala by se tato činnost do podvědomí veřejnosti jako nezákonná a působila by jako určitá forma prevence odrazující určitou část uživatelů od porušování těchto práv.

Ze strany veřejnosti a uživatelů často slýcháme mnohá zdůvodnění, proč zrovna ta jejich činnost je v pořádku. Ať už se lidé odvolávají na to, že to tak dělají všichni, či že jsou počítačové programy předražené, nebo dokonce že se jedná o sport či koníček a že to vlastně dělají pro zábavu, žádný z těchto argumentů nelze akceptovat a vždy se bude jednat o porušování autorských práv.

Společenské řešení snížení míry porušování autorských práv lze spatřovat v několika možnostech. První je snížení cen počítačových programů a jiných autorsky chráněných děl na takovou úroveň, kdy si je bude většina uživatelů ochotna koupit. Záměrně uvádím slovo „většina“, jelikož existují i uživatelé, kteří by za kvalitní program nebyli ochotni zaplatit ani 1,- Kč. Druhou možností je vyvinutí takové ochrany proti kopírování, kterou by nebylo možné prolomit. Tudíž by sloužila jen takovému uživateli, kdo si takto chráněné autorské dílo legálně zakoupí či na něj sjedná licenční smlouvu. Obě tyto možnosti jsou jen těžko realizovatelné a nebál bych se je zařadit do skupiny utopických přání, která pravděpodobně nikdy nebudou splněna. Ze společenského hlediska tedy nezbývá než na veřejnost působit různým druhem

protipirátských kampaní či vytvořit exemplární rozsudky a využít je jako prostředek prevence.

Z právního hlediska lze považovat současnou právní úpravu této problematiky za nedostatečnou. Ani v celosvětovém měřítku nenajdeme příliš mnoho průlomových rozhodnutí ze soudní praxe, natož pak v rámci České republiky. V případě členů warez scény se bude stále narážet na stejné problémy, mezi něž patří zejména zašifrovaná data a nemožnost přinutit pachatele sdělit heslo či vypovídat. Tyto instituty jsou zakotveny již v Ústavě České republiky a dále provedeny v mnoha dalších zákonech. Jen těžko si lze představit změnu legislativy v tomto směru a proto je nutné se zaměřit jinam.

Současná právní úprava je založena na subjektivním principu odpovědnosti a tedy i zavinění. V případě trestního postihu jsou soudy nuceny v rámci zásad trestního práva beze vší pochybnosti identifikovat pachatele i kompletní seznam jím porušených autorských děl. Dokazování bude často velice obtížné a ani do budoucna zřejmě nepovede k úspěšnému konci, pokud nedojde ke změně.

Taková změna by mohla spočívat v objektivní odpovědnosti alespoň u některých článků řetězce osob porušujících autorská práva. Pokud by byla například osoba provozující FTP server objektivně odpovědná za jeho obsah, či za data z něj šířená, bylo by dokazování mnohem snazší. Taktéž v rámci domácností by se mohla přenést odpovědnost na osobu, která uzavřela smlouvu s poskytovatelem služby připojení k internetu. Pokud by pak docházelo ze strany tohoto uživatele k porušování autorských práv, bylo by jej možné odpojit od internetu, či shledat odpovědným za takové porušení byť jen na bázi osoby uvedené ve smlouvě. Určitě bude mnoho odpůrců, kteří budou namítat, že jejich připojení k internetu mohl někdo zneužít, ale je přeci obecnou povinností každého uživatele si svůj počítač zabezpečit. To by pak každý mohl na ulici nechat ležet legálně drženou, nabitou a odjištěnou zbraň a doufat, že ji nikdo nepoužije. Proti objektivní odpovědnost bude mnoho odpůrců, ale vezměme si příklad třeba z Německa, kde majitel vozidla je plně odpovědný za spáchání přestupku jeho vozidlem, i když ho sám neřídil… Bylo by takto možné v případě počítače či internetu?

11. Seznam použité literatury

1. Telec, I., Tůma, P. *Autorský zákon: komentář*, Praha, C.H. Beck 2007, 1. vydání
2. Kříž, J. *Ochrana autorských práv v informační společnosti*, Praha, Linde 1999, 1. vydání
3. Čermák, J. *Internet a autorské právo*, Praha, Linde 2003, 2. vydání
4. Smejkal, V. a kolektiv Právo informačních a telekomunikačních systémů, Praha, C.H. Beck 2004, 2. Aktualizované a rozšířené vydání
5. Jelínek, J. a kolektiv *Trestní právo hmotné*, Praha, Linde 2008, 3. přepracované a aktualizované vydání
6. Litvák, D. *Warez je sport*, Internet #59, str. 14-20
7. *Vše o warezu*, Computer 3/2006, str. 82-87
8. Craig, P. *Software Piracy Exposed*, Syngress Publishing, Inc. 2005

Právní předpisy:

1. Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
2. Zákon č. 40/1964 Sb., Občanský zákoník
3. Zákon č. 513/1991 Sb., Obchodní zákoník
4. Zákon č. 140/1961 Sb., Trestní zákon

12. Summary

Software piracy is nowadays one of the most important social phenomenon. The primary reason is current fast development of information technologies, mainly the international electronic network that provides files and data transfer called Internet. This development caused that almost everyone is able to get a pirated copy of copyrighted work by using any computer on any place. That's why the protection of copyrighted works and intellectual property rights in general is becoming very important question of law. The reason why I have chosen this topic is that I have been working as a software auditor for a few years. I also use computers every day in work and at home as well. Study of law provides me with a different perspective of view and because of that I was able to combine technical and legal components in my work.

The purpose of my work was to define software piracy in general, but it is almost impossible without many single definitions which I have included in first two chapters. In three following chapters I have defined classes of software (computer programs) and common examples of breaching the intellectual property law in connection with software piracy. I have also mentioned some exceptions relating to software, particularly copy for personal use.

The largest chapter of my work deals with the possibilities of breaching the law by using the Internet. I have focused on two main parts, which are in my point of view the most important and most frequent. The first one is so called "warez" community, its origin, definition, typology and the second chosen topic is P2P (peer-to-peer) sharing. After a short introduction into P2P technical specifications, I have summarized the most important P2P networks from the past. For the closer look into practical area I have described two very important cases which are taking place on trial nowadays.

In the next chapter I have tried to gave a legal analysis in respect to all subjects (including individuals, server operators and internet service providers). The main legal question was the responsibility of all concerned subjects regardless it was civil or criminal responsibility.

The last chapter describes legal possibilities de lege ferenda and gives a short brief of unsolved legal issues, notably the absence of judicature in the Czech republic.

13. Klíčová slova (keywords)

software

pirátství

autorské právo

software

piracy

intellectual property