UNIVERSITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA
KATEDRA TRESTNÍHO PRÁVA

Trestněprávní a kriminologické aspekty internetové kriminality

DIPLOMOVÁ PRÁCE
31.7.2008

Vedoucí diplomové práce: JUDr. et Bc. Tomáš Gřivna, Ph.D.

Diplomant: Jiří Krupička, 5. ročník

Adresa: Vladivostocká 807/5
Praha 10 - Vršovice
100 00

Obor: Trestní právo a trestní řízení

Akademický rok : 2007/2008

Prohlášení o původnosti diplomové práce

Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a že jsem vyznačil prameny, z nich jsem pro svou práci čerpal, způsobem ve vědecké práci obvyklým.

V Praze dne 31.7.2008

Jiří Krupička

Obsah

Seznam použitých zkratek:

tr.zák., TZ	zákon č. 140/1961 Sb., trestní zákon
nov.tr.zák., NTZ	vládní návrh zákona trestní zákoník, sněmovní tisk č. 410 ze dne 25.2.2008
AutZ	zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
TČ	trestný čin
Informační směrnice	směrnice č. 2001/29/ES o harmonizaci některých aspektů práva autorského a práv souvisejících v informační společnosti
úmluva	Úmluva o počítačové kriminalitě, sjednaná dne 23.11.2001 v Budapešti, ve znění dodatkového protokolu ze dne 28.11.2003 ve Štrasburku o kriminalizaci jednání rasistické a xenofobní povahy spáchaných počítačovými systémy

Úvod

Internetová kriminalita je fenomén velice mladý, vždyť internet v podobě, jak ho známe dnes, je starý přibližně 15 let. To však neznamená, že by tento druh kriminality byl méně závažný nebo méně rozšířený než ostatní druhy kriminality. Masovost, relativní anonymita a postupující globalizace v internetu spolu s překotným rozvojem techniky poskytují specifické podmínky, které jsou využívány jak organizovaným zločinem, tak jednotlivci k páchání nejrůznějších sociopatologických činů různého stupně společenské nebezpečnosti od přestupků až po nejzávažnější trestnou činnost.

Současná kriminologie a trestněprávní nauka však tuto problematiku ponechává poněkud na okraji zájmu, nejspíše z důvodu úzkého sepětí internetové kriminality s moderními a pro „laika" těžko pochopitelnými technologiemi. Tomuto fenoménu je věnováno v porovnání s ostatními druhy kriminality daleko méně monografií, většinou od úzkého okruhu autorů. Komplikovanost studia internetové kriminality pak je umocněna doslova překotným technologickým rozvojem, který způsobuje, že odborná literatura popisující dané téma velice rychle zastarává. Jen v málokterém kriminologickém či trestněprávním oboru je nutné přehodnotit výsledky bádání již po několika málo letech. Tak například ještě v roce 1998 bylo nejrozšířenější přenosné datové médium disketa o kapacitě cca 1,44 MB. Nyní, v roce 2008 je tímto médiem disk DVD o kapacitě cca 4,7 GB, tedy asi 3.500 x větší! Tak překotný vývoj v počítačových technologiích musel nutně mít za následek změnu i v oblasti internetu (rychlost přenosu dat v internetové síti se taktéž zněkolikanásobila) a ve svém důsledku muselo dojít i ke změně kriminálních jevů, které se v souvislosti s používáním internetu objevují. Vědecké disciplíny zabývající se trestnou činností tak ani nemohou dostatečně rychle reagovat na nejaktuálnější problémy a ve svých výzkumech je alespoň obecně popsat.

Tato práce nemá sloužit vzhledem ke svému rozsahu k zevrubnému a všeobjímajícímu rozboru internetové kriminality. Cílem práce je kriminologický popis společensky nebezpečných jevů vyskytujících se v souvislosti s internetem, a to konkrétně podmínky a okolnosti vzniku těchto jevů, nejčastější způsob páchání trestné činnosti, možnosti prevence a následně trestněprávní kvalifikace těchto jevů. Práce sama pak je rozdělena do tří samostatných částí.

První část obsahuje obecný úvod do problematiky. Nalezneme zde definici pojmu internetu a internetové kriminality, její odlišení od pojmu počítačové a kybernetické kriminality a její členění.

Druhá část popisuje vybrané typy trestné činnosti páchané přímo nebo prostřednictvím internetu, v každé hlavě je rozbor (kriminologický a následně trestněprávní) jednoho typu. Ve výběru byl dán důraz na nejaktuálnější problémy, tedy na ochranu autorských práv (této problematice je věnována nejrozsáhlejší část této práce), „hacking" a internetové viry, tzv. nigerijské listy a „phishing", nelegální šíření pornografie, zejména dětské, a zneužívání strojového času v souvislosti s internetem.

Poslední část sestává z analýzy právních předpisů a jednotlivých norem jak současného stavu (de lege lata), tak zamýšlených změn v novém dosud nepřijatém trestním zákonu. Nebudou chybět ani úvahy nad potřebnými změnami do budoucna (de lege ferenda).

Před přečtením práce je třeba čtenáře upozornit, že s ohledem na výše naznačenou propojenost problematiky s moderními technologiemi není možné, aby tato práce, ač primárně právní (resp. kriminologická a trestněprávní), se od technické terminologie zcela oprostila. Je tomu tak zejména při popisu jednání, kterým pachatel naplňuje skutkovou podstatu trestného činu spáchaného prostřednictvím internetu nebo v jeho souvislosti. V takových případech se autor snažil nezabředávat do zbytečných a s problematikou přímo nesouvisejících detailů, nebo se je pokusil ve stručnosti a poněkud „laickém" duchu vysvětlit.

I. Obecná část

1. Vymezení pojmů

Narozdíl od oborů technických, kde je možné snad každý pojem, institut či proces poměrně jasně definovat, je u oborů humanitních (tedy i v kriminologii) toto vymezení značně obtížnější. Je tomu tak zejména proto, že obsah pojmů je většinou každou individualitou vnímán rozdílně. Definice v těchto oborech jsou tak ve snaze zachytit vše, co by pod zkoumaný pojem mohlo spadat, příliš obecné, nebo naopak, pokud jsou konkrétní, často nepostihují všechny aspekty zkoumaného fenoménu. To platí zejména u těch společenských jevů, které se v čase vyvíjí, takže se mění i jejich reálný obsah. Bohužel je to i případ internetové či počítačové kriminality.

K tomu, abychom mohli předložit definici internetové kriminality, bude třeba taktéž definovat jevy nadřazené, příbuzné či dokonce synonymní a odlišit je od sebe navzájem. Těmito pojmy jsou zejména „počítačová kriminalita" a „kybernetická kriminalita".

1.1 Pojem počítačové kriminality

Tento pojem bývá nejobecněji definován jako nekalá (společensky škodlivá, trestná) činnost páchaná pomocí počítačů[1], a to shodně i v zahraničních pramenech[2]. Další možnou definicí je trestná činnost, při které tvoří počítač či počítačová síť nezbytnou součást této činnosti, a zároveň takové jednání, při kterém je počítač použit k umožnění spáchání trestného činu[3]. Tyto obecné definice se pak potýkají se základním problémem, a to že zahrnují i jednání, která vlastně s počítačovou kriminalitou nemají nic společného, například pokud pachatel počítačem udeří oběť trestného činu do hlavy a způsobí ji tak těžké zranění.

Dalším možným přístupem k definování počítačové kriminality bývá výčet druhů jednání, která pod tento pojem spadají jako:

1) útok na počítač, program, data, komunikační zařízení
2) neoprávněné užívání počítače či komunikačního zařízení (zneužívání či krádež počítačového času)
3) neoprávněný přístup k datům, získání utajovaných informací (počítačová špionáž) nebo jiných informací o osobách, podniku, výrobě, atp.
4) neoprávněná změna v programech a datech či v hardwaru počítače
5) zneužívání počítačových prostředků k páchání jiné trestné činnosti, zejména podvodům

---

[1] Musil, S.: Počítačová kriminalita. IKSP, Praha 2000, str. 7

[2] Watson Business Systems Ltd: A Guide To Computer Crime - An Introduction To Computer Crime and Internet Fraud, http://legal.practitioner.com/computer-crime/, zobrazeno 20.6.2008, 16:22

[3] Wikipedia; http://en.wikipedia.org/wiki/Computer_crime; zobrazeno 20.6.2008, 16:20

6) porušování průmyslových práv a práv duševního vlastnictví prostřednictvím počítače či sítí (tzv. počítačové pirátství)[4]
K tomuto výčtu bych ještě přiřadil:
7) výroba a šíření pornografie (zejména dětské) prostřednictvím počítačů a počítačových sítí
8) propagace rasismu a xenofobie prostřednictvím počítačových sítí
9) počítačový terorizmus

Tyto definice výčtem, ač v době uveřejnění i vyčerpávající, mohou vzhledem k překotnému pokroku v IT technologiích záhy zastarávat. Poslouží však dobře k pochopení obsahu pojmu, tedy jaká jednání pojem počítačová kriminalita zahrnuje.

1.2 Pojem internetové kriminality

Při definici pojmu internetové kriminality se nutně musíme potýkat se stejnými problémy jako u pojmu počítačové kriminality. Tu můžeme nejjednodušeji definovat jako trestnou činnost páchanou v síti internet, užíváním internetu, popřípadě prostředky internetu[5]. Podobně vyzní definice internetové kriminality jako aktivity, při nichž je užito internetu za účelem spáchání trestného činu či jiného deliktu. Ve vztahu k počítačové kriminalitě lze říci, že počítačová kriminalita je pojem nadřazený pojmu internetové kriminality, neboť si lze jen těžko představit trestný čin spáchaný prostřednictvím internetu, který by nebyl spáchaný i prostřednictvím počítače. Samotná podstata internetu totiž spočívá v decentralizované vzájemně propojené síti tzv. serverů, které nejsou ničím jiným než k tomuto cíli upraveným počítačem.

1.2.1 Podstata internetu

Protože zde podaná definice je vlastně definice kruhem („internetová kriminalita je kriminalita páchaná ve spojení s internetem"), bude zde nutné krátce pohovořit o podstatě internetu a jeho historii.

Internet můžeme v krátkosti definovat jako celosvětovou síť, která propojuje obrovské množství jednotlivých lokálních sítí, na níž je kdykoliv možný přístup, pokud je připojení, a kde dochází k přenosu dat v rámci těchto sítí. Nejznámější službou, kterou internet poskytuje, je World Wide Web (zjednodušeně vzájemně propojený soubor dokumentů a dalších zdrojů umožňující prohlížení stránek). Dalšími službami jsou např. e-mail (elektronická pošta) a sdílení souborů.

Ačkoliv vznik internetu se datuje už ke konci 60. let 20. století (tehdy pod názvem ARPANET jako vojenský projekt americké armády během studené války[6]), pravý rozmach internetu přišel až počátkem 90. let minulého století, kdy 9.8.1991 ve vědeckém středisku CERN na švýcarsko-francouzské hranici byl představen World Wide Web (www., taktéž zkráceně web), jenž proměnil internet od univerzitní sítě k celosvětově rozšířenému médiu.

---

[4] Dastych, J.: Počítačová kriminalita – stručný přehled v Musil, S.: Počítačová kriminalita. IKSP, Praha 2000, příloha 2

[5] Wikipedia; http://en.wikipedia.org/wiki/Internet_crime; zobrazeno 20.6.2008, 17:20

[6] poprvé představen 29.10.1969

K 31.3.2008 byl počet uživatelů internetu již 1.412.489.652[7], přičemž tento počet neustále narůstá.

1.3 Pojem kybernetické kriminality

Dostatečně definovat pojem kybernetické kriminality je v rámci všech tří uvedených pojmů zdaleka nejsložitější. Tento pojem je totiž i v odborné literatuře používán v různých významech. Většinou je uváděn jako synonymum k pojmu počítačová kriminalita. Tak je tomu i v případě nejvýznamnější úmluvy týkající se počítačové, resp. internetové kriminality, tzv. Úmluvy o počítačové kriminalitě sjednané dne 23.11.2001 v Budapešti, jejíž anglický název je „Convention on Cybercrime", tedy vhodnější by se zdál překlad „Úmluva o kyberkriminalitě".

Při vymezení tohoto pojmu nelze využít ani sémantického výkladu slova kybernetický, neboť od původního významu znamenajícího „týkající se řízení a sdělování v živých organismech a strojích"[8] došlo k podstatnému posunu. Je možné souhlasit s tvrzením, že kybernetická kriminalita je kriminalita v kyberprostoru, tedy kriminální činnost páchaná v jakémsi elektronickém (virtuálním) světě, která má však zásadní dopady ve světě reálném[9].

Jelikož je tento kyberprostor vytvářen zejména elektronickými sítěmi, zdá se být velice výstižná[10] definice pojmu kybernetické kriminality jako souhrn všech kriminálních aktivit, které jsou páchány prostřednictvím komunikačních zařízení propojených v síti. Může se tak dít prostřednictvím internetu, telefonních, mobilních či jiných obdobných sítí.[11] V takovém případě by „kyberkriminalita" netvořila podmnožinu počítačové kriminality, jelikož určitá trestná činnost by mohla být páchána prostřednictvím např.mobilního telefonu. V takovém případě bychom nemohli hovořit o počítačové kriminalitě. Naopak internetová kriminalita by potom ležela v průniku počítačové kriminality a kybernetické kriminality.

Ve většině případů (zejména v zahraniční literatuře) se však pojmy kybernetická kriminalita a počítačová kriminalita používají promiscuae, obecný trend však spěje k nahrazení termínu počítačová kriminalita pojmem kybernetická kriminalita.

2. Členění internetové kriminality

2.1 Typové členění

---

[7] World Internet Usage Statistics News and Population Stats, http://www.internetworldstats.com/stats.htm, zobrazeno 20.7.2008, 14:50

[8] Wiener, N.: Kybernetika a společnost. Academia, Praha 1963

[9] Jaishankar, K.: Cyber Criminology: Evolving a novel discipline with a new journal, in International Journal of Cyber Criminology. Vol 1 Issue 1, Editorial, January 2007

[10] pokud tedy chceme vzájemně odlišit počítačovou a kybernetickou kriminalitu

[11] Wikipedia; http://en.wikipedia.org/wiki/Cybercrime; zobrazeno 20.6.2008, 17:25

Stejně jako u počítačové kriminality je možné rozdělit internetovou kriminalitu na základní 2 skupiny: 1) přímá internetová kriminalita

2) nepřímá internetová kriminalita

Toto členění vychází z řešení otázky, zda je internet esenciální součástí trestné činnosti, tedy zda se tento druh kriminality děje výhradně v prostředí internetu, či zda je internet pouhý prostředek k usnadnění páchání trestné činnosti.

Do první skupiny patří zejména všechna jednání, která souborně nazýváme „hackerství" (někdy „hacking"), tedy spočívající v průniku do počítačových a síťových systémů, dále je sem možno zařadit krádež počítačového času – v případě internetu je to typicky krádež konektivity, dále např. spamming (masové rozesílání nevyžádaných zpráv, zejména reklamy) a v rámci porušování autorských práv je to tzv. crackování (softwarové překonávání účinných technických prostředků ochrany).

Pro tuto skupinu je typické, že kriminální aktivity v této skupině obsažené nemají obvykle výrazně podobný ekvivalent mimo kybernetický svět. Jsou obvykle spjaty s nelegálními počítačovými programy speciálně vytvořenými pro tuto činnost (tzv. „malware") a od počátku do konce těchto aktivit nedochází k fázi odpoutání se od internetu k trestné činnosti v reálném světě. Tato jednání obvykle naplňují skutkovou podstatu trestných činů, které byly za účelem postihu specifických projevů internetové kriminality do trestních předpisů doplněny.

Oproti tomu druhá skupina, kam patří zejména propagování rasismu a xenofobie prostřednictvím internetu, šíření dětské a zvrácené pornografie, podvodná jednání prostřednictvím internetové sítě, on-line gamblerství a neoprávněné provozování loterie nebo podobné sázkové hry, popřípadě internetové obtěžování (stalking), obvykle svůj protějšek v realitě má nebo není svou existencí na internetu závislá.

Na rozdíl od první skupiny není většinou k páchání těchto aktivit nutný nelegální počítačový program, prostředky internetu, které tyto aktivity využívají, jsou obvykle legální. Také jejich trestněprávní kvalifikace spočívá na subsumpci pod obvyklé skutkové podstaty známé z neinternetového prostředí (podvody, vydírání, ohrožování mravnosti, podpora a propagace hnutí směřujících k potlačení práv a svobod člověka, atd.).

Je pochopitelné, že hranice mezi těmito dvěma skupinami není vždy ostrá, některá kriminální jednání mají částečně vlastnosti první skupiny, částečně druhé. Jedná se typicky o porušování autorských práv, zejména v peer to peer sítích, některé typy phishingu, kyberterorismus, aj.

2.2 Členění dle úlohy internetu při páchání trestné činnosti

Jiným (avšak do značné míry příbuzným) druhem členění může být dle postavení internetu v kriminálních aktivitách. Poté je možné internetovou kriminalitu rozdělit na[12]:

[12] tamtéž

1) trestnou činnost, při níž je internet použit jak prostředek, či spíše nástroj. Klasickým zástupcem bude spamming, phishing a porušování autorských práv, zejména v peer to peer sítích

2) trestná činnost, při níž je internet (síť, některá jeho složka nebo služba) cílem – předmětem – útoku. Sem patří hacking a krádež konektivity

3) trestnou činnost, při níž je internet pouhým místem útoku. Hlavním představitelem této skupiny jsou trestné činy spočívající v porušování práv k ochranným známkám a nekalé soutěži.

2.3 Členění dle motivu

1) ty společensky škodlivé aktivity, jejichž primární účel je zisk nebo jiný prospěch

2) trestná jednání páchaná „nezištně"

Internet je oproti reálnému světu specifický zejména tím, že trestné činy tu spáchané nemusí mít často za účel získání hmatatelnějšího prospěchu. To je patrné zejména u hackerství, kde průniky do cizích systémů jsou často prováděny bez úmyslu získat přístupem nějaký prospěch, ale třeba jen pro radost či uspokojení z toho, že je hacker lepší, než „protivník na druhé straně", tedy bezpečnostní technik, správce sítě, administrátor, atd. Neznamená to však, že by tato jednání nebyla společensky nebezpečná, mohou znamenat obrovské ztráty (vyřazení sítě, náklady na nápravu bezpečnostních mezer, ztráty na výdělku apod.).

2.4 Členění dle objektu

Internetovou kriminalitu je možné členit taktéž dle objektu, k jehož porušení či ohrožení směřují jednání tvořící v souhrnu internetovou kriminalitu. Toto rozdělení (majetkové trestné činy v síti internet, trestné činy proti republice, hospodářské, hrubě narušující občanské soužití...) se neliší od obecného členění trestných činů trestněprávní naukou, a proto v podrobnostech na ni odkazuji.

3. Důvody rozmachu a latence internetové kriminality

3.1 Nejdůležitější faktory růstu prevalence internetových deliktů

Hlavními důvody exponenciálnímu růstu internetových deliktů jsou:

1) Globalizace – internet se v dnešní době rozšířil po celém světě. S tím se však pochopitelně rozšířil i dosah internetové kriminality, takže pachatel může v „teple svého domova" páchat trestné činy s efektem v nejrůznějších státech na celém světě.

2) Technologický pokrok, který s sebou nese i rychlý vývoj a zvyšující se dostupnost prostředků internetové kriminality (zejména speciální programy určené k páchání této trestné činnosti)

3) Nízké náklady internetové kriminality – k páchání trestné činnosti spojené s internetem postačí často pouhý počítač v hodnotě několika málo tisíců korun a dostatečně kvalitní připojení.

4) Závislost dnešního světa na internetu a počítačích vůbec – kdo by si dnes mohl představit fungování běžného života bez internetu (e-mailu, webu jako informačního zdroje, etc.)? Zřejmě jen málokdo. Vždyť i vysoké školy vykonávají velkou část své administrativní agendy (přihlašování do ročníku a ke zkouškám, sdělování studijních informací, předávání informačních zdrojů aj.) pouze elektronicky. S tímto vývojem pak ruku v ruce jde i umísťování stále více důležitých (a zneužitelných) informací na internetu. Je zřejmé, že toto prostředí pak představuje skvělé podhoubí nejrůznějších trestných činů.

5) Absence schopných strážců – jelikož je internet ve skutečnosti decentralizovaná síť, která není vlastněna určitou osobou (pouze jsou tu poskytovatelé připojení a tzv. poskytovatelé volného prostoru), neexistuje ani určitá osoba, která by využívání internetu kontrolovala. Policejní orgány jednotlivých zemí často narážejí na omezenou teritoriální působnost a často jim chybí dostatečně kvalifikovaný a zkušený personál. Trestní represi pak o to víc ztěžuje, že (datové) stopy činu velice rychle mizí či jsou velice těžko identifikovatelné.

6) Anonymita (někdy však relativní) pachatelů – internet je lákavým prostředím k páchání trestné činnosti, neboť nabízí pachatelům anonymitu, kterou by ve skutečném světě nikdy neměli. I když existují prostředky (zejména softwarové), které napomáhají identifikovat pachatele (IP a MAC adresy), existují stejně tak i prostředky, které identitu pachatele skryjí, či umožní vydávat se za osobu jinou.

3.2 Důvody latence kriminality

Internetová kriminalita je nejvíce skrytá kriminalita, kde je nízká pravděpodobnost detekce, vysoká neochota tuto trestnou činnost oznamovat a nedostatečné zabezpečení.[13] Tento názor dokládají i statistické výzkumy, dle kterých zůstává 90 % internetové kriminality neodhaleno.[14]

Je smutnou skutečností, že většina trestných činů spáchaných v internetu není vůbec zjištěna, a to díky podcenění bezpečnostních opatření. Důsledné dbání na bezpečnost osobních i firemních počítačů je z hlediska prevence internetové kriminality bezpodmínečnou nutností. Uživatelé internetu, pokud se nechtějí stát oběťmi internetové kriminality, musí využívat co nejširší kombinaci bezpečnostních prvků, jako je antivirový program, firewall a stahování bezpečnostních aktualizací programů instalovaných v počítači.

Neochota oznamovat zjištěné trestné činy orgánům činným v trestním řízení je spolu s dalšími obecnými důvody latence kriminality typická pro většinu druhů kriminality. V případě internetové kriminality je však tato zdrženlivost až extrémní. Jsou k tomu minimálně tři základní důvody. Prvním z nich je obava oběti (zejména organizací) ze ztráty důvěry klientů, zaměstnanců či akcionářů v případě, že by se dozvěděli o útoku. Ztráta této důvěry by pro mnoho společností mohla znamenat větší škody, než ztráty, které utrpěly samotným trestným činem.

---

[13] Adamski A.: Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI) in HEUNI's publication Series No. 34, 1998.

[14] Wikipedia; http://en.wikipedia.org/wiki/Cybercrime; zobrazeno 20.6.2008, 17:25

Druhým důvodem (zde zejména u fyzických osob) je ten, že se obávají poskytnout orgánům činným v trestním řízení dostatečnou součinnost, při které by mohlo být zjištěno, že tyto osoby k internetové kriminalitě samy přispívají, např. neoprávněným užíváním software, či jen z pouhého pocitu, že by je samotné vyšetřování příliš obtěžovalo.

Posledním důvodem je pak možnost přilákání spáchání dalšího internetového trestného činu na prvotní oběti. Zvyšuje se tak tzv. viktimnost = stupeň rizika, že se ten který jedinec stane obětí trestného činu (jedná se tedy o disponovanost jedince či skupiny osob stát se i třeba znovu obětí trestného činu).

4. Pachatelé internetové kriminality

Internetová kriminalita se od jiných typů kriminality liší tím, že její vznik a rozvoj je přímo spojen s moderními technologiemi. Tato skutečnost se pak odráží v mnoha specifických rysech internetové kriminality, např. v typologii pachatele.

Vzhledem k sepětí internetové kriminality s technologiemi, je možné obecně říci, že typický pachatel internetové trestné činnosti je spíše nadprůměrně inteligentní a v drtivé většině mladšího (často ve věku náctiletých) až středního věku. Je to způsobeno tím, že starší generace obvykle hůře akceptují nové technologické vymoženosti, a proto, pokud se uchylují k trestným aktivitám, uskutečňují je spíše tradiční cestou. Některé typy deliktů internetové kriminality (typicky hacking) vyžadují ke svému provedení značnou technickou znalost. Je proto pochopitelné, že osoby s vyšším inteligenčním kvocientem získají tuto znalost rychleji a často efektivněji, než osoby s podprůměrnou inteligencí.

Jiným aspektem, který spoluurčuje charakter pachatele internetové kriminality je ten, že se zde prakticky nevyskytují trestné činy proti životu a zdraví (jednou z mála výjimek, které si lze představit, je případ hackera, který úmyslně změní data v databázi pacientů nemocnice tak, že jim je podán jiný lék, který způsobí smrt, a dále některé druhy kyberterorismu). Proto bude v prostředí internetu (odhlédneme-li od propagace a šíření rasismu a xenofobie a dále od sadistických pedofilů) jen málo „násilnických" typů pachatele.

Díky rapidnímu zvýšení počítačové gramotnosti a rozšíření internetu není internetová kriminalita již dávno výsadou vyšších společenských tříd. O internetové kriminalitě obecně nelze hovořit jako o kriminalitě bílých límečků, ačkoliv mnoho druhů činů páchaných v internetu má charakter majetkové či hospodářské kriminality. Jako zářný příklad dobře poslouží obvyklý pachatel - „hacker", kterého lze charakterizovat všemi možnými atributy, jen ne právě „bílým límečkem".

Výhodou kybernetického světa, kde se internetová kriminalita odehrává, je (alespoň pro pachatele) skutečnost, že nemusí absolutně korespondovat s realitou. Pachatelé se tu často cítí, a dokonce i mohou být, úplně jiným člověkem, než jsou ve skutečném světě. Kyberprostor a internetová kriminalita pak mohou sloužit jako prostředek „seberealizace" a možnosti dokázat si, že jsem lepší než ostatní. Že k tomuto cíli může posloužit i kriminální činnost, je dobře známé i z reálného světa. Prostředí internetu k tomu však nabízí takřka ideální podmínky.

5. Vybrané trestněprávní aspekty internetové kriminality

5.1 Obecně k trestní odpovědnosti

Aby mohl být pachatel odpovědný ze spáchání trestného činu[15], je vždy bezpodmínečně nutné, aby byly vždy naplněny všechny znaky trestného činu uvedené v trestním zákoně[16] (naplnění všech znaků trestného činu jako conditio sine qua non trestní odpovědnosti). Právní nauka dělí tyto znaky na formální a materiální (formální a materiální stránka TČ). Toto rozdělení vychází z formálně-materiálního pojetí trestného činu uvedeného v definici v ust. § 3 odst. 1, 2 tr.zák[17]. Formálními jsou ty znaky TČ, které jsou uvedeny v trestním zákoně. Jsou jimi obecné znaky (příčetnost a věk[18]) a znaky skutkové podstaty trestného činu (objekt, objektivní stránka, subjekt a subjektivní stránka, protiprávnost).[19]

5.2 Společenská nebezpečnost a internetová kriminalita

Téma společenské nebezpečnosti jednání pachatelů vedoucí k trestněprávní odpovědnosti je v odborných kruzích značně diskutované[20]. Aby byla naplněna materiální stránka trestného činu, je dle § 3 odst. 2 tr.zák. nutné, aby nebezpečnost činu pro společnost byla vyššího stupně než nepatrného[21]. Samotný pojem nebezpečnosti činu pro společnost však není v zákoně definován. Nauka tento pojem definuje jako ohrožení nebo porušení společenských vztahů (zájmů, hodnot), vyjadřuje celkovou závažnost činu pro společnost, a to z hlediska objektivních i subjektivních znaků včetně pachatele[22], a dále potřebu společnosti reagovat na pachatelovo jednání uložením trestněprávní sankce. Konkrétní stupeň nebezpečnosti činu pro společnost je příkladmo uveden v § 3 odst. 4 tr.zák. jako význam chráněného zájmu, který byl činem dotčen, způsob provedení činu a jeho následky, okolnosti spáchání trestného činu, osoba pachatele, míra zavinění pachatele a jeho pohnutka.

K tomuto je třeba doplnit, že se hodnotí konkrétní význam konkrétního zájmu zasaženého trestním činem, nikoliv význam typový, neboť ten již je vyjádřen ve skutkové podstatě TČ a

---

[15] resp. provinění u mladistvých pachatelů, dále jen: „trestný čin" či „TČ"

[16] dále také „tr.zák."

[17] V této souvislosti je třeba upozornit na skutečnost, že de lege ferenda je v návrhu nového tr.zák. toto pojetí opuštěno a nahrazeno pojetím formálním – viz část III. Úvahy de lege lata a de lege ferenda

[18] K věku pak přistupuje rozumová a mravní vyspělost (tzv. relativní trestní odpovědnost mladistvého)

[19] Podrobněji např. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 101 a násl.

[20] viz např. diskuze k vybraným tématům na webu www.itpravo.cz

[21] u mladistvých pak vyšší než malého (§ 294 ZSVM)

[22] Dolenský, A.: Pojem, povaha a stupeň nebezpečnosti činu pro společnost v Diferenciace trestní odpovědnosti, sborník. Univerzita Karlova, Praha 1983, str. 172

v trestní sazbě.[23] Tak například v případě porušování autorských práv prostřednictvím internetu se posuzuje, do jaké míry bylo zasaženo do autorských práv (jiná bude jistě nebezpečnost činu pro společnost v případě provozování serveru, na kterém jsou nelegálně poskytnuta díla stovky autorů, a jiná bude u osoby, která na své osobní stránky na neznámé doméně zpřístupní zkrácenou nahrávku písně své oblíbené kapely). U způsobu provedení činu a jeho následku bude z hlediska materiální stránky trestného činu relevantní zejména rozsah škod trestnou činností způsobených, nemusí to však být jediným kritériem. Ohledně hodnocení okolností, za kterých byl čin spáchán, je třeba u internetové kriminality, která je jinak „sterilní", co se týče místa a doby spáchání trestného činu (místem TČ je internetová síť a ta místa, kde se nachází počítač či přímo server, prostřednictvím nichž k trestné činnosti dochází), zkoumat, zda stoupá tendence k páchání podobných trestných činů a zda je podobná kriminalita na vzestupu či nikoliv.

Problematické bude posuzování materiální stránky trestného činu z hlediska pachatele, konkrétně jeho věku. Obecně totiž platí, že pokud je čin spáchán osobou mladistvou či pachatelem ve věku blízkého věku mladistvých, není nebezpečnost činu pro společnost taková, jako například u „zkušeného a protřelého" recidivisty, a to zejména z důvodu, že u osob nižšího věku lze předpokládat, že nemají doposud úplné povědomí o všech právních předpisech (ačkoliv ignoratia legis non excusat) a že jsou více nerozvážní a jednají impulzivněji) [24]. U internetové kriminality je to však obvykle právě pachatel mladšího věku, zejména z důvodu vyšší schopnosti pochopit a pojmout nové technologické trendy, kdo je zkušený a kdo si je často velice dobře vědom následků svého jednání.

5.3 Místní působnost norem trestního práva

Místní působností se rozumí okruh případů (společenských vztahů), na které se trestněprávní norma vztahuje se zřetelem k místu, kde byl čin spáchán[25]. Při otázce, zda-li se určité jednání pachatele bude posuzovat podle trestněprávní normy určitého státu, bude třeba taktéž přihlédnout k místu spáchání trestného činu.

Jedním ze dvou základních principů v rámci určování působnosti trestního zákona ČR, je princip teritoriality (§ 17 tr.zák.), který stanoví, že: *Podle zákona České republiky se posuzuje trestnost činu, který byl spáchán na území republiky.* (§ 17 odst. 1 tr.zák.). Přitom za čin spáchaný na území republiky se považují i taková jednání pachatele na území České republiky, i když porušení nebo ohrožení zájmu chráněného trestním zákonem nastalo nebo mělo nastat (a to i z části) v cizině (§17 odst. 2 písm. a) tr.zák.), nebo se za ně považují ta pachatelova jednání uskutečněná v cizině, pokud na území republiky pachatel porušil nebo ohrozil zájem chráněný trestním zákonem (či měl-li tu takový následek nastat).

---

[23] Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 142

[24] tamtéž, str. 143

[25] tamtéž, str. 48

Vedle zásady teritoriality se dále uplatňuje zásada personality, tj. že podle trestního zákona se posuzují i trestné činy spáchané občany ČR v cizině (§ 18 tr.zák.). K těmto základním principům přistupují další tzv. princip ochrany, univerzality a subsidiární zásada ochrany[26].

Mezi těmito zásadami ovládající určování místní příslušnosti je to právě zásada teritoriality, která je pro internetovou kriminalitu určitým způsobem specifická. Tato specifičnost je dána tím, že prostředí internetu nemá ve své podstatě územní omezení, a tudíž je velice obtížné stanovit, pokud byl tento čin spáchán v prostředí internetu, na území kterého státu byl spáchán. U některých aktivit je zodpovězení této otázky zřejmé. Tak například u hackingu jsou těmito státy místo fyzického umístění předmětu útoku (počítač koncového uživatele, server, atd..) a místo, odkud hacker vysílal softwarové příkazy či soubory (hackerův počítač, počítačová kavárna atd.). I zde však nalezneme určité problémy: Pokud totiž hacker napadne a vyřadí funkci webových stránek, které[27] mohou být zpřístupněny odkudkoliv a informace na nich obsažené mohou mít esenciální význam pro adresáty, je otazné, zdali bude možné pak aplikovat trestní normy země původu adresátů (neboť tam měla trestná činnost největší dopad). Výkladem ust. § 17 odst. 2 písm. b) tr.zák. dojdeme k závěru, že ano. Otázkou ale je, zda to platí i u případů, kdy by se měla místní působnost trestních norem odvozovat od pouhé skutečnosti, že trestný čin byl spáchán prostřednictvím internetu a podstatou této trestné činnosti je využívání internetu jako místa činu (porušování autorských práv, šíření pornografie, rasismu a xenofobie, atd.). Americké soudy obecně působnost amerických trestněprávních norem dovozují, v Evropě je často vyžadován alespoň minimální vztah k území státu, jehož trestněprávní normy přicházejí v úvahu k užití.[28]

5.4 Kriminální aktivity na internetu a jejich trestněprávní kvalifikace

Jak již bylo řečeno výše, pod pojem internetová kriminalita spadá řada trestných jednání, které se od sebe navzájem v mnoha aspektech liší (chráněný zájem, který ohrožují či porušují, způsob provedení, předmět útoku, motiv, atd.), jediným společným prvkem pak bývá právě internet. Stejně tak se i liší jejich trestněprávní kvalifikace. V následující tabulce je stručný přehled (nikoliv však úplný) různých jednání, která pod internetovou kriminalitu řadíme, a trestné činy, jejichž základní skutkovou podstatu mohou obvykle naplňovat.[29]

---

[26] v podrobnostech např. Novotný, O., Vanduchová, M. a kol.: Trestní právo hmotné. I. Obecná část. ASPI, a.s., Praha 2007, str. 98 a násl.

[27] navíc nohou být uloženy na serveru jiné země, než je země původu většiny návštěvníků této stránky

[28] Viz např. rozhodnutí německého Spolkového soudního dvoru ze dne 12. prosince 2000, sp.zn.: 1 StR 184/00.

[29] Trestněprávní kvalifikace nezahrnuje všechny možné jednočinné souběhy trestných činů, zde uvedeny jsou pouze ty trestné činy, které jsou při daném jednání naplněny takřka vždy.

	Jednání	Trestný čin
1.	Hacking	Poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 tr.zák.
2.	Phishing	Podvod dle § 250 odst. 1 tr.zák.
3.	Kyberterorismus	Teroristický útok dle § 95 odst. 1, 2 tr.zák., popř. Sabotáž podle § 97 odst. 1 tr.zák. či Obecného ohrožení dle § 179 odst. 1 tr.zák.
4.	Krádež (zneužívání) počítačového času a konektivity	Neoprávněné užívání cizí věci dle § 249 odst. 1 alinea 1, 2 tr.zák., Krádež dle § 247 odst. 1 písm. a) tr.zák., Poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 tr.zák.
5.	Šíření zvrácené pornografie a zpřístupňování pornografie dětem	Šíření pornografie dle § 205 odst. 1, 2 tr.zák.
6.	Propagace rasismu a xenofobie	Násilí proti skupině obyvatelů a proti jednotlivci dle § 196 odst. 1 tr.zák., Hanobení národa, etnické skupiny, rasy a přesvědčení dle § 198 odst. 1 tr.zák., Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 198a odst. 1 tr.zák., popř. Podpora a propagace hnutí směřujících k potlačení práv a svobod člověka podle § 260 odst. 1, § 261 a § 261a tr.zák.
7.	Internetové pirátství, neoprávněné užití děl, softwarová krádež	Porušování autorských práv, práv souvisejících s autorským právem a práv k databázi dle § 152 odst. 1 tr.zák.

8.	Neoprávněné užívání obchodního jména, označení původu, uvedením do oběhu zboží nebo služeb neoprávněně označované ochrannou známkou jiného	Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu dle § 150 odst 1, 2 písm. a), b) tr.zák.
9.	Počítačová špionáž	Vyzvědačství dle § 105 odst. 1, 2 tr.zák., popř. Ohrožení utajované informace dle § 106 odst. 1, § 107 tr.zák.
10.	Neoprávněné internetové loterie a neoprávněné provozování gamblingových serverů a kybercasin	Neoprávněné provozování loterie a podobné sázkové hry dle § 118a odst. 1 tr.zák.
11.	Pomlouvání a lživé osočování na internetových serverech a fórech	Pomluva dle § 206 odst. 1 tr.zák.

II. Zvláštní část

1. Porušování autorských práv v prostředí internetu

1.1 Úvod do problematiky a podmínky vzniku

Internet je takřka nekonečný zdroj informací, které jsou díky globálnímu rozšíření internetu přístupné každému v jakémkoli místě a čase. Proto internet slouží jako skvělé místo publikace, výměny, šíření a opatřování těchto dat, ať už zdarma či za úplatu. Že při tom dochází ke střetu s právy duševního vlastnictví, je navýsost zřejmé. Normy obsahující úpravu práv duševního vlastnictví, zejména pak normy autorskoprávní ochrany, jsou beze sporu nejčastěji porušovanými normami v prostředí internetu a jejich četnost jistě předčí i možná více obávané a diskutované hackerství. V této části publikace bude podrobněji pojednáno právě o porušování autorských práv, práv souvisejících s autorským právem a práv k databázi.

Důvody tak velkého nárůstu rozsahu porušování autorských práv a práv souvisejících jsou, jak už to u složitějších společenských fenoménů bývá, různé, mezi ty nejpodstatnější však lze zařadit tyto:

1. Zpřístupnění díla velkému množství adresátů je velice snadné. Neexistuje totiž žádné jiné masmédium (dle mého názoru ani televizní vysílání, které ostatně může být taktéž šířeno přes word wide web), jež by v jeden okamžik umožnilo přístup k dílu stovkám miliónů lidí na celém světě (počet uživatelů k internetu byl k 31.3.2008 přes 1,4 mld).

2. Rapidní technologický pokrok v hardware, který umožnil na jedné straně zvyšování kapacity disků serverů[30] při jejich současné miniaturizaci a na druhé straně růst kapacity připojení (konektivity). Ještě před několika lety byla většina uživatelů internetu v České republice připojena pomocí vytáčeného analogového telefonního připojení s maximální rychlostí 8 kB/s[31], avšak často s hodnotou výrazně nižší. Toto připojení umožňuje návštěvu nenáročných webových stránek, vzhledem k blokaci telefonní linky a zároveň jeho nákladnosti však neumožňuje stahování většího objemu dat. Rozmach vysokorychlostních připojení (ADSL, Ethernet, WiFi)[32] s rychlostí často přesahující 1MB/s umožnil přístup

---

[30] Zde ve významu počítač (hardware), který poskytuje službu FTP, world wide web a elektronické pošty.

[31] Na tomto místě je třeba upozornit, že často udávaná hodnota 56 kb/s je vyjádřením v jednotkách „kilobit za sekundu", přičemž 1 byte („B") = 8 bitů. K vyjádření velikosti souboru se užívá z praktických důvodů jednotka „byte" a její násobky (např. kapacita 1 disku CD-R je 700 megabyte). Poskytovatelé internetového připojení však používají k vyjádření jeho rychlosti jednotku „bit za sekundu", aby budili zdání vyšší rychlosti připojení.

Hodnoty jsou vždy uvedeny pro rychlost stahování (download), rychlost odesílání (upload) je vždy nižší (např. 4,2 kB/s pro vytáčenou linku).

[32] ADSL = vysokorychlostní připojení pomocí telefonních linek

uživatelů prakticky k jakémukoliv dílu umístěnému na internetu od hudby přes filmy až po nejrůznější programy včetně počítačových her a náročných pracovních aplikací, jejichž velikost dosahuje i několika gigabytů.

3. Růst obliby systému sdílení souborů založených na technologii peer to peer (viz níže).

4. Pachatelé se mohou skrývat v relativní anonymitě, popřípadě se „ukrývají" (rozuměj: uchylují se) do oblastí s nízkou, nebo mizivou ochranou práv duševního vlastnictví jako je jihovýchodní Asie, země bývalého SSSR, oblast Karibiku, atd.

5. Minimální náklady a bezpracnost zpřístupnění díla způsobené jednak tím, že k tomu postačí stisk několika málo kláves na klávesnici, a dále tím, že hlavním příjmem poskytovatelů prostoru (na webových serverech) je příjem z reklam, příjem za poskytnutí prostoru je v tomto ohledu velice nízký.

6. Autorské dílo nelze v síti internet chránit druhotně pomocí hmotného předmětu (nosiče), pomocí něhož je vyjádřeno, tak, jak je tomu například u originálních disků CD s hudbou.

7. Obecné neuznávání autorských práv ve společnosti, resp. jejich malá akceptace, zejména pak odpor ke kolektivním správcům a k velkým, často dominantním nahrávacím společnostem.

I když k masivnímu porušování autorských práv[33] docházelo od samého počátku vzniku internetu (drtivá většina webových stránek, resp. jejich tvůrci, určitým způsobem autorská práva porušují, když ke zvýšení atraktivity svých stránek za účelem vysoké návštěvnosti stránek a následně zisku z reklam na nich umístěných využívají cizí obrázky, ikonky, texty, zvuky, videoklipy a jiné prvky bez souhlasu autora). Následky tohoto porušení však často nebyly natolik závažné, aby oprávněné osoby hájily svá autorská práva soukromoprávními žalobami na základě odpovědnosti delikventa, natož pak aby, vzhledem k subsidiaritě trestní represe (trest až jako ultima ratio) a nutnosti naplnění materiálního znaku trestného činu, bylo šířeji využíváno institutů trestního práva.

V dnešní době však, z důvodů výše uvedených, se masovost porušování autorských práv v prostředí internetu stává závažným společenským problémem, který má za následek jak značné majetkové škody, tak i, s ohledem na osobnostně majetkovou povahu těchto práv, újmu na osobnostních právech autorů. Často tak bývá porušením autorských práv naplněna

---

Ethernet = vysokorychlostní připojení pomocí lokální sítě (nejčastěji LAN) propojené kabelem, typické pro tzv. „kabelové připojení"

WiFi = bezdrátové připojení pomocí mikrovlnného elektromagnetického záření

[33] V rámci zjednodušení bude v dalším textu využíváno pouze výrazu „autorská práva", vzhledem k podobnosti institutů však lze mnohé vztáhnout i na oblast práv s autorským právem související a práv k databázi, stejně jako bude využíváno pouze výrazu „autor", i když se mnohé bude vztahovat i na výkonného umělce, výrobce zvukového a zvukové obrazového záznamu, nakladatele, vysílatele a tvůrce databáze

jak formální stránka trestného činu (v českém právním řádě trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 152 odst. 1, 2 trestního zákona – viz níže), tak stránka materiální.

1.2 Autorská práva, jichž se internetová kriminalita týká

Před odpovědí na otázku, jakými způsoby lze prostřednictvím internetu porušit autorská práva, je třeba určit, co je obsahem autorských práv, tedy jaká práva (resp. tomu odpovídající povinnosti) jsou v konkrétním případě porušována.

Oblast autorských práv (soukromoprávní aspekty) je v českém právním řádě upravena v zákoně č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění (dále jen: „AutZ"). Obsah práva autorského je pak v § 10 cit. zákona definován tak, že: *Právo autorské zahrnuje výlučná práva osobnostní (§ 11) a výlučná práva majetková (§ 12 a násl.).* Mezi osobnostní práva dle § 11 AutZ patří:

1. rozhodování o zveřejnění svého díla

2. právo osobovat si autorství, včetně rozhodování o uvedení autorova jména při zveřejnění díla a dalším jeho užití.

3. právo autora na nedotknutelnost svého díla

Tato práva zanikají se smrtí autora (§ 11 odst. 4 AutZ) kromě práva osobovat si autorství k dílu a povinnosti užití díla 3. osobami jen způsobem nesnižujícím hodnotu díla.

Mezi majetková práva autora náleží právo dílo užít a tzv. jiná majetková práva (§§ 24, 25 AutZ). Právem dílo užít se rozumí (§ 12 odst. 4 AutZ):

a) právo na rozmnožování díla (§ 13),

b) právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14),

c) právo na pronájem originálu nebo rozmnoženiny díla (§ 15),

d) právo na půjčování originálu nebo rozmnoženiny díla (§ 16)

e) právo na vystavování originálu nebo rozmnoženiny díla (§ 17),

f) právo na sdělování díla veřejnosti (§ 18), zejména

1. právo na provozování díla živě nebo ze záznamu a právo na přenos provozování díla (§ 19 a 20),

2. právo na vysílání díla rozhlasem či televizí (§ 21),

3. právo na přenos rozhlasového či televizního vysílání díla (§ 22),

4. právo na provozování rozhlasového či televizního vysílání díla (§ 23).

Tento výčet však není uzavřený (taxativní), § 12 odst. 5 stanoví, že dílo lze užít i jiným způsobem než je uveden v odst. 4 cit. ustanovení.

Jiným majetkovým právem je dle § 24 a § 25 právo na odměnu při opětném prodeji originálu díla uměleckého a na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu.

Autorské dílo je definováno v § 2 odst. 1, 2 AutZ, autor této práce v podrobnostech na tato ustanovení odkazuje.

Z výše uvedených práv je pro prostředí internetu charakteristické zejména porušování práva na rozhodování o zveřejnění díla (§ 11 odst. 1 AutZ), právo na rozmnožování díla (§ 13 AutZ) a právo na sdělování díla veřejnosti (§ 18 a násl. AutZ). Zvláštní porušení autorských práv pak přistupuje v § 43 odst. 1,2 AutZ, a to konkrétně tím, že delikvent obchází účinné technické prostředky ochrany autorských práv a také výrobou, dovozem, přijímáním, rozšiřováním, prodejem, pronajímáním, propagací pronájmu či prodeje nebo držením k obchodnímu účelu zařízení, výrobky, nebo součástky nebo poskytováním služeb, které jsou k takovémuto obcházení určeny, vyráběny, upravovány, prováděny, nabízeny, propagovány či uváděny na trh, popřípadě mají kromě tohoto obcházení jen omezený obchodně významný účel nebo jiné užití. § 44 následně stanoví (zjednodušeně řečeno), že porušením autorského práva jsou i různá jednání spočívající v pomoci k porušování práva autorského tím, že bez svolení autora se odstraní jakákoliv elektronická informace o správě práv k dílu nebo že se užije dílo, ze kterého byla tato informace nedovoleně změněna či odstraněna. Zásah do autorského práva způsobí také ten, kdo použije pro své dílo názvu nebo vnější úpravy již použitých po právu jiným autorem pro dílo téhož druhu, pokud by to mohlo vyvolat nebezpečí záměny (§ 45 AutZ).

1.3 Modus operandi porušování autorských práv

1.3.1 Typy projevu porušování autorských práv na internetu

Nejčastějším způsobem, jakým bývá do výše uvedených práv zasaženo, je neautorizované zpřístupnění díla veřejnosti prostřednictvím sítě internet. K tomuto zpřístupnění může docházet zásadně dvěma základními způsoby. Prvním z nich je umístěním tohoto díla (počítačového programu, fotografie, filmu, hudby, literárního díla...) na webové stránce, odkud si jej mohou stáhnout koncoví uživatelé, druhým pak sdílením díla přímo koncovými uživateli internetu mezi sebou navzájem, a to konkrétně systémy sítí typu „peer to peer" popřípadě cestou e-mailu. K prvnímu z těchto dvou následně přistupují další 2 způsoby nepřímého porušení autorských práv zpřístupnění, tedy určitá forma účastenství (viz kapitola 1.4 Trestní odpovědnost), tj. poskytování odkazu a tzv. rámování (frames).

K odlišnému porušování autorských práv prostřednictvím internetu dochází při samotném stahování autorských děl koncovými uživateli internetu. Zde bude třeba odlišit stahování počítačových programů a elektronických databází na jedné straně a stahování ostatních děl na straně druhé. Taktéž je třeba odlišit případy, kdy se bude jednat pouze o stahování pro osobní potřebu uživatele a kdy tomu tak nebude.

Další způsob porušování autorských práv se týká účinných technických prostředků ochrany autorských práv. Jedná se konkrétně o rozšiřování, prodej a propagaci prodeje prostředků a služeb sloužící k jejich obcházení či přímo odstranění.

K poměrně častému porušování autorských práv dochází taktéž použitím názvu díla po právu již použitého jiným autorem pro dílo stejného druhu, které může vyvolat nebezpečí záměny, například pojmenování svých webových stránek názvem užitým již dříve jiným pro webové stránky s podobnou tématikou. Tato problematika (mimochodem úzce související s tzv. ochranou doménových jmen a zásahem do práv k ochranné známce) se však, ač se často na internetu vyskytuje, neliší příliš od porušování autorských práv mimo prostředí internet, a tak se už v dalších částech práce, zejména z kapacitních důvodů, nebude probírat.

1.3.2 Porušení práv prostřednictvím zpřístupnění v internetové síti

1.3.2.1 Porušení práv umístěním díla na webových stránkách

Delikvent v tomto případě zasáhne do práv autora tím, že cizí dílo (vyjma volného díla[34]), na které se vztahují autorská práva, bez licence či souhlasu autora uloží na server, který je přístupný přes webové stránky. Odtud pak může být stažen větším či menším okruhem uživatelů webu. Dochází tak k neoprávněnému užití díla formou sdělování díla veřejnosti dle § 18 odst. 1, 2 AutZ, neboť podle odst. 2 cit. ust. je sdělováním díla veřejnosti i *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.* Užití díla je výhradním majetkovým právem autora, a tak je výše uvedeným jednáním způsoben zásah do autorských práv.

Společensky nebezpečnější je výše uvedené jednání, pokud dílo nebylo dosud zveřejněno. Podle § 4 AutZ je dílo zveřejněno *prvním oprávněným veřejným přednesením, provedením, předvedením, vystavením, vydáním či jiným zpřístupněním veřejnosti.* Jelikož je právo rozhodnout o zveřejnění díla výlučným osobnostním právem autora (§ 11 odst. 1 AutZ), dochází tak nejen k porušení autorových majetkových práv, a tedy k materiální újmě, ale i k zásahu do práv osobnostních a tím i k často nenapravitelné újmě morální. O tomto závažnějším porušování autorských práv můžeme poslední dobou slýchat zejména v souvislosti s nejnovějšími filmy, kdy jsou tyto poskytnuty ke stažení dokonce několik týdnů před samotným uvedením filmu do kin, a to i přesto, že má film premiéru v jeden den po celém světě.

1.3.2.2 Porušení práv sdílením díla v systémech typu „peer to peer"

Sdílení díla v peer to peer[35] sítích se stalo v posledních letech velice aktuálním problémem, když s postupným tlakem ze strany autorit a zábavního průmyslu na provozovatele

---

[34] Volné dílo je dle § 28 odst. 1 AutZ takové dílo, u kterého uplynula doba trvání majetkových práv. Toto dílo může každý volně užít.

[35] Slovo „Peer" je přejato z anglického jazyka a znamená „rovný". Systém „peer to peer" tedy doslovně znamená rovný s rovným". Často se pro toto označení používá zkratka „P2P"

centrálních serverů s obsahem porušující autorská práva a následným jejich zrušením nebo přesunutím do zemí s nízkou ochranou autorských práv (viz 1.1), avšak s neutuchající poptávkou po získání děl zdarma či za minimální cenu bez ohledu na dodržování autorských práv, došlo k přesunu těchto „zájemců" k technologii peer to peer, kde dochází k neustálému masivnímu porušování autorských práv.

Zjednodušeně je peer to peer technologie decentralizovaná síť mnoha koncových uživatelů, kteří už nevystupují v postavení pouhých příjemců dat, ale data sami poskytují, i když často na omezenou dobu a v omezeném množství. V těchto sítích tak často ztrácí význam centrální server, ke kterému se připojují uživatelé a z kterého jsou pak stahována data. Jeho místo je nahrazeno větším či menším počtem (liší se v závislosti na typu a zaměření sítě od několika až po miliony) jedinců, kteří na svých osobních počítačích tzv. nasdílí[36] určitý objem dat a kteří se tak sami dostávají do postavení serverů. Je zřejmé, že obsahem výměny v sítích peer to peer nebudou pouze autorsky nechráněná data a soubory, ale naopak často nejnovější filmy, hudba, software či literatura. Majetkové škody tak v souhrnu dosahují astronomických částek.

Z právního hlediska však není rozdíl mezi tím, kdo poruší autorská práva neoprávněným umístěním díla na webových stránkách, a tím, kdo je, taktéž neoprávněně, sdílí v peer to peer sítích. Zásah do autorských práv je v obou případech stejný a postihuje stejná práva, rozdíl je pouze v tom, že u peer to peer sítí se odpovědnost „rozmělní" na obrovské množství jednotlivců, kteří ve větší či menší míře autorská práva porušují.

Peer to peer sítě mohou mít nejrůznější podobu, lišící se zejména v míře decentralizace a způsobu sdílení. První a asi obecně nejznámější byl Napster, jenž byl založen v červnu 1999 Shawnem Fanningem. Tato síť nebyla zcela čistou peer-to-peer sítí vzhledem k existenci centrálního serveru, který udržoval databázi uživatelů a jimi sdílených souborů. Uživatelé se tedy po spuštění programu přihlásili k tomuto serveru, který obdržel informace o sdílených souborech. Případný dotaz na vyhledávání pak šel také přímo k tomuto centrálnímu serveru a jako odpověď program obdržel adresy uživatelů, kteří sdíleli požadovaná data. Systém tedy umožňoval poměrně snadné a rychlé vyhledávání dat, která si pak již uživatelé nahrávali přímo mezi sebou navzájem. V únoru roku 2001 počet uživatelů této sítě činil více než 25 miliónů[37].

Centrální server však byl i největší slabinou tohoto systému, když 12. června 2000 podala RIAA[38] na Napster žalobu o náhradu škody. Soud Napster shledal spoluodpovědným (contributory copyright liability) a tzv. zástupně odpovědným (vicarious copyright liability)[39] z porušování autorského práva uživateli systému (80 % všech děl přístupných v této síti bylo

---

[36] tj. zpřístupní určitý objem dat pro ostatní uživatele sítě ke stažení

[37] Wikipedia; http://en.wikipedia.org/wiki/Image:Napster_Unique_Users.svg; zobrazeno 13.7.2008, 22:18

[38] Recording Industry Association of America

[39] Blíže k pojmům spoluodpovědnosti a zástupné odpovědnosti viz Čermák J.: Internet a autorské právo. 2. aktualizované a rozšířené vydání. Linde Praha, a.s., Praha 2003; s. 104 a násl.

chráněno určitým způsobem autorskými právy a 70 % všech děl byly zvukové záznamy vytvořené členy RIAA) a dne 5. března 2001 byl vynesen soudní příkaz, kterým bylo Napsteru uloženo zabránit sdílení hudby chráněné autorskými právy v jeho síti a v červenci téhož roku Napster zastavil zcela provoz své sítě. V roce 2002 po vleklých problémech vstoupil Napster do konkurzu a jeho pozice získaly nové systémy peer to peer.

Nástupci Napsteru již představují decentralizované formy peer to peer sítí bez centrálního indexu, mezi koncovými uživateli tak dochází i k vyhledávání souborů, nejen k jejich stahování. Ke stažení hledaného souboru pak postačí příslušný software a znalost nejméně jednoho dalšího uživatele, který, v případě že hledaný soubor nesdílí, řetězově umožní vyhledání u dalších uživatelů, které má na seznamu. Toto vysvětlení funkce decentralizovaných systémů je však velice zjednodušené a u různých protokolů (software s protokolem pracující) se může značně lišit. Typickým případem je rozdílnost systémů Direct Connect (DC++) a systému pracující s tzv. torrenty (Bittorrent)[40]. Jako další příklady těchto decentralizovaných sítí lze uvést Grokster, Morpheus a Kazaa.

Speciálním typem peer to peer sítí je systém sdílení dat s distribuovaným anonymním ukládáním. U tohoto systému uživatel vyčlení na pevném disku svého počítače volnou kapacitu, která slouží jako sdílený prostor pro soubory distribuované v síti. Dílo, které je pak do sítě poskytnuto, je zašifrováno a uloženo dočasně na počítači jednoho z uživatelů sítě. Soubory poskytnuté do sítě v ní kolují a ty málo používané jsou postupem času přemazávány soubory novými. Zájemce o soubor pouze vyhledá soubor pod známým jménem a stáhne na svůj počítač. Původní poskytoval tak ztrácí zcela kontrolu nad jím poskytnutým souborem a lze ho i velice obtížně vystopovat. Typickým představitelem tohoto systému je projekt Freenet[41].

1.3.2.3 Poskytování odkazu

Poskytování odkazu je určitou formou účasti na porušování práv způsobené neoprávněným umístěním díla na webových stránkách. Při tomto jednání sice nedojde k přímému porušení autorských práv (s výhradou tzv. inliningu, viz níže), neboť poskytování odkazu (link) na neoprávněně zpřístupněná díla sice přímo neporušuje autorská práva, ale porušování značně napomáhá, popřípadě dokonce k němu navádí.

K poskytování odkazu na neoprávněně umístěná díla dochází nejčastěji na serverech věnovaných stahování hudby. Jelikož je přímé neoprávněné poskytnutí díla na serveru ve většině zemí s vyšší právní kulturou postihováno, byly servery s tímto obsahem přesunuty do zemí s nízkou ochranou autorských práv (viz výše). Aby uživatel tyto servery našel, vznikly webové stránky provozované obvykle v lokálních jazycích, kde jsou katalogy nejrůznějších

---

[40] podrobné vysvětlení rozdílů těchto a dalších systému přesahuje rámec této publikace, bližší informace např.:

Wikipedia; http://en.wikipedia.org/wiki/.torrent; zobrazeno 13.7.2008, 22:30

Wikipedia; http://en.wikipedia.org/wiki/Direct_Connect_(file_sharing); zobrazeno 13.7.2008, 22:35

[41] Wikipedia; http://en.wikipedia.org/wiki/Freenet#Current_development; zobrazeno 13.7.2008, 22:50

děl spolu s uvedeným odkazem na server, z něhož lze dílo stáhnout. Že tyto stránky, ač často nazvané „mp3 zdarma", „mp3 for free" či „hudba gratis", nejsou úplně nezištné, dokládá obrovské množství reklam na těchto stránkách se vyskytujících. I když autoři těchto webových stránek na nich často prohlašují, že neodpovídají za porušení autorských práv, protože autorská díla nejsou na jejich serverech uložena a oni sami nemohou ovlivnit obsah serverů, na kterých jsou odkazovaná díla uložena, jedná se o prohlášení pouze účelové, které není a ani nemůže být právně relevantní. Tyto stránky jsou takřka vždy vytvořeny za účelem zisku z reklam na nich umístěných a jejich tvůrci jsou vždy minimálně srozuměni, že odkazy na jejich stránkách přímo vedou k neoprávněně poskytovaným autorským dílům[42].

Od pouhého poskytování odkazu je třeba odlišit využívání odkazu (inlining). V tomto případě totiž není na volbě koncového uživatele, zda poskytnutý odkaz (link) použije či nikoliv, ale uživateli se přímo zobrazí odkazovaný dokument, aniž by ho sám aktivoval. Dle mého názoru tak při aktivaci na uživatelově obrazovce vznikne složené dílo (dílo, které leží na serveru, na který je odkazováno a dílo webové stránky (pozadí), ve kterém se odkazovaný dokument zobrazí. Protože je autorskoprávní ochrana poskytována i dílům dočasným (§ 2 odst. 1 AutZ, dochází při každém užití (sdělování díla veřejnosti) bez souhlasu autora odkazovaného díla k porušování autorských práv (§ 2 in fine § 18 odst. 1,2 AutZ)[43].

Využívání Inliningu se velice podobá rámování (frames). Podstatou této technologie je rozdělení webové stránky do několika částí, ve kterých se může zobrazovat různý obsah a které jsou vlastně samostatnými webovými stránkami. V jedné části tak například může být umístěna navigace (seznam odkazů) a v jiné otevřený obsah dokumentu (typicky dílo umístěné na jiném serveru), který byl vybrán pomocí navigace v první části. Ve své podstatě tak zobrazením na obrazovce uživatele vznikne složené dílo, stejně jako je tomu tak v případě inliningu. Zodpovězení otázky porušování autorských v případě rámování je proto stejné jako u inliningu a v tomto ohledu lze tedy odkázat na předchozí odstavec.

1.3.3 Porušení práv v případě stažení díla koncovými uživateli.

1.3.3.1 Stahování počítačových programů a elektronických databází[44]

Obecně platí, že stažení programu je užitím díla dle AutZ, a to konkrétně jeho rozmnožováním (§ 13 odst. 1, 2 AutZ). Aktem stažení se totiž dílo „nepřesune" ke

---

[42] úsměvným působí prohlášení uvedené například na serveru „mp3 zadarmo CZ" (http://www.mp3zadarmo.cz/stahuj): *„Mp3, které si zde můžete stáhnout, nejsou uloženy na serveru mp3 zadarmo cz => neodpovídáme za kvalitu ani za autorská práva. MP3 jsou uloženy na webech se kterými nemá server mp3 zadarmo cz nic společného.*
Tato hudební nahrávky jsou zpravidla z ruských serverů, které platí autorské poplatky." Je totiž všeobecně známo, že poplatky, které jsou vybírány a které odvádí oprávněným ruští kolektivní správci autorských práv, jsou zlomkové hodnoty oproti poplatkům vybíraných v zemích poskytujících těmto právům plnou ochranu.

[43] V některých publikacích je vyjádřen opačný názor (Čermák J.: Internet a autorské právo. 2. aktualizované a rozšířené vydání. Linde Praha, a.s., Praha 2003, s. 72 a násl., v této publikaci se však vychází z dnes neplatné premisy, že výčet způsobu užití díla uvedený v § 12 odst. 4 je taxativní).

[44] Dále v této souvislosti jen „počítačové programy" či „programy"

koncovému uživateli, ale zůstává na původním serveru a uživateli vznikne na jeho počítači pouze kopie. V této souvislosti je třeba poznamenat, že obecně nedochází k porušení autorských práv, když vznikne v operační paměti koncového uživatele pouze dočasná, tzv. technická kopie, např. při navštěvování webových stránek (§ 38a odst. 1 písm. a, b AutZ)[45]. Proto je v dalším textu rozvedeno pouze cílené stahování koncových uživatelů do „pevné" paměti počítače. Takovéto stažení počítačového programu koncovým uživatelem, pokud k němu nebyl dán souhlas autora či svolení nevyplývá z platně uzavřené licenční smlouvy, znamená, mimo výjimky uvedené v AutZ, porušení autorských práv. Stahování počítačových programů totiž dle (§ 30 odst. 3 AutZ) nespadá pod tzv. volná užití uvedená v § 30 odst. 1, 2 AutZ (viz níže).

1.3.3.2 Nemožnost aplikace institutu vyčerpání práva (first sale doctrine)

Porušovat autorská práva může i ten, kdo si hudbu stáhl legálně (například z internetového obchodu s hudbou) a dále ji šíří (pošle kamarádovi v e-mailu nebo ji někomu prodá), a to proto, že u děl legálně stažených z internetu se neuplatní pravidlo o vyčerpání autorských práv k dílu jeho prvním převodem (§ 14 odst. 2). Je to jednak z toho důvodu, že se poskytnutím jinému nepřevede vlastnické právo k rozmnoženině díla (vytvoří se jeho kopie), a jednak proto, že se toto pravidlo uplatňuje pouze na rozmnoženiny vyjádřené v podobě hmotného předmětu. Jedná se tak vlastně o akt rozmnožení, které pravidlo o vyčerpání práva nezahrnuje.

1.3.3.3 Stahování děl „nikoliv pro vlastní potřebu"

Jak je již uvedeno výše (1.3.3.1), znamená každé stažení užití díla (§ 13 odst. 1, 2). To ovšem neznamená, že by každé toto jednání, pokud by nebylo učiněno se souhlasem autora, znamenalo porušení autorských práv, a to proto, že autorský zákon obsahuje k § 13 speciální ustanovení v § 30 (odst. 1, 2, 3) týkající se tzv. volných užití:

§ 30

Volná užití

(1) Za užití díla podle tohoto zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.

(2) Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.

(3) Nestanoví-li tento zákon dále jinak, užitím podle tohoto zákona je užití počítačového programu či elektronické databáze i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu; stejně je užitím podle tohoto zákona zhotovení

---

[45] Podrobněji k problematice technických kopií viz Čermák J.: Internet a autorské právo. 2. aktualizované a rozšířené vydání. Linde Praha, a.s., Praha 2003, s. 49 a násl., vlivem změny úpravy vyvolané provedením tzv. Informační směrnice (2001/29/ES) však neodpovídají odkazy na příslušná ustanovení AutZ dnes platné právní úpravě

rozmnoženiny či napodobeniny díla architektonického stavbou i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby (§ 30a) a pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu (§ 20) i pro osobní potřebu fyzické osoby.

V praxi to znamená, že pokud je dílo (vyjma výjimky dle § 30 odst. 3 AutZ) staženo pro osobní potřebu uživatele a nemá za cíl hospodářský či finanční prospěch, nejedná se o zásah do autorských práv. Důležité je proto stanovit rozsah pojmu „pro osobní potřebu". Předně je třeba zmínit, že vlivem harmonizace práva ČR s právem EU[46] bylo přímo do znění zákona vloženo, že se musí jednat o osobní potřebu fyzické osoby. Starší úprava toto zpřesnění neobsahovala a pojem „osobní potřeba" a jurisprudence někdy rozšiřovala tento pojem i na „vnitřní potřebu právnické osoby".[47]

Obsah pojmu „osobní potřeba" lze shrnout následovně:

1. Jde o potřebu koncového uživatele internetu, nikoliv pro potřebu 3. osoby.
2. Jedná se pouze o jednu rozmnoženinu (kopii).
3. Nejedná se o komerční účel.
4. Staženým dílem není počítačový program ani elektronická databáze
5. Stažení díla nesmí být na újmu oprávněným zájmům autora

(6.) Dle čl. 5 odst. 2 písm. b) Informační směrnice musí nositelé práv z tohoto zákonného omezení získat spravedlivou odměnu[48].

Jakékoliv jiné neoprávněné stažení díla, než které splňuje uvedené podmínky, je porušením autorského práva (samozřejmě s větší či menší intenzitou).

1.3.4 Porušování autorských práv týkající se účinných technických prostředků ochrany.

Jelikož s rozvojem internetu dochází čím dál většímu rozmachu neautorizovaného užívání děl, přistoupili autoři, zejména ale nahrávací společnosti, k využívání určitých technických prostředků, jejichž účelem je znemožnění (nebo alespoň znesnadnění) nedovoleného užití autorských děl).

Reakce na tyto prostředky nenechala na sebe dlouho čekat a záhy byly zveřejněny způsoby, jak technické prostředky ochrany autorských práv překonávat. Nutno podotknout, že časem se z tohoto překonávání ochrany stal v komunitě hackerů jakýsi sport, v němž se účastníci předhánějí, kdo tu či onu ochranu prolomí (v případě softwarových prostředků) či najde způsob jejího překonání (hardwarové prostředky ochrany). Dnes často dochází k prolomení protikopírovací ochrany již za několik měsíců, viz příloha č. 1.

Jak vznik protikopírovací ochrany a jiných účinných technických prostředků ochrany práv autoru, tak jejich překonávání mělo záhy odraz v platné právní úpravě. V českém právním

---

[46] čl. 5 odst. 2 písm. b) Informační směrnice (2001/29/ES)

[47] např. Telec, I.: Autorský zákon. Komentář. 1. vydání, C. H. Beck, Praha 1997

[48] v ČR provedeno ust. § 25 AutZ

řádu tak bylo učiněno v §§ 43, 44, 45 AutZ. V těchto ustanoveních jsou účinné technické prostředky definovány, jsou dány meze jejich užití a následně stanovena jednání týkající se překonávání těchto prostředků, která jsou považována za zásah do autorských práv.

V konkrétních případech má toto jednání formu nabízení odstranění ochrany na webových stránkách, dále zpřístupnění, sdílení a zasílání souborů, které má za úkol technickou ochranu obejít či přímo neautorizované poskytnutí díla veřejnosti s připojeným programem, který umožní technickou ochranu překonat (generátory kódů a tzv. cracky).

Ne všechny účinné technické prostředky jsou však legální, jejich užití podléhá určitému omezení. Zoufalá situace některých nahrávacích koncernů je však často nutí uchýlit se až k drastickým prostředkům, jejichž použití je taktéž protiprávní a často se jedná o trestnou činnost. Asi nejdále v tomto ohledu zašla společnost Sony BMG. Ta vybavovala svá zvuková CD protikopírovací ochranou XCP-Aurora od společnosti First 4 Internet, která se však do počítače kupujícího sama nainstaluje jako rootkit.[49] To ve stručnosti znamená, že ochrana je uložena hluboko v operačním systému uživatele, aniž ten by o této skutečnosti věděl, zůstává neustále aktivní, komunikuje s internetem a je velice obtížně zjistitelná běžným antivirovým programem. Navíc tato „ochrana" zpočátku obsahovala bezpečnostní chybu, kterou mohli hackeři využít (a také tak činili) k neoprávněným přístupům k informacím uložených u nic netušících koncových uživatelů. Tato ochrana nejen zabraňuje kopírování CD, ale i vypalování zvukových CD obecně, ať už by měl být jejich obsah jakýkoliv! Poté, co se tato aféra „provalila" na veřejnost, musela společnost Sony BMG nést důsledky. Na základě soudního vypořádání zaplatila společnost 750.000,- USD peněžitou pokutu a každému poškozenému zákazníkovi 175 USD.[50]

1.4 Trestní odpovědnost

1.4.1 Úvod

V předchozích částech této kapitoly věnované fenoménu porušování autorských práv bylo pojednáno zejména o skutečnostech, co je dle práva zásahem do autorských práv, jak k tomuto porušování dochází a v jakých modalitách se nejčastěji projevuje. Tato část nazvaná Trestní odpovědnost naopak popisuje, kdy výše uvedená jednání jsou postižitelná z hlediska trestní odpovědnosti.

1.4.2 Nebezpečnost činu pro společnost

O materiální stránce TČ, tedy o určení nebezpečnosti činu pro společnost, lze u porušování autorských práv obecně odkázat na společný výklad ke všem druhům internetové kriminality v I. (Obecné) části této práce. Proto zde jen krátce ke specifickým rysům společenské nebezpečnosti porušování autorských práv.

---

[49] více k tomuto v hlavě 2 Hackerství

[50] podrobně k tomuto viz např. časopis CHIP.CZ, č.2/2006, str. 16

Při zkoumání společenské nebezpečnosti v případě porušování autorských práv, je vždy nutné si uvědomit, jaká konkrétní práva mohla být jednáním pachatele zasažena. V případě zásahu nejen do výhradních majetkových práv autora, ale i do práv výlučně osobnostních je totiž vždy nutné považovat toto jednání za společensky nebezpečnější. Majetková škoda totiž prakticky vždy může být nahrazena, v případě morální a jiné psychické újmy tomu tak být nemusí.

Dalším hlediskem společenské nebezpečnosti pachatelova jednání jsou i okolnosti, za kterých byl čin spáchán, zejména prevalence podobných typů jednání v daném místě a čase. U porušování autorských práv nabývá tento aspekt nebezpečnosti činu pro společnost zvláštní důležitosti, neboť se stoupajícím rozmachem neoprávněných zásahů do autorských práv (peer to peer sítě, poskytování hudby a filmů...), roste i společenská potřeba reakce v podobě trestní represe.

Co se týká naplnění materiální stránky trestného činu u tohoto typu internetové kriminality ve vztahu k pohnutce pachatelova jednání, bude obecně posuzováno jako společensky nebezpečnější jednání, které sledovalo určitý hospodářský nebo podnikatelský účel, tedy zda pachatel jednal, aby dosáhl zisku. Proto bude jistě pro společnost škodlivější neoprávněné poskytování děl „zdarma" na serverech, a to za účelem odměn z reklam tam taktéž umístěných, než zaslání jedné skladby kamarádovi prostřednictvím e-mailu.

1.4.3 Formální stránka trestného činu

1.4.3.1 Obecné znaky trestného činu

Jak je uvedeno výše, jsou obecnými znaky trestného činu věk (dosažení patnácti let) a příčetnost (schopnost rozpoznávací a schopnost ovládací). V tomto ohledu není pro internetové porušování autorských práv žádné specifikum, a proto autor odkazuje v podrobnostech na obecné výklady teorie trestního práva[51]

1.4.3.2 Skutková podstata trestného činu § 152 tr.zák.

K určení trestní odpovědnosti pachatele je nutné subsumovat jednání, jakým lze způsobit porušování autorských práv pod konkrétní ustanovení tr.zák., které toto jednání postihuje.

V případě jednání uvedených v předchozích oddílech této kapitoly je jím zejména § 152 tr.zák. upravující skutkovou podstatu trestného činu Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi.

Tento paragraf je členěn na dva odstavce, první upravuje základní skutkovou podstatu a druhý obsahuje tzv. kvalifikovanou skutkovou podstatu (okolnost podmiňující použití vyšší trestní sazby):

§ 152

---

[51] např. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 185 a násl.

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

(1) Kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

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

b) dopustí-li se takového činu ve značném rozsahu.

Tento trestný čin je systematicky zařazen mezi trestné činy hospodářské do Hlavy druhé Zvláštní části trestního zákona, konkrétněji do Oddílu čtvrtého – Trestné činy 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.

1.4.3.2.1 Základní skutková podstata TČ podle § 152 tr.zák.

Ze znění § 152 odst. 1 tr.zák. vyplývá, že zákonodárce se v případě tohoto trestného činu (podobně jako většina trestných činů upravených v tomto oddíle trestního zákona) rozhodl využít úpravy formou blanketní normy. Blanketní norma trestního práva je taková norma, která sama pravidlo chování přímo neobsahuje, ale ve své dispozici odkazuje obecně na normu či více norem stejného druhu, v tomto případě na právní odvětví práva autorského. Mezi základní prameny autorského práva patří na mezinárodní úrovni Smlouva Světové organizace duševního vlastnictví o právu autorském sjednaná dne 20.12.1996 v Ženevě a vyhlášená pod číslem 33/2002 Sb. m. s., Smlouva Světové organizace duševního vlastnictví o výkonech výkonných umělců a o zvukových záznamech sjednaná dne 20. 12. 1996 v Ženevě a vyhlášená pod číslem 48/2002 Sb. m. s., Bernská úmluva o ochraně děl literárních a uměleckých z roku 1886 a vyhlášená pod čísly 133/1980 Sb. a 19/1985 Sb. a dále Všeobecná úmluva o autorském právu sjednaná v roce 1952 v Ženevě a vyhlášená pod čísly 2/1960 Sb. a 134/1980 Sb.

V komunitárním právu je z hlediska pramenů autorského práva podstatná zejména Informační směrnice (2001/29/ES), Směrnice 91/250/EHS o právní ochraně počítačových programů, 96/9/ES o právní ochraně databází a Směrnice 2000/31/ES o elektronickém obchodu.

Na vnitrostátní úrovni je tímto pramenem autorského práva autorský zákon (viz výše).

Objektem tohoto trestného činu je ochrana autorského práva, práv souvisejících s právem autorským a práv k databázi[52]. Vzhledem k tomu, že ochrana těchto zájmů je primárně zajištěna normami soukromého práva (AutZ, občanský zákoník, obchodní zákoník), je vždy

---

[52] tamtéž, str. 507

nutné z hlediska pomocné role trestní represe (ultima ratio) vždy pečlivě uvážit naplnění materiální stránky trestného činu (společenské nebezpečnosti) a zhodnotit, zda k účinné ochraně práv nepostačuje využití institutů soukromoprávní odpovědnosti či prostředků správního trestání, a to zejména v těch případech, kdy půjde pouze o nezištné jednání koncových uživatelů (viz např. rozsudek Nejvyššího soudu ČR sp. zn.: (Rt) 5 Tz 75/2001).

Objektivní stránku tohoto trestného činu spáchaného prostřednictvím internetu tvoří ta jednání uvedená v kapitole 1.3 této hlavy Zvláštní části, která vedou, popř. mohou vést, (v rámci kauzálního nexu) k zásahu do autorských práv (následku).

Pachatelem může být jakákoliv fyzická osoba, bez ohledu na její zvláštní vlastnosti, postavení či způsobilost. Obvykle jím nebývají z důvodů již výše nastíněných osoby vyššího věku, naopak je incidence tohoto trestného činu rozšířená u mladší věkové kategorie.

V rámci subjektivní stránky trestného činu vyžaduje trestní zákon u tohoto trestného činu zavinění ve formě úmyslu, postačuje i úmysl nepřímý, eventuální (§ 3 odst. 4 in fine § 152 odst. 1, arg. a contrario).

Jedním z dalších důsledků blanketní dispozice § 152 odst. 1 je i ten, že norma soukromoprávní (autorského práva) je vlastně „vtažena" mezi normy trestněprávní, což má za následek z hlediska zavinění, že neznalost předpisů autorského práva bude posuzována stejně jako neznalost normy trestní, v rámci právního omylu, a tedy na rozdíl od omylu skutkového nebude zbavovat pachatele odpovědnosti za úmyslný trestný čin (ignoratia legis non excusat[53]).

Právem autorským nejsou obecně dotčena práva s autorským právem související, jejich ochrana se uplatňuje vedle sebe a jedním skutkem tak pachatel může porušovat práva jak autorů, tak výkonných umělců, výrobců zvukových a audiovizuálních záznamů i televizních vysílatelů[54]. Jelikož teorie ani praxe obecně neuznává jednočinný souběh stejnorodý, půjde tak o trestný čin jediný, jeho společenská nebezpečnost však bude pochopitelně vyšší.

1.4.3.2.2 Kvalifikovaná skutková podstata TČ podle § 152 tr.zák.

Kvalifikovaná skutková podstata vyjádřená v odst. 2 § 152 tr.zák. obsahuje dvě okolnosti podmiňující použití vyšší trestní sazby. První je získání tímto trestným činem značného prospěchu (§ 152 odst. 2 písm. a) tr.zák.), druhá pak páchání této trestné činnosti ve značném rozsahu (§ 152 odst. 2 písm. b) tr.zák.). Při naplnění této skutkové podstaty pachateli hrozí trest odnětí svobody v délce trvání 6 měsíců až 5 let.

Pro určení výše prospěchu se dle výkladového ustanovení § 89 odst. 11 věta 2 užije obdobně ustanovení téhož odstavce (věta 1) týkající se výše škod. Z toho důvodu se získáním značného prospěchu rozumí zisku částky nejméně 500.000,- Kč. Složitější je však výklad pojmu „značný rozsah", neboť tento pojem tr.zák. nevykládá a nelze bez dalšího říci,

---

[53] Neznalost zákona neomlouvá

[54] např. neoprávněné vysílání záznamu koncertů popové zpěvačky

že se analogicky užijí hodnoty pro výši škody (už jen proto, že v trestním právu hmotném je analogie in malam partem[55] nepřípustná). V případech, kdy lze tyto pojmy vyjádřit v penězích a kdy do hry nevstupují další podstatné okolnosti, však praxe při vymezení těchto pojmů pro konkrétní případ používá obdobně kritérií uvedených v § 89 odst. 11 tr.zák.[56]

V případě porušování autorských práv v síti internet ovšem často nastává základní problém aplikace těchto okolností podmiňujících použití vyšší trestní sazby, a to že vzniklý prospěch či rozsah zásahu do autorských práv nelze vždy reálně určit. To platí zejména pokud pachatelův primární motiv nebylo získání peněžního prospěchu (typicky peer to peer sítě). Nelze totiž říci, že „značný rozsah" je určen zejména částkou, kterou by oprávnění z autorských práv obdrželi při legálním užití těchto děl (např. při prodeji hudebních CD), jak se snaží tvrdit zejména nahrávací společnosti a kolektivní správci autorských práv. Je totiž velice pravděpodobné, že by uživatelé díla v případě nemožnosti této nelegální cesty vůbec dílo neužili. Praxe se proto uchyluje často k tomu, že otázku určení prospěchu či rozsahu ponechávají nevyřešenou (mimo rozhodování o dosaženém stupni společenské nebezpečnosti) a kvalifikují jednání pachatele pouze podle základní skutkové podstaty[57]. Některé nejnovější rozsudky však již vyčíslení škody obsahují.[58]

1.4.3.3 Zvláštní případ účastenství[59] na TČ podle § 152 tr.zák. spáchaného v souvislosti s internetem

Účastníkem na dokonaném trestném činu nebo jeho pokusu je podle § 10 odst. 1 písm. a), b), c) tr.zák. ten, kdo úmyslně:

> *a) spáchání trestného činu zosnoval nebo řídil (organizátor),*
> *b) navedl jiného k spáchání trestného činu (návodce),*
> *c) poskytl jinému pomoc k spáchání trestného činu, zejména opatřením prostředků, odstraněním překážek, radou, utvrzováním v předsevzetí, slibem přispět po trestném činu (pomocník).*

Česká právní úprava účastenství tak spočívá na zásadě tzv. akcesority účastenství, a to v tom smyslu, že účastenství podle § 10 tr.zák. bude trestné pouze v takovém případě, kdy hlavní pachatel čin dokonal nebo se o něj alespoň pokusil.

V prostředí internetu se setkáváme s určitou specifickou formou účastenství, kterou je poskytování odkazů. Pro přehlednost zopakuji, že poskytování odkazu na neoprávněně

---

[55] v neprospěch pachatele

[56] Novotný, O., Dolenský, A., Jelínek, J., Vanduchová, M.: Trestní právo hmotné. I. Obecná část. 3. vydání. Codex, Praha 1997, str. 90

[57] viz rozhodnutí ve věci „obalycd.cz" – příloha č. 2

[58] např. rozhodnutí v případu „Rafťáci", zde byl pachatel odsouzen k trestu odnětí svobody na tři měsíce s podmíněným odkladem na jeden rok, k trestu propadnutí věci - počítače a pirátské nahrávky, a k náhradě škody téměř čtvrt milionu korun.

[59] zde v tzv. užším smyslu účastenství

zpřístupněná díla spočívá obvykle v jednání, kdy je koncovému uživateli „přiblížen a zjednodušen" přístup k neoprávněně rozšiřovanému dílu poskytnutím odkazu, který koncového uživatele dovede přímo na místo uložení tohoto díla. Poskytování odkazu neznamená až na výjimky zásah do autorských práv. Z výše uvedeného však plyne, že poskytovatel odkazu může být za určitých okolností postižen jako účastník ve formě pomocníka (v extrémních případech i návodce[60]) na trestném činu podle § 152 tr.zák. (§ 10 odst. 1 písm. c), event. b), § 152 tr.zák).

K trestnosti poskytování odkazu podle ustanovení o účastenství bude potřeba splnění těchto podmínek:

1) Došlo k dokonání trestného činu nebo jeho pokusu – tato podmínka bude takřka vždy splněna, protože těžko bude někdo poskytovat odkaz na server, kde dílo nebylo doposud zveřejněno. Jediný případ nenaplnění této podmínky bude v případě, že na serveru, na který je odkazováno, nebylo nakonec dílo uloženo, popřípadě bylo z něj odstraněno před momentem poskytnutí odkazu.

2.) Úmysl účastníka zahrnující jednání, které účastenství charakterizuje, tedy v tomto případě úmysl poskytnout jinému pomoc k spáchání trestného činu. Stejně jako u hlavního pachatele bude postačovat i úmysl nepřímý. Úmyslné zavinění bude často odvozováno od konkrétních okolností. Tak například (a poněkud paradoxně) pokud pomocník na svém webu s databází velkého množství odkazů na neoprávněně poskytnutá díla umístí taktéž prohlášení, že neodpovídá za obsah serverů (a tedy i za porušování autorských práv), na které je odkazováno, a zároveň se jedná o nejnovější hudební skladby či filmy, které nebudou jistě zpřístupněny oprávněně „zadarmo", musí být minimálně srozuměn s tím, že obsah serverů, na které poskytuje odkaz, bude často nelegální a že poskytnutím takového odkazu napomáhá hlavnímu pachateli. Důležitou okolností pro posouzení zavinění je i skutečnost, zda jsou stránky s odkazy provozovány za účelem zisku z reklamy, kdy je zřejmé, že nejvíce budou stránky navštěvovány, pokud budou obsahovat odkaz na díla, která podléhají autorskoprávní ochraně. Tito poskytovatelé tak minimálně vědí, že jejich jednání napomáhá hlavnímu pachateli k porušení či ohrožení zájmu chráněného zákonem (ochrana autorských práv) a v případě, že se tak stane, jsou s tímto následkem srozuměni, neboť z tohoto jednání sami profitují.

3.) Naplnění ostatních znaků trestného činu (materiální stránka TČ a obecné znaky formální stránky TČ.

Při splnění těchto podmínek můžeme kvalifikovat jednání poskytovatelů odkazu jako účastenství ve formě pomoci na trestném činu Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 10 odst. 1 písm. b), § 152 odst. 1 tr.zák.

---

[60] O návod by mohlo jít, pokud by poskytovatel odkazu měl na svých webových stránkách např. toto: „Chceš film Matrix zdarma, bez placení poplatků autorům či nahrávacím společnostem? Tak neváhej a klepni *sem*..." Taková situace není ale příliš pravděpodobná.

1.4.3.4 Souběh s dalšími TČ při porušování autorských práv v síti internet

Při porušování autorských práv prostřednictvím internetu může docházet i k jednočinnému souběhu s jinými trestnými činy. Tak například je možný jednočinný souběh TČ podle § 152 a TČ Neoprávněného podnikání podle § 118 tr.zák. v případě provozování výdělečných serverů s neoprávněně zpřístupněnými autorskými díly bez živnostenského oprávnění. Není vyloučen ani souběh s trestným činem Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu dle § 150 tr.zák. (např. provozování stránek nazvaných „SONY BMG free download", na kterých budou neoprávněně poskytována autorská díla), popř. s TČ Nekalé soutěže podle § 149 tr.zák. (pachatel v rámci nekalosoutěžního jednání mezi internetovými obchody taktéž neoprávněně nakládá s autorským dílem). V neposlední řadě je také možný souběh s TČ Šíření pornografie podle § 205 tr.zák. (neoprávněné zpřístupnění pornografického díla vytvořeného jinou osobou prostřednictvím internetu osobám mladších 18 let).

1.4.4 Trestní odpovědnost poskytovatelů volného prostoru a poskytovatelů připojení

1.4.4.1 Trestní odpovědnost poskytovatelů volného prostoru

Trestní odpovědnost poskytovatelů prostoru[61] je dle čl. 14 směrnice č. 2000/31/ES o elektronickém obchodu vyloučena, pokud poskytovatel neměl vědomost o obsahu porušujícím autorská práva. Přitom dle čl. 15 směrnice nemají poskytovatelé volného prostoru povinnost průběžně kontrolovat obsah uložený v jimi poskytnutém prostoru ani povinnost aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní činnost. Trestní odpovědnost těchto poskytovatelů tak bude zcela výjimečná.

1.4.4.2 Trestní odpovědnost poskytovatelů připojení

Co se týče poskytovatelů připojení, nauka i praxe (a to i zahraniční) se zde vzácně shodují, že vztah poskytovatelů připojení a porušování autorských práv těmi, kdo poskytnuté připojení využívá, je příliš vzdálený, než aby se u poskytovatelů připojení dala vyvozovat soukromoprávní odpovědnost za porušování autorských práv, a to včetně i tzv. spoluodpovědnosti[62]. Tím spíše proto nemůžeme dovodit, vzhledem k blanketnímu ustanovení § 152 tr.zák. a nutnosti naplnění materiálního znaku trestného činu, trestní odpovědnost poskytovatelů připojení.

---

[61] *Poskytovatelem volného prostoru* (hosting provider) se rozumí právnická nebo fyzická osoba, který na základě smlouvy poskytuje na Internetu datový prostor jiným subjektům a tak zpřístupňuje cizí obsah prostřednictvím počítačové sítě Internet, případně poskytuje další služby s tím spojené. (Matejka Ján, Čermák Jiří: Odpovědnost poskytovatelů volného prostoru na Internetu za cizí obsah. www.itpravo.cz, zobrazeno 19.7.2008, 13:25)

[62] Autorský zákon, podobně jako Informační směrnice, v § 18 odst. 3 stanoví, že sdělováním díla veřejnosti není pouhé provozování zařízení umožňujícího nebo zajišťujícího takové sdělování.

1.4.5 Kazuistika

České trestní soudy v minulosti již rozhodovaly několik případů porušování autorských práv na internetu. Na následujících řádcích jsou některé z rozhodnutí uvedeny v úplném znění v anonymizované podobě. Ve většině případů se však jedná o trestní příkazy, a tak není odůvodnění podrobnější.[63]

a) Rozhodnutí týkající se sdílení v peer to peer sítích:

DOŠLO 11. 04. 2007

Jednací číslo: 3 T 160/2006

Toto rozhodnutí nabylo právní moc
dne 26. 04. 2007 PRO PRAHU 10

ČESKÁ REPUBLIKA

TRESTNÍ PŘÍKAZ

Samosoudce Obvodního soudu pro Prahu 10 vydal dne 29.září 2006 podle § 314e odst.1 trestního řádu tento **t r e s t n í p ř í k a z :**

Obviněný

L R ,

nar. 1972 ve Varnsdorfu, trvale bytem Bořanovice,

j e v i n e n, ž e

v době nejméně od roku 2002 do 16.1.2006 na svém pracovišti v Praze 10 ve společnosti se na pracovním počítači jako uživatel internetové výměnné sítě vystupující pod přezdívkou LUBOSOFT připojoval k Internetu, kde v rámci výměnných sítí za použití speciálního programu DC++ sdílel a tím ostatním uživatelům těchto výměnných sítí nabízel ke stažení hudební a audiovizuální soubory, a to bez vědomí a souhlasu nositelů autorských práv, ke škodě České národní skupiny Mezinárodní federace hudebního průmyslu z celkem 717 šířených a zajištěných komerčních titulů, Ochranného svazu autorského pro práva k dílům hudebním z počtu 621 skladeb a České protipirátské unii za provedení rozmnožení filmových titulů,

t e d y : zasáhl neoprávněně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému a zvukově obrazovému záznamu a dopustil se takového činu ve značném rozsahu,

TRR082 - (Tr.ř. 82 - trestní příkaz)

[63] Zdroj: http://www.cpufilm.cz/rozsudky.html, zobrazeno 31.7.2008, 16.40

čímž spáchal

trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1, odst. 2 písm. b) trestního zákona,

a za to se odsuzuje

Podle § 152 odst. 2 tr. zákona k trestu odnětí svobody v trvání 7 měsíců.

Podle § 58 odst. 1 tr. zákona a § 59 odst. 1 tr. zákona se výkon trestu podmíněně odkládá na zkušební dobu 14 měsíců.

Podle § 229 odst. 1 tr. řádu se poškozená Česká protipirátská unie se sídlem Praha 8, Sokolovská 37/24 odkazuje s nárokem na náhradu škody na řízení ve věcech občanskoprávních.

Poučení: Proti tomuto trestnímu příkazu lze do osmi dnů od jeho doručení podat u zdejšího soudu odpor. Právo podat odpor nenáleží poškozenému. Pokud je odpor podán včas a oprávněnou osobou, trestní příkaz se ruší a ve věci bude nařízeno hlavní líčení. Při projednání věci v hlavním líčení není samosoudce vázán právní kvalifikací ani druhem a výměrou trestu obsaženými v trestním příkaze. Nebude-li odpor řádně a včas podán, trestní příkaz se stane pravomocným a vykonatelným. V případě, že obviněný odpor nepodá, vzdává se tím práva na projednání věci v hlavním líčení.

V Praze dne 29.září 2006

Mgr. Radek Mařík v.r.
samosoudce

OBVODNÍ SOUD PRO PRAHU 10

Za správnost vyhotovení:
Andrea Šléglová

TRR052 - (Tr.ř. 52 - trestní příkaz)

b) Rozhodnutí ve věci „Rafťáci" (viz výše)[64]

Spisová značka: **6 T 46/2007**

Toto rozhodnutí nabylo právní moci: 25. 4. 2007
OKRESNÍ SOUD V MOSTĚ
dne 9. května 2007

POLICIE ČR – okresní ředitelství služba kriminální policie a vyšetřování 434 75 Most
Došlo: 15. V. 2007
Č.j.
Přílohy:

ČESKÁ REPUBLIKA

TRESTNÍ PŘÍKAZ

Samosoudce Okresního soudu v Mostě vydal dne 22.3.2007 v Mostě podle § 314e odst. 1 tr. řádu následující **t r e s t n í p ř í k a z :**

Obviněný

M Z ,

nar. 1988 v Mostě, bytem trvale Most, ,

j e v i n e n , ž e

1) dne 12.3.2006 v kině Cinema City Flora v paláci Flora v Praze 3, ul. Vinohradská čp. 130, při promítání filmu „Rafťáci" pořídil kamerou bez souhlasu vlastníka práv k tomuto filmu, spol. Cinemania s.r.o. Praha 2, nelegální záznam tohoto filmu, který poté převedl ve svém počítači v místě svého trvalého bydliště v Mostě, , do souboru s názvem „Raftaci_CAM_by_b-s-h.wmv", a dne 13.3.2006 ho nabídnul ke stažení na veřejnou počítačovou síť Internet a tento soubor s výše uvedeným filmem zpřístupnil neomezenému množství dalších osob a v následujících dnech opakovaně zveřejňoval na internetu odkazy na webové stránky, z nichž bylo možno jím natočený a upravený film kopírovat,

2) v době od 12.1.2006 do 30.4.2006 měl ve svém počítači umístěném v místě svého bydliště v Mostě, , vědomě nainstalovány k užívání počítačové programy Adobe Photoshop v7.0 CE Czech, Dreamweaver 4, Dreamweaver MX, Microsoft Office Professional Edition 2003, Microsoft Windows XP Professional, Norton Internet Security 2005, Auto CAD 2006 Z.54.10, Avast! Antivirus Professional v.4.6, Borland C++ Application Frameworks 3.1, MOBILedit! 2.00, Total Commander v.6.03a, Autoškola professional 20.2, Autoškola professional 2002 v11.2, Autoškola professional v20.5, Autoškola professional 2002 11.9, PC Translator 2005 a HALF-LIFE COUNTERSTRIKE, aniž by získal právo k jejich instalaci koupí příslušných licencí od společností ADOBE SYSTEMS INCORPORATED, 345 Park Avenue, San Jose, California USA, MICROSOFT INC., One Microsoft Way, Redmont, USA, SYMANTEC CORPORATION, 20330 Stevens Creek Blvd., Cupertino, California, USA, AUTODESK INC., 111 McInnis Parkway, San

[64] Zdroj: Tamtéž

Rafael, California, USA, ALWIL Software, Praha 10, BORLAND spol. s.r.o., Praha 4, COMPELSON Trade, spol. s.r.o. Praha 9, JIMAZ, spol. s r.o., Praha 7, Bc. Jana Dobeše, Dačice, a LangSoft spol. s.r.o. Korytná, přičemž těmto vlastníkům autorských práv ke shora uvedenému komerčnímu software způsobil škodu ve výši 248.750,- Kč,

t e d y neoprávněně zasáhl do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovanému záznamu,

č í m ž s p á c h a l

trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 tr. zákona,

a o d s u z u j e s e

Podle § 152 odst. 1 tr. zákona s přihlédnutím k § 314e odst. 2 tr. řádu k trestu odnětí svobody v trvání **t ř i /3/** měsíců.

Podle § 58 odst. 1 a § 59 odst. 1 tr. zákona se výkon tohoto trestu podmíněně odkládá a stanoví se zkušební doba na **j e d e n /1/** rok.

Podle § 55 odst. 1 písm. a) tr. zákona se obviněnému zároveň ukládá **trest propadnutí věci**, a to 1 ks počítačové skříně šedé (metalové) barvy a 1 ks kazety DVC zn. Panasonic, které byl zajištěny při domovní prohlídce konané dne 3.5.2006.

Podle § 228 odst. 1 tr. řádu se obviněnému ukládá povinnost uhradit poškozeným zastoupeným advokátní kanceláří Voborník a Nigrini se sídlem Praha 1, Štupartská 9, částku ve výši **247.750,- Kč** (spol. Adobe 63.452,- Kč, spol. Autodesk 153.110,- Kč, spol. Microsoft 29.620,- Kč, spol. Symantec 1.568,- Kč).

P o u č e n í : Proti tomuto trestnímu příkazu mohou obviněný, osoby, které jsou oprávněny podat v jeho prospěch odvolání, a státní zástupce podat do osmi dnů ode dne doručení příkazu odpor u Okresního soudu v Mostě.

Byl-li podán proti trestnímu příkazu oprávněnou osobou v lhůtě odpor, trestní příkaz se ruší a samosoudce nařídí ve věci hlavní líčení; přičemž při projednávání věci v hlavním líčení není samosoudce vázán právní kvalifikací a ani druhem a výší trestu obsaženými v trestním příkazu.

Jinak se trestní příkaz stane pravomocným a vykonatelným.

Po doručení trestního příkazu může se oprávněná osoba odporu výslovně vzdát.

V Mostě dne 22.3.2007

JUDr. Benno Eichler, v.r.
samosoudce

Za správnost vyhotovení:

c) Rozhodnutí ve věci prodeje pirátských kopií prostřednictvím internetu (zkrácená verze).[65]

značka: 7T 111/2000

ČESKÁ REPUBLIKA

ROZSUDEK

JMÉNEM REPUBLIKY

Obvodní soud pro Prahu 1 vyhlásil v hlavním líčení konaném dne 22.3.2001 v Praze samosoudcem JUDr. Vladimírem Hermannem takto:

obžalovaní

1/ J J

1972 bytem Tachov,

2/ R Š

1973 , bytem Chrudim,

jsou vinni, že

v době od 4.9.1998 do 7.5.1999 nabízeli prostřednictvím kontaktní internetové adresy http: /members.zoom.com/palirna/ pirátské kopie CD nosičů s audio a video nahrávkami, a to tak, že přes mobilní telefon Pegas Twist si zájemce objednal na dobírku vybrané CD nosiče, které obdržel poštou a zaplatil na účet vedený u EXPANDIA BANKY a.s. , který byl dne 31.7.1998 založen na odcizené doklady obvinění prostřednictvím platební karty č. vystavené na jméno získané finanční prostředky vybírali, tímto způsobem obdrželi CD nosiče :

[65] Zdroj: Tamtéž

a získali tak minimálně finanční částku ve výši 187 943,- Kč, svým jednáním způsobili škodu spol. JRC, Vaníčkova č. 5, Praha 6, ve výši 17879,- Kč, spol. MICROSOFT Inc. USA zastoupeném Mgr. Martinem Vobornikem, AK Senovážné nám. 3, Praha 1, ve výši 20 600,- Kč, IFPI ČR, Senovážné nám. 23, Praha 1, ve výši 1500,Kč, BSP Praha s.r.o. , Čerčanská č. 3, Praha 4, ve výši 500,- Kč, COREL CORPORATION Kanada zastoupené Mgr. Martinem Vobornikem, AK Senovážné nám. 3,

Praha 1, ve výši 18782,50 Kč, spol. BUTTERFLY ENTERTAIMENT GROUP, Kvestorská č. 5, Praha 4, ve výši 100 000,Kč,

t e d y : jednak společným jednáním se zvukovým a obrazovým záznamem, který je předmětem práva příbuzného právu autorskému neoprávněně nakládali způsobem, který přísluší výrobci zvukového a obrazového záznamu a nositeli těchto práv,

jednak neoprávněně ve větším rozsahu provozovali výdělečné podnikání.

č í m ž   s p á c h a l i

ve spolupachatelství dle § 9 odst. 2 trt. zákona jednak tr. čin porušování autorského práva dle § 152 odst. 1 tr. zákona a jednak tr. čin neoprávněného podnikání dle § 118 odst. 1 tr. zákona

a   o d s u z u j í   s e

oba obžalovaní shodně dle § 152 odst. 1 tr. zákona za použití § 35 odst. 1 tr. zákona **k úhrnnému peněžitému trestu a to**

obž.J   J ve výši **š e d e s á t t i s í c /60.000,-/ K č** a pro případ, že by ve stanovené lhůtě nebyl trest vykonán, náhradní trest odnětí svobody v trvání **š e s t (6) m ě s í c ů ;**

obž. R   Š ve výši **č t y ř i c e t t i s í c /40.000,-/ K č** a pro případ, že by ve stanovené lhůtě nebyl trest vykonán, náhradní trest odnětí svobody v trvání **č t y ř i (4) m ě s í c e .**

Podle § 229 odst. 1 tr. řádu se poškození a to Centrum českého videa se sídlem Praha 1, Konviktská č.5, společnost Microsoft Corporation a společnost Corel Corporation zastoupené JUDr.Františkem Honsou, advokátem AK Burns Schawarts se sídlem Praha 1, Senovážné nám.č. 3 a s.r.o. Butterfly E.G. se sídlem Praha 4, Kvestorská č.5 se odkazují se svými uplatňovanými nároky na náhradu škody odkazují na řízení ve věcech občanskoprávních.

P o u č e n í : Proti tomuto rozsudku je právo odvolání do osmi dnů od odručení prostřednictvím zdejšího soudu k městskému soudu v Praze.

V Praze dne 22. března 2001   **JUDr.Vladimír Hermann** - samosoudce

OBVODNÍ SOUD PRO PRAHU 1 171

1.5 Závěr

V posledních letech, zejména s příchodem nových technologií, značně stoupá rozsah porušování autorských práv. V případech, kdy toto porušení nabývá takové společenské škodlivosti, že k nápravě již nepostačují instituty soukromého práva, nastupuje trestní represe. Tak je tomu i v českém prostředí, kde v poslední době přibývá odsuzujících rozsudků v trestních věcech týkajících se porušování autorských práv. Tyto rozsudky však postihují zejména „malé ryby", přičemž porušování autorských práv ve velkém bývá často nepotrestáno. Za vše hovoří masivní porušování autorských práv v kolejních sítích vysokých škol, které je prozatím ve většině případů ponecháno bez povšimnutí a jsou často mlčky trpěny i samotnými vysokými školami. Oprávnění z autorských práv se proto snaží nalézt cestu prostřednictvím prevence, v současnosti např. probíhá v masmédiích rozsáhlá kampaň České protipirátské unie, ve které upozorňují na trestnost neoprávněného užívání děl[66]. O úspěšnosti boje proti tomuto fenoménu však vypovídá i skutečnost, že po osmi letech je Česká republika znovu na seznamu zemí monitorovaných pro zvýšenou míru pirátství - Special 301 Watch List – každoročně vydávaného Úřadem obchodního zmocněnce USA (USTR - Office of the United States Trade Representative).[67] Naše země se tak (alespoň co se porušování autorského práva týče) znovu zařazuje po bok států, jako jsou Itálie, Litva, Maďarsko, Polsko a Rumunsko.

---

[66] V kampani je označováno předmětné trestněprávně relevantní jednání nesprávně jako „krádež", pro účely kampaně je však toto laické zjednodušení pochopitelné.

[67] Viz příloha č. 3.

2. Hackerství

2.1 Úvod

Hackerství neboli hacking je obecně ve společnosti pojímáno jako to, co ztělesňuje internetovou kriminalitu. Je to zejména proto, že internet tvoří integrální část tohoto fenoménu, bez něj tento fenomén prakticky neexistuje. Mnozí lidé si myslí, že podstatou hackingu je jakási revolta proti společnosti, lépe řečeno projevy hackingu jsou namířeny zejména proti veřejným autoritám, establishmentu, atd. V praxi však toto označení zahrnuje jednání, jejichž původci tvoří velice diversifikovanou skupinu osob od členů organizovaného zločinu po proti autoritám revoltujícího teenagera, které mají často diametrálně odlišný zájem a taktéž prostředky.

2.2 Definice a obecné aspekty hackerství

Pojem hacking, jenž pochází z anglického slova hack (rozseknout), bychom mohli definovat jako neoprávněné pronikání do počítačových a jiných elektronických systémů.

Podle toho, jaký je důvod těchto průniků, můžeme členit hacking na:

1.) Hackerství ze záliby, v konkrétních případech se jedná o jakýsi druh sportu. Jde o to, aby byl útočník (hacker) lepší, než jsou protiopatření obránce (oběti). V rámci internetové komunity je právě tato komunita označována za „pravé" hackery, kteří se od ostatních[68] liší tím, že svým jednáním nechtějí způsobovat škodu ani nic ničit, ze svého jednání nemají žádný zisk. Pokud zasahují do systému, je to proto, aby si udrželi přístup i nadále nebo po sobě zahlazovali stopy[69]

2.) Vandalský hacking, tato forma je odrazem obvyklého vandalismu v reálném světě. Pachatel chce zejména způsobit škodu, něco zničit či překazit.

3.) Stalking hackerství, zde se jedná o speciální druh obtěžování či slídění (harassment). Nejčastější je tato forma v případě zhrzených bývalých manželů či druhů, kdy pachatel pronikne do počítače oběti a nainstaluje tam závadný software (nebo již tak učiní dříve, když k němu má fyzický přístup), pomocí něhož získává osobní, někdy velice důvěrné informace o oběti, jako jsou přístupová hesla, obsah e-mailů s přáteli a případným novým druhem, atd.).

4.) Hackerství za účelem zisku, tento druh tvoří drtivou většinu hackingu a zároveň trpí největším procentem latence, jelikož jeho smysl není na sebe upozornit, jako je tomu v případě vandalství či některých forem hackerství ze záliby, nýbrž naopak být co nejdéle skryt a nezpozorován. Tento typ ovládá do značné míry organizovaný zločin (hovoří se o ruské internetové mafii[70]) a zisky z něj a jím způsobené škody dosahují někdy

---

[68] Pro označení „škodících" hackerů a jejich odlišení od hackerů „pravých" se využívá pojem „crackeři". To může však budit poněkud matoucí dojem, protože téže pojmenování se často používá pro určitou specializovanou skupinu hackerů, kteří odstraňují ochranný kód programu (tzv. účinných prostředků ochrany – viz hlava 1 Zvláštní části) za účelem jeho volného použití. Praví hackeři proto tuto skupinu nazývají „knackery".

[69] https://akela.mendelu.cz/~lidak/bis/seminar2004/seminarky/makovsky.doc., zobrazeno 15.7.2008, 16:40

[70] autor@chip.cz: Internetové mafii na stopě, časopis CHIP.CZ, č. 1/2008, str. 157 a násl.

astronomických částek. Bývá prostředkem nejrůznějších finančních podvodů a machinací, průmyslových špionáží a nekalosoutěžních jednání. Obecně je považováno za nejnebezpečnější.

Z výše uvedeného členění vyplývá i různá typologie pachatelů[71]:

1.) Inovátoři – jsou to odborníci, kteří se věnují hledání bezpečnostních chyb v systémech či zkoumají nová prostředí, aby mohli zjistit možnosti jejich překonání. Představují pouze 2 % z pachatelů hackingu. Obecně nejsou vnímáni jako vysoce nebezpeční.

2.) Slávychtiví amatéři a kopírovači – Mají obvykle omezené znalosti a nižší programátorskou dovednost. Touží po slávě a zájmu médií. Používají buď známé postupy a programy, nebo aplikují známé, jednoduché útoky. Jejich nebezpečí spočívá zejména v tom, že mohou svým jednáním spustit útok, aniž by věděli, jaké budou jeho následky.

3.) Vnitřní nepřátelé – jsou to obvykle nespokojení či bývalí zaměstnanci, dodavatelé a konsultanti. Jejich hlavním motivem je pomsta. Díky přístupu a znalosti bezpečnostních systémů mohou být velice nebezpeční a způsobit rozsáhlé škody.

4.) Organizovaní počítačoví gangsteři – Odhodlaní a velkým ziskem motivovaní počítačoví zločinci, mají rozsáhlé schopnosti i zdroje. Jako v jiných formách organizovaného zločinu tu dochází k vnitřní dělbě úkolů v rámci organizace a napojení na různou trestnou činnost (jedni získávají hackingem informace, druzí je prodávají a dostávají objednávky od potenciálních klientů, třetí perou špinavé peníze a poslední zajišťují chod a integritu celé organizace). Ze všech typů pachatelů hackingu jsou samozřejmě nejnebezpečnější.

2.3 Prostředky trestné činnosti hackerů - malware

K dosažení svých cílů využívají hackeři speciální software, pro nějž se vžilo označení „malware" či obecně viry v širším slova smyslu. Od prapůvodních virů známých z doby před rokem 1995, došlo s příchodem internetu k revoluci i v této oblasti a poměrně jednotná typologie virů se rázem začala diferencovat. Záhy vznikly dříve neznámé formy škodlivého softwaru a díky globálním možnostem internetu se viry změnily z jakéhosi prostředku zábavy úzké skupinky „fandů" či „záškodníků" v masový prostředek velice nebezpečného druhu kriminality a ve skvělou zbraň organizovaného zločinu.

Podle oficiálních dat, které zveřejňuje přední světová antivirová společnost F-Secure, překročil v roce 2004 celkový počet různých typů škodlivých kódů číslo 100 000. Odborníci zabývající se analýzou virů přitom každý den hlásí v průměru deset nových virů či jejich variant. V některých obdobích zvýšené aktivity pisatelů virů je však tento počet ještě daleko vyšší.[72]

---

[71] zdroj: Zpráva společnosti McAfee o internetové kriminalitě, časopis CHIP.CZ, č. 5/2007, str. 16 a násl.

[72] Nádeníček, P.: Počítačové viry známé a neznámé. 1. díl Úvod do problematiky & souborové viry, časopis PC WORLD, č. 11/2005

První kategorií malware jsou internetové viry v užším slova smyslu (tzv. souborový virus). Jedná se vlastně o následovníka původních virů známých z předinternetové doby. Virem je nazýván proto, že stejně jako jeho biologický protějšek (který je ostatně jeho předobrazem), dokáže své programové instrukce přidat do cizího (hostitelského) souboru (infikovat ho) a tak se dál šířit. V nejhorším případě, pokud se rozšíří do podstatných souborů, může znehodnotit určitý program či dokonce celý systém. Jejich vývoj je ale na ústupu, neboť jsou pro antivirové programy uživatelů snadno zjistitelné.

Druhým typem škodlivých kódů jsou e-mailové a síťové červy. Pro oba typy je společné, že na rozdíl od souborových virů nepotřebují ke svému šíření hostitelský program. Odlišují se však ve způsobu šíření. Síťový červ (jako dokonalejší forma) se totiž dokáže šířit úplně sám, bez asistence koncového uživatele, když využívá bezpečnostních slabin systémů. Oproti tomu e-mailový červ se ,jak už z názvu vyplývá, šíří pouze prostřednictvím e-amilů, resp. e-mailových klientů. E-mailový červ se nikdy neobejde alespoň bez minimální asistence koncového uživatele, neboť ten musí červa z přiloženého souboru k e-mailu spustit nebo minimálně otevřít infikovaný e-mail. E-mailové červy měly svůj vrchol počátkem tohoto desetiletí (kdo by neznal červ s názvem „I love you", který jako důmyslně využíval tzv. sociální inženýrství (viz hlava 3 Zvláštní části), v současné době však jejich využívání stagnuje.

Síťové červy tuto genezi nesledují, díky jejich šíření neodvislému od počínání koncových uživatelů, mohou znamenat hrozbu obrovských škod. Tak například 1.5.2004 propukla „epidemie", jehož hlavním aktérem byl červ Sasser. Šířil se pomocí bezpečnostní díry u služby, která se používá v operačních systémech Windows 2000 a XP. Projevoval se restartováním operačního systému, což mělo v řadě podniků a organizací fatální důsledky: Byl zastaven provoz na železnici australské společnosti RailCorp, což jistě nelibě neslo jejich 300.000 cestujících. Vážné problémy musely řešit tři velké mezinárodní bankovní ústavy, napadení asi 5000 počítačů dvou švédských nemocnic způsobilo výrazné omezení jejich činnosti a vyřadilo z provozu rentgenová zařízení. Nakaženy byly dokonce i mnohé počítače Evropské komise aj. Tvůrce tohoto červu byl dopaden, i díky odměně věnované společností Microsoft ve výši 5.000.000,- dollarů, již ani ne týden po vypuštění červa. Byl jím mladý německý programátor Sven Jaschen, jenž byl následně odsouzen k trestu odnětí svobody v délce trvání 21 měsíců s podmíněným odkladem výkonu po dobu 3 let a k 30 hodinám veřejně prospěšných prací. V soudním řízení byla vyčíslena celková škoda ve výši 130.000,- € a celkové náklady na dopadení pachatele se odhadují na 7.000.000,- €.

Jiným druhem malware představuje trojský kůň. I zde se jedná o paralelu s jinak známou skutečností, tedy „danajským darem". Trojský kůň neboli trojan je škodlivý počítačový program, který vykonává kromě toho, co se od něj očekává, i věci, které nejsou z hlediska uživatele žádoucí. Lakonicky by se dalo shrnout: „Navrch huj, vespod fuj."[73] Může mít mnoho projevů, které jsou někdy řazeny jako samostatné typy malware. Jedním z prvních byly tzv. dialery, které těžily ze skutečnosti, že většina uživatelů v počátcích internetu vužívala vytáčené telefonní připojení. Tyto dialery pak vytočily a přesměrovaly připojení přes velice drahé servery. Koncový uživatel pak s údivem zjistil, že jeho účet za telefon má o jednu či více cifer více než obvykle.

---

[73] Přibyl, T.: Druhý dech trojských koní, časopis PC WORLD, č. 2/2008, str. 110 a násl.

Dalším projevem trojského koně bývají škodlivé kódy, které umožňují, nebo usnadňují vzdálený přístup. Je jím jednak tzv. backdoor (zadní vrátka), který slouží k následnému obejití bezpečnostních prvků infikovaného systému a nahráním dalších škodlivých programů hackerem, popřípadě přímo převzetím kontroly. Extrémní formou pak je „Bot", díky němuž může uživatel přímo ztratit kontrolu nad svým počítačem (ten se pak stává „zombie počítačem"). Nejnovější formy Botů jsou dokonce plně automatizované a tak i rozšiřované, takže vytvářejí jakési armády, typicky v rukou organizovaného zločinu, díky nimž je možné podnikat útoky typu distribuovaného DoS útoku, který spočívá v zahlcení určitého systému, serveru, sítě, atd. provozem (žádostmi, e-mailovými zprávami) naráz tisíců infikovaných počítačů.

V neposlední řadě se projevují trojané jako spyware (nechtěné programy, které sbírají data a odesílají je, ať už jednorázově či soustavně, ven ze systému tvůrci nebo třetí osobě. Nejnebezpečnější jsou v rámci spywaru keyloggery (programy zaznamenávající stisknutí kláves, což umožňuje zisk jinak šifrovaných hesel) a snímače obrazovky, popřípadě vůbec nejnebezpečnější jejich kombinace. Nelze zapomenout také na zničující či žertovné projevy trojských koní.

Poslední zde uvedenou skupinou škodlivých kódů jsou rootkity. Ač nejmladší, představují závažné nebezpečí, neboť bývají obtížně detekovány i nejnovějšími antivirovými programy. Pracují na nízké úrovni operačního systému (kernel), což v něm těmto programům umožňuje získání nejvyšších práv. Zjednodušeně řečeno, rootkity pracují na nadřazené úrovni operačního systému než samotné antivirové programy, a proto se před nimi dokážou skrýt, a dokonce udělají to samé i s jinými (obvykle škodlivými) soubory. Dalším nebezpečím rootkitů je jeho umístění v kernelovém módu. Ten, na rozdíl od módu uživatelského, kde se nachází drtivá většina souborů včetně obvyklého malwaru, má neomezený přístup k celému operačnímu systému, nikoliv jen k omezenému prostoru. Tohoto velice rafinovaného prostředku využila i společnost SONY BMG jako účinného prostředku ochrany autorských práv. Po skandálu, který vyvolalo zjištění, že na jí vyrobené disky vkládá i rootkit, a následných žalobách od tohoto způsobu ochrany opustila. I když mnohé antivirové programy nedokážou rootkit vypátrat, existují naštěstí speciální programy, které je umí nalézt a zlikvidovat.

Jak je z výše uvedeného patrné, mají různé skupiny škodlivých kódů různou funkci a hackeři je využívají k různým cílům. Malware může dobře posloužit k ovládání počítače a převzetí kontroly (Boti, backdoor), shromažďování informací a jejich odesílání jiným osobám (spyware, keyloggers, snímače obrazovky), poškození informací (viry, některé trojské koně, červy), skrytí jiných škodlivých aktivit (rootkity), k pobavení či pozlobení (viry, trojané, červy), ale nemusí dělat také vůbec nic, to zejména v případech hackingu „ze sportu".

2.4 Modus operandi hackingu a jeho obvyklý průběh

V případech, kdy hacking neslouží jen k pobavení hackera je součástí rafinovaného kriminálního jednání, které má za účel zejména někoho výrazně poškodit a je prostředkem tučných zisků (zejména při průniků do systémů organizací), hackerské jednání nespočívá pouze v obvykle předpokládané podobě, že hacker je jakési počítačové individuum, které v přítmí svého obydlí vymyslí určitý škodlivý kód, který tak nějak pustí do světa. Tak tomu je pouze v případě hackerů ze záliby. V případech hackerství za účelem zisku (hospodářského hackingu) má toto jednání určitý typizovaný průběh, který můžeme rozdělit na určité fáze:

2.4.1 Získávání informací

V této fázi se hacker snaží získat co nejvíce informací o své oběti, zejména o způsobu fungování jejího počítačového systému, vnitřní sítě, webového serveru a samozřejmě bezpečnostních opatření. Za tím účelem u velkých organizací studuje inzeráty na zaměstnání IT specialistů, které samy o sobě mohou mnohé napovědět, když v požadavcích na schopnosti budoucího pracovníka bývá označení programů či systémů, které společnost využívá. To umožní pachateli soustředit se pouze na zjišťování bezpečnostních mezer právě v těchto programech. Obvyklé také je, že hacker úplně zkopíruje obsah webových serverů, které následně podrobně zanalyzuje.

2.4.2 Zjišťování infrastruktury sítě

V druhé fázi hacker zkouší jednotlivé možnosti a místa průniku do sítě. Tak vlastně nachází cesty, kterými by mohl do systému oběti proniknout. K tomuto výborně poslouží „technika" nazvaná skenování portů, díky níž pachatel zjistí, které porty[74] používají rozličné serverové služby. Celá řada serverových služeb při skenování portů zároveň zobrazuje číslo verze. I tato informace může být pro hackera velice cenná, která mu umožní vybrat nejlepší způsob a metodu svého finálního útoku.

Aby se hacker vyhnul identifikaci své IP adresy, která se musí nutně při skenování portů zobrazit, využívá někdy tzv. zombie počítače (viz výše), k tak jednoduché operaci postačí i běžně dostupné utility, nemusí zombie počítač ovládat Botem.

úplně nejefektivnější metodou zjišťování infrastruktury firemní sítě je skenování sítě uvnitř napadené společnosti. Pokud není hacker jejím zaměstnancem, je tato činnost velice riskantní a pachatel k ní potřebuje jistou dávku odvahy až drzosti. Obvykle se využívají metody sociálního inženýrství[75]. Pachatel se při fyzické návštěvě oběti vydává za potenciálního zákazníka, který například požádá o připojení hudebního přehrávače z důvodu dobytí baterie, na který pak stáhne potřebné informace, či se vydává za externího IT specialistu řešícího „aktuální problém systému".

Dalším způsobem může být skenování bezdrátových sítí pomocí speciálních a opět poměrně běžně dostupných programů. Pokud bude společnost využívat starší a méně bezpečný typ šifrování WEP, doba průniku nepřesáhne několik minut.

2.4.3 Zjištění možnosti přístupu a jeho provedení

Po získání dostatku informací týkajících se jeho oběti může hacker po jejich vyhodnocení přistoupit k samotnému průniku. Hacker si vybere (identifikuje) určité slabé místo systému a na něj použije některou z vhodných metod:

1) Využití problému „buffer overflow" (přetečení bufferem).

---

[74] Porty slouží k tomu, aby jedna IP adresa uživatele mohla být použita pro více služeb běžících na serveru.

[75] viz hlava 3 Phishing

Příčinou tohoto problému je chyba programátora, který stanoví určité omezení (např. 100 znaků) pro vyplnění určitého údaje uživatelem na webových stránkách společnosti. Programátor pak už ale nezjišťuje, co se stane, pokud uživatel toto omezení překročí (data přetečou). Obvyklé jsou dvě varianty. První způsobí, že dojde zatuhnutí aplikace. To sice může mít určité škodlivé konsekvence, nicméně neumožní hackerovi proniknout. Druhá varianta je značně nebezpečnější, neboť při ní dojde k zapsání přetečených dat (v našem případě škodlivého kódu hackera) přímo do paměti. Takto zapsaný kód může sám o sobě napáchat značné škody nebo může fungovat jako „zavaděč" dalších malware.

2.) Prolomení přístupového hesla.

Tento způsob patří k nejstarším a byl využíván i v době před vznikem internetu. Spočívá jednoduše v tom, že hacker získá určitými prostředky přístupové heslo do systému, se kterým pak má volnou dispozici. K prolomení hesla vede několik různých cest. Jedna spočívá v technice „brute force" (hrubá síla), tedy vyzkoušení pomocí speciálních aplikací kombinaci postupně všech možných písmen, čísel a znaků. Jelikož je toto testování časově obrovsky náročné (u hesla o osmi znacích při zohlednění malých a velkých písmen je počet kombinací 8^{62}), využívají se pokročilejší metody, konkrétně slovníkové, které vycházejí z předpokladu, že většina hesel je tvořena určitým významovým slovem z běžné řeči. Vyhledávací program pak testuje pouze slova zařazená do určité slovníkové databáze, což celý proces značně urychlí. Pokud ani tento způsob nevede k cíli, program rozšíří slovníkovou metodu o testování kombinace slova a čísel, atd. Jiným způsobem získání hesla je prostřednictvím sociálního inženýrství. Pachatel získá heslo tím, že mu ho oběť, resp. důvěřivý zaměstnanec jednoduše sdělí (pachatel uměle vyvolá krizi a zároveň navrhne řešení, k němuž však potřebuje přístupové heslo... Účinný je také nátlak.). Poslední obvykle využívanou metodou je „dumpster diving", tedy zjednodušeně řečeno prohledávání odpadků, kde by mohly být útržky papírků s hesly.

3.) Nekorektní zpracování chyby.

Pachatel zde využívá informací, které získává z chybových hlášení napadaného serveru. Ty totiž mohou při správné kombinaci „nesmyslných" dotazů poskytnout hackerovy cenné informace a nalézt detailní mezeru, pro niž napíše svůj vlastní škodlivý program, kterým pronikne do systému. Tento způsob vyžaduje již značnou míru schopností a znalostí problematiky.

4.) SQL Injection

Při této metodě útoku hacker těží z možnosti webových dotazníků či ukládání informací do databáze serverem. Pachatel proto napíše (či využije cizí) škodlivý kód a připojí ho k dotazu na databanku. Ta tento dotaz provede a zanese i škodlivý kód hackera.

5.) Cross–side scripting (zneužití serverů k odeslání skriptů – XSS)

Tento mechanizmus přenosu útoku na koncový počítač uživatele spočívá v narušení webových stránek využitím chyb v jejich zabezpečení, především ošetření vstupu jednotlivých uživatelů. Hacker zde podstrčí do cizích stránek svůj škodlivý kód napsaný v jazycích Java nebo Active X, které umožňují spouštění programů přímo ve webovém rozhraní, čímž pachatel propašuje svůj škodlivý kód do počítače oběti.

6.) Man in the middle (muž uprostřed, prostředník)

Poslední zde zmíněná metoda (v praxi jich však existuje mnohem více) se odlišuje od ostatních metod v tom, že k přímému průniku zde vůbec nedojde, pachatel pouze stojí mezi počítačem koncového uživatele a serverem, na který jsou přenášena data z něj, přičemž tento přenos dokáže odposlechnout. Hacker se tedy zachytí všechna data z počítače oběti, provede s nimi, co potřebuje, a následně je vrátí na server, kam byly původně adresovány. Může také využít některá hardwarová zařízení k odposlouchávání, např. ta, která dokáží zachytit vyzařování dat z počítače oběti.

2.4.4 Utajení

Aby nebyl hacker odhalen či dokonce mohl stejnou bezpečnostní chybu využívat i v budoucnu, musí po získání potřebných dat po sobě zahladit stopy. V opačném případě by totiž jím obtížně nalezená bezpečnostní mezera byla záhy zaplatována. Pachatel tedy musí např. vrátit zpět seznam naposledy vložených dokumentů. Obvyklé je taky nainstalování malware typu backdoor, aby mohl hacker v případě potřeby získat přístup k počítači i po nápravě bezpečnostní mezery uživatelem.

2.4.5 Využití výstupů z hackingu

Poslední fází hackerského jednání je využití informací a dat (přístupových hesel, obchodních materiálů a jiných dokumentů), které při svém průniku získal. Nejčastější jsou podvodná jednání (využití ukradené identity k spáchání jiného trestného činu), průmyslová špionáž (předání obchodních dokumentů, strategií, výrobních postupů konkurenci), ale nechybí třeba ani vydírání oběti v případech, že do systému při svém průniku nainstaloval škodící malware, který znemožňuje jeho řádné fungování či dokonce přebírá nad ním plnou kontrolu. Vyděrač pak nabídne své oběti, že škodlivý kód z jejího systému odstraní, pokud mu zaplatí dostatečně vysokou částku...

2.5 Prevence hackingu

V oblasti ochrany před hackerstvím existují v zásadě dvě základní pravidla. Prvním z nich je nikomu a ničemu nedůvěřovat, obzvláště pokud je v sázce získání přístupových či osobních údajů. Hackeři často využívají rafinované metody a techniky, které dokážou obelstít jinak pozorného a inteligentního člověka. Lidé mají obvykle vyšší důvěru k počítačovým datům a informacím, aniž by si často uvědomili, že i tyto mohou být zmanipulované. Je proto nutné vždy pochybovat o pravdivosti tvrzení a nabídek, které požadují vyplnění nebo zaslání určitých citlivých údajů, nebo nutí uživatele stáhnout či otevřít některé neznámé soubory.

Druhým a možná důležitějším pravidlem prevence je využívání bezpečnostních programů. Nelze se vždy spoléhat pouze na zdarma přístupné antivirové programy. Zejména pro různé organizace by mělo být pravidlem využívání celého bezpečnostního balíčku služeb obsahujícího profesionální verzi antivirového programu, firewallu (zjednodušeně kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje[76]) a antispamu (prostředku na ochranu před nevyžádanými nebo nechtěnými zprávami a soubory).

---

[76] Wikipedia; http://cs.wikipedia.org/wiki/Firewall; zobrazeno 13.6.2008, 15:25

Ve velkých společnostech je dnes také běžné využívání metod penetračního testování. Jedná se vlastně o využití hackerů na objednávku, kteří pak zjišťují všechny možné bezpečnostní slabiny systému.

2.6 Trestní odpovědnost

2.6.1 Nebezpečnost činu pro společnost

Jako v případě jiných typů kriminálních jednání bude třeba při zkoumání trestné odpovědnosti pachatele vždy zkoumat nebezpečnost činu pro společnost. V případě hackingu bude nutné podrobně zkoumat naplnění materiální stránky trestného činu zejména u těch hackerských jednání, která nemají za cíl získat majetkový prospěch ani výrazně poškodit svou oběť, ale jedná se o hacking z žertu za účelem pouhého pozlobení adresáta takového jednání, popřípadě o hacking ze „sportu".

2.6.2 Trestněprávní kvalifikace

V českém právním řádu jsou většina jednání spadajících pod hacking stíhána podle ustanovení § 257a tr.zák. upravující trestný čin Poškození a zneužití záznamu na nosiči informací:

§ 257a

Poškození a zneužití záznamu na nosiči informací

(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch
a) takových informací neoprávněně užije,
b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo
c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,
bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu.

Tento trestný čin je systematicky zařazen do Hlavy deváté trestního zákona. Trestné činy proti majetku a lze jej zařadit mezi trestné činy poškozovací. Objektem tohoto trestného činu tak je zájem na ochraně dat uložených na nosiči informací (jejich změně, neoprávněným užitím) a dále ochrana počítačů a jiného telekomunikačního zařízení před neoprávněným zásahem. Tím však není okruh chráněných zájmů zdaleka vyčerpán, trestní zákon tímto

ustanovením taktéž nepřímo chrání obchodní a bankovní tajemství, autorská díla, citlivé údaje, atd., pokud je nosič informace obsahuje.[77]

Předmětem útoku je v konkrétním případě počítač nebo systém, do kterého se hacker snaží proniknout, popřípadě informace, kterou se snaží získat, změnit či poškodit.

V případě hackerství se pachatel dopouští jednání uvedené v předchozí kapitole této hlavy a části diplomové práce. Stávající právní úprava však, na rozdíl od zvažovaného návrhu trestního zákona, nepostihuje hackerské jednání spočívající v samotné přípravě průniku, např. odstranění bezpečnostních bariér (pokud nezasáhne do programového vybavení počítače) či v získání přístupu jako takového. Stejně tak není trestné vytváření škodlivých kódů, které by mohly k průniku sloužit. (oboje arg. a contrario § 257 odst. 1 tr.zák.)[78]

Přístup k počítači může být zjednán i na dálku, tj. internetem, což se také v praxi u hackerství děje nejčastěji. Samotný přístup může být získán oprávněně i neoprávněně, což postihuje i ty případy, kdy pachatel měl k nosiči informací přístup poskytnut (zaměstnavatel, přítel, atd.).

K trestnosti hackerství se vyžaduje úmyslná forma zavinění, a to orientovaná ke způsobení škody nebo jiné újmy jinému nebo neoprávněného prospěchu pro sebe nebo jiného. Ke škodě nebo prospěchu však nemusí dojít.[79]

Subjektem tohoto jednání může být kdokoli.

Naplnění kvalifikovaných skutkových podstat TČ podle § 257 a odst. 2, 3 tr.zák spočívá ve spáchání těžších následků (účinků) a ve spáchání hackerství jako člen organizované skupiny.

Jak je zmíněno výše, je hackerské jednání často prostředkem k spáchání mnoho jiných trestných činů, není proto vyloučen jednočinný souběh trestného činu podle § 257a tr.zák s TČ Podvodu (§ 250 tr.zák.), včetně jeho zvláštních forem Pojistného a Úvěrového podvodu (§ 250a, § 250b tr.zák.), Krádeže (§ 248 tr.zák.), Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 152 tr.zák.), Nekalé soutěže (§ 149 tr.zák.), Porušování tajemství dopravovaných zpráv (§ 239 odst. 1 písm. b), odst. 2 písm. a) tr.zák.), aj.

2.7 Kasuistika

Zřejmě nejznámějším dopadeným hackerem na světě je Vladimír Levin, ruský programátor a správce sítě, který v roce 1994 dokázal podvodně vyvést z účtů několika významných klientů Citibank prostřednictvím bezpečnostních mezer platebního systému banky (přesný postup, jakým Levin vyvedl peníze, se doposud nepodařilo přesvědčivě zjistit, někteří dokonce tvrdí, že mu informace o chybách systému byly prodány za 100 $) celkem 10,7 milionů $ a poslat

---

[77] Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 711 a násl.

[78] blíže k tomu v části III Úvahy de lege lata a de lege ferenda této práce

[79] Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 712

je na účty svých komplicu ve Finsku, Izraeli, Německu, USA a Nizozemí. Tři z těchto pomocníků byli záhy zadrženi při výběru převedených částek v Tel Avivu, San Franciscu a Rotterdamu. Výslechy přivedly vyšetřovatele na stopu Vladimíra Levina tehdy žijícího v Sankt Petersburku. Jelikož tehdy neexistovaly mezi Ruskou federací a USA žádné extradiční mezinárodní smlouvy týkající se tohoto trestného činu, zůstával Vladimír Levin dlouho mimo dosah amerických trestních orgánů. V květnu roku 1995 ho však na londýnském letišti zatkli příslušníci Scotland Yardu a po proběhlém vydávacím řízení byl v červnu 1997 postaven ve Spojených státech před soud. Levin se sám přiznal k vyvedení pouze částky 3,7 milionů $. Byl uznán vinným a odsouzen ke třem letům odnětí svobody. Podle prohlášení Citibank se do její dispozice nevrátilo pouze 400.000,- $ z celé ukradené částky. Po zkompromitování počítačového platebního systému musela postižená banka zavést zcela nové bezpečnostní prvky k ochraně před podobnými transakcemi[80].

V českém prostředí je značně mediálně známá skupina CzERT, jejíž vrchol byl koncem 90. let minulého století. Její členové však nebyli nikdy dopadeni. Z odsouzených případů je možné zmínit Věnka Herynka, který byl v říjnu roku 2003 definitivně uznán vinným ze spáchání trestného činu Podvodu a odsouzen k trestu odnětí svobody v délce trvání 7 let. Čin měl spáchat tím, že jako počítačový expert GE Capital Bank vyvedl z účtů banky 193 milionů korun na několik svých účtů u různých německých bankovních ústavů.[81]

2.8 Závěr

Hackerství představuje nový typ kriminálního jednání, které v reálném životě nemá svůj protějšek. Je nejtypičtějším představitelem kybernetické kriminality. Má mnoho variant a projevů, obvykle v závislosti na tom, za jakým účelem je hackerské jednání uskutečňováno a kdo je jejím pachatelem. Obrovské nebezpečí představuje hacking jako nástroj organizovaného zločinu. Na rozdíl od hackerů individuálů je totiž jejich dopadení díky strukturám organizovaného zločinu velice obtížné a zůstává neodhaleno, nebo jejich vyšetřování skončí nezdarem. Navzdory možným astronomickým hodnotám škod, které může hacking vyvolat, jsou stávající hrozby trestů, pokud nejsou zároveň naplněny znaky jiného trestného činu, neúměrně nízké, když při způsobení škody velkého rozsahu je horní hranice trestní sazby za tento čin omezená 5 lety, což rozhodně neodpovídá typové nebezpečnosti tohoto jednání.

---

[80] zdoj: http://en.wikipedia.org/wiki/Vladimir_Levin, zobrazeno: 7.6.2008, 13:53

[81] http://www.novinky.cz/clanek/93889-pocitacovi-pirati-uz-obrali-banky-o-stovky-milionu.html, zobrazeno 15.7.2008, 13:05

3. Phishing

3.1 Úvod

S rozvojem elektronických platebních prostředků, ale i internetového nakupování, dražeb a aukcí a dalších aktivit, kde se užívají citlivé osobní údaje (čísla účtů, přístupová hesla, adresy, atd.), začala se objevovat i trestná činnost, jejíž cílem bylo tyto údaje získat a následně zneužít. Postupně získávaly tyto aktivity čím dál více na rafinovanosti a začaly těžit z těch výhod, které v nekybernetickém světě neexistují. Těmito výhodami jsou zejména bezplatnost e-mailů a možnost jejich rozšíření po celém světě. Jednou z těchto podvodných aktivit je i phishing, někdy česky překládaný jako rhybaření.

3.2 Vymezení pojmu

Phishing je většinou definován jako kriminální jednání, jehož cílem je podvodně získat či vylákat citlivé informace jako jsou přihlašovací jména, hesla a údaje o kreditních a debetních kartách tak, že se pachatel maskuje za důvěryhodnou osobu či organizaci, a to prostřednictvím elektronické komunikace[82]. Nejčastějšími prostředky této komunikace bývají e-mail a programy typu „instant messaging[83]". Pachatelé se nejčastěji ukrývají za identitu banky oběti, internetové obchody jako e-bay, PayPal, Amazon či za servery typu YouTube.

3.3 Předchůdce phishingu – nigerijské listy

Jako předchůdce phisingu bývá označováno jednání známé pod názvem nigerijské listy (dopisy) či „419 podvod"[84]. To spočívalo v hromadném rozesílání dopisů a s příchodem internetu e-mailových zpráv, jejichž účelem je vylákat z důvěřivé oběti určitou sumu, přičemž je slíben několikanásobně vyšší zisk. Samotné nigerijské dopisy mají původ v podobném podvodném jednání nazvaném „španělský vězeň", jehož předmětem bylo přesvědčení oběti, že jistý pohádkově bohatý (fiktivní) spoluvězeň je ochoten se o toto bohatství rozdělit, pokud bude osvobozen. Za tím účelem proto měla oběť zaslat peníze k podplacení stráže...

U nigerijských listů je záminka vylákání peněz různá, obvykle bývá podkladem nabídka pohádkového zisku převedením mnohamilionových částek z „mrtvých kont" po obětech nebo svržených diktátorech po proběhlé občanské válce v Nigerii či jiné africké zemi. Podobnou zástěrkou je příběh místních bohatých podnikatelů a farmářů, kteří po převratu jsou ohroženi na životě a majetku, a tak se rozhodli emigrovat, přičemž nechtějí za sebou zanechat veškerý poctivě a namáhavě vydělaný majetek. K tomu však nutně potřebují asistenci...

Společné všem těmto podvodům je, že po zahájení příslušných kroků k převodu peněz se začne cosi komplikovat, nejčastěji je třeba zaplatit určitý poplatek za zřízení společnosti, přes kterou se majetek vyvede ze země, poplatek za rozhodnutí úřadu o povolení k vyvedení

---

[82] Wikipedia: http://en.wikipedia.org/wiki/Phishing, zobrazeno 6.6.2008, 13:20

[83] Výraz se obvykle v českém jazyce používá v původním anglickém znění, jedná se o prostředky okamžité komunikace, kdy adresátům se zasílané zprávy zobrazují takřka okamžitě po odeslání odesílatelem, přičemž lze obvykle sledovat historii této komunikace.

[84] Název je paralelou k číslu paragrafu nigerijského trestního zákoníku upravující trestný čin podvodu.

peněz, poplatek za převod samotný, atd. Tyto „poplatky" dosahují i hodnot tisíců dolarů, a tak oběť pozvolna přichází o nemalé peněžní sumy, ale proklamovaného zisku se nikdy nedočká. Organizovanost pachatelů těchto trestných činů (obvykle pocházejí z Nigerie, Jihoafrické republiky, Toga, ale dokonce i z Nizozemí apod.), dosahuje velmi vysokého stupně a jsou zdokumentovány případy únosů a vražd těch obětí, které se rozhodli „asistovat" převedení peněz přímo na místě.[85]

Zde je ukázka typického úvodního dopisu:

REQUEST FOR URGENT BUSINESS RELATIONSHIP

FIRST, I MUST SOLICIT YOUR STRICTEST CONFIDENCE IN THIS TRANSACTION. THIS IS BY VIRTUE OF ITS NATURE AS BEING UTTERLY CONFIDENTIAL AND 'TOP SECRET'. I AM SURE AND HAVE CONFIDENCE OF YOUR ABILITY AND RELIABILITY TO PROSECUTE A TRANSACTION OF THIS GREAT MAGNITUDE INVOLVING A PENDING TRANSACTION REQUIRING MAXIIMUM CONFIDENCE.

WE ARE TOP OFFICIAL OF THE FEDERAL GOVERNMENT CONTRACT REVIEW PANEL WHO ARE INTERESTED IN IMPORATION OF GOODS INTO OUR COUNTRY WITH FUNDS WHICH ARE PRESENTLY TRAPPED IN NIGERIA. IN ORDER TO COMMENCE THIS BUSINESS WE SOLICIT YOUR ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THE SAID TRAPPED FUNDS.

THE SOURCE OF THIS FUND IS AS FOLLOWS; DURING THE LAST MILITARY REGIME HERE IN NIGERIA, THE GOVERNMENT OFFICIALS SET UP COMPANIES AND AWARDED THEMSELVES CONTRACTS WHICH WERE GROSSLY OVER-INVOICED IN VARIOUS MINISTRIES. THE PRESENT CIVILIAN GOVERNMENT SET UP A CONTRACT REVIEW PANEL AND WE HAVE IDENTIFIED A LOT OF INFLATED CONTRACT FUNDS WHICH ARE PRESENTLY FLOATING IN THE CENTRAL BANK OF NIGERIA READY FOR PAYMENT.

HOWEVER, BY VIRTUE OF OUR POSITION AS CIVIL SERVANTS AND MEMBERS OF THIS PANEL, WE CANNOT ACQUIRE THIS MONEY IN OUR NAMES. I HAVE THEREFORE, BEEN DELEGATED AS A MATTER OF TRUST BY MY COLLEAGUES OF THE PANEL TO LOOK FOR AN OVERSEAS PARTNER INTO WHOSE ACCOUNT WE WOULD TRANSFER THE SUM OF US$21,320,000.00(TWENTY ONE MILLION, THREE HUNDRED AND TWENTY THOUSAND U.S DOLLARS). HENCE WE ARE WRITING YOU THIS LETTER. WE HAVE AGREED TO SHARE THE MONEY THUS; 1. 20% FOR THE ACCOUNT OWNER 2. 70% FOR US (THE OFFICIALS) 3. 10% TO BE USED IN SETTLING TAXATION AND ALL LOCAL AND FOREIGN EXPENSES. IT IS FROM THE 70% THAT WE WISH TO COMMENCE THE IMPORTATION BUSINESS.

PLEASE,NOTE THAT THIS TRANSACTION IS 100% SAFE AND WE HOPE TO COMMENCE THE TRANSFER LATEST SEVEN (7) BANKING DAYS FROM THE DATE OF THE RECEIPT OF THE FOLLOWING INFORMATIOM BY TEL/FAX; 234-1-7740449, YOUR COMPANY'S SIGNED, AND STAMPED LETTERHEAD PAPER THE ABOVE INFORMATION WILL ENABLE US WRITE LETTERS OF CLAIM AND JOB DESCRIPTION RESPECTIVELY. THIS WAY WE WILL USE YOUR COMPANY'S NAME TO APPLY FOR PAYMENT AND RE-AWARD THE CONTRACT IN YOUR COMPANY'S NAME.

WE ARE LOOKING FORWARD TO DOING THIS BUSINESS WITH YOU AND SOLICIT

---

[85] Wikipedia: http://en.wikipedia.org/wiki/Nigerian_letters, zobrazeno 6.6.2008, 13:53

YOUR CONFIDENTIALITY IN THIS TRANSATION. PLEASE ACKNOWLEDGE THE RECEIPT OF THIS LETTER USING THE ABOVE TEL/FAX NUMBERS. I WILL SEND YOU DETAILED INFORMATION OF THIS PENDING PROJECT WHEN I HAVE HEARD FROM YOU.

YOURS FAITHFULLY,

DR CLEMENT OKON

NOTE; PLEASE QUOTE THIS REFERENCE NUMBER (VE/S/09/99) IN ALL YOUR RESPONSES.[86]

3.4 Modus operandi phishingu

Phishing má s nigerijskými listy mnoho společného. První z těchto společných znaků je způsob provedení, tj. šíření prostřednictvím e-mailové komunikace. Ta z těchto jednání činí velice nebezpečnou kriminální činnost, protože pachatel může oslovit miliony potenciálních obětí na celém světě. Většina obětí phishingu nepředpokládá, že by mohla obdržet e-mailovou zprávu od neznámého podvodníka, kterému adresu nikdy neposkytla, a tak slepě důvěřují obsahu zpráv, které se tváří, že pochází od známých obchodníků, bank, apod. Pro pachatele je dnes však velice snadné získat e-mailovou adresu kohokoli. Způsob je jednoduchý, na internetu je možné zakoupit i databáze s e-mailovými adresami. Ty se získávají od majitelů webových stránek, kam uživatelé čas od času e-mailové adresy vyplní (např. při sjednávání pojištění po internetu, registrace na různá fóra, atd.), a ti je pak neoprávněně poskytnou těmto „sběratelům adres".

Jediné, co je pachateli phishingu na překážku, jsou jazykové rozdíly. Zde se totiž ukazuje značná výhoda češtiny jako obtížného a málo používaného jazyka. Zatímco zahraniční čtenáři pokusů phishingových pachatelů musí při čtení těchto e-mailů více uvažovat, čeští uživatelé internetu jsou v drtivé většině případů této činnosti ušetřeni, naopak je phishingový e-mail může spíše pobavit, když obdrží od své seriozní banky takovouto zprávu: „My dekovat ty za tva duvera a tesit se na ty vyuzivat clen urcity sluzba my poskytnout." Z hlediska celosvětového používání internetu malý počet českých uživatelů zřejmě nestojí pachatelům phishingu za zaplacení správného překladu, a tak využívají automatické překladače, které si s nástrahami českého jazyka zatím (z hlediska phishingu naštěstí) neumí dostatečně poradit. Proto se v českých podmínkách uplatňují pouze phishingové útoky lokální, tedy jednání páchaná přímo českými občany. O to jsou však tyto formy nebezpečnější, protože tito pachatelé sami dobře znají prostředí, ve kterém se pohybují i jejich potenciální oběti.

Druhým společným znakem phishingu a nigerijských listů je využívání tzv. sociálního inženýrství. V kriminologii tohoto pojmu využívá pro vyjádření umění někoho přesvědčit, aby prozradil o sobě nebo někom jiném určité citlivé informace či údaje[87]. Metody sociálního inženýrství lze rozdělit do dvou skupin: 1.) Computer based Social Engineering a 2.) Human

---

[86] zdroj: http://www.snopes.com/crime/fraud/nigeria.asp, zobrazeno 21.7.2008, 13:40

[87] Čepička, D., Arnold, A., Behrens, D.: Odhalte triky hackerů, časopis PC WORLD, č. 12/2007, str. 68 a násl.

Based Social Engineering. Rozdíl mezi nimi je v tom, že zatímco v druhém případě je informace získávána pachatelem osobně (fyzicky přítomným či alespoň telefonicky), čemuž je ale obtížnější odolat, v prvním případě se informace vyloudí z oběti prostřednictvím elektronických prostředků, zejména e-mailu. Zde je menší důvěra adresátů v pachatelovo neosobní sdělení vykompenzována jejich obrovským počtem, který zvýší šance úspěchu pachatele. Sociální inženýrství je tak založeno na zneužití důvěry, kterou pachatel získá různými úskoky.

V případě phishingu se konkrétní jednání pachatele projeví tak, že oběti přijde e-mail, který se tváří jako důležitá zpráva od obvyklého poskytovatele některých služeb, které oběť využívá. V této zprávě je oběť vyzvána, aby na webové adrese, na kterou je přímo v e-mailu poskytnut link (odkaz), vyplnil údaje, které poskytovatel potřebuje k ověření totožnosti, správnosti nastavení, z důvodu aktualizace databáze, přechodu na nový informační systém, atd. Tato adresa však nemá se skutečným poskytovatelem služeb nic společného, pouze design webových stránek, na které odkazuje, je shodný či podobný se stránkami skutečného poskytovatele, či se alespoň zdá seriózní. Když pak nic netušící oběť stránku otevře a údaje vyplní, získá je útočník, který s nimi pak může volně disponovat (skrývat se za identitou jiného) a v případech podvodů s elektronickým bankovnictvím mohou phishingoví pachatelé vybrat oběti i všechny finanční úspory.

V rafinovanějších útocích pak není poskytnut v e-mailu přímo link na pachatelovy stránky, ale je zde ukrytý např. javascript, který dokáže modifikovat zapsanou správnou adresu přímo v prohlížeči. Někdy jsou při phishingu taktéž využívány hackerské metody jako cross site scripting.[88]

Typický phishingový e-mail má tuto podobu (zdroj: http://en.wikipedia.org/wiki/Phishing):

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc

[88] Baudiš, P.: Staronové nebezpečí Rhybaření, časopis CHIP.CZ, č. 4/2006, str. 14

Zde je příklad z českého prostředí, nejprve poněkud úsměvný:[89]

Drahousek Zakaznik,

Ceska Sporitelna docasny prerusit tvuj ucet.Duvod : Karta Cislo nedostatek. My naridit tebe az k cely neurc. clen ucet aktualizovat asi tolik my pocinovat odemknout tvuj ucet. Az k dat na pretres clen urcity aktualizovat beh cvaknout zde :

** Druhdy tebe mit cely clen urcity beh , my vule poslat tebe neurc.*
** Clen elektronicka posta oznameni aby tvuj ucet is pristupny zas. Potom tebe pocinovat pristup tvuj ucet kdykoliv.*
** Clen urcity hlaseni darovat vule byt bajecna vec do drzost a opatreny do nas bezpecny databazovy .*

-li tebe byt ve stychu az k darovat naridit hlaseni tvuj ucet vule byt automaticne odstranit dle Ceska Sporitelna databazovy

http://www.csas.cz/banka/appmanager/portal/banka?_nfpb=true&_pageLabel=home

© 2008 Ceská Sporitelna Bank.

A zde už rafinovanější forma:[90]

Varovani pred novou verzi podvodnych e-mailu

Vazeni klienti,

Radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Stavebni Sporitelna - Ceske Sporitelny, tentokrat vsak z oficialni e-mailove adresy banky burinka@sscs.cz. Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju.

Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize:

https://www.servis24.cz/ebanking-s24/app/register.pl?code=2E1E-EBB6-EA1N-D1EC&step=vrf_email_actions

Verifikovaci spojeni je platne do 24 hodin.

---

[89] http://blog.jancermak.cz/phishing-ceska-sporitelna-sbirka-nejpopularnejsiho-spam-phishingu-poslednich-dni/2008/03/19/, zobrazeno 17.6.2008, 16:23

[90] tamtéž

3.5 Prevence

V případech phishingu musí prevence této kriminality spočívat zejména na veřejném upozorňování na tento fenomén, a to jak ze strany autorit, tak i poskytovatelů služeb, kteří díky těmto útokům ztrácejí mezi svými zákazníky dobrou pověst. I když existují mnohé technické prostředky ochrany před tímto fenoménem (většina e-mailových klientů je vybavena rozpoznávači útoků typu phishing, některé české banky zavádějí složitější systémy přihlášení k účtu, například pomocí verifikační sms, atd.), nejdůležitější je, aby byl tento druh trestné činnosti mezi veřejností znám. Upozorňovat by se mělo zejména na skutečnost, že žádný finanční ústav či seriózní poskytovatel služeb nebude zasílat žádosti o sdělení hesla k přístupu ke službám e-mailem. Stejně tak by si každý měl dobře rozmyslet důsledky, které mohou nastat, pokud své osobní údaje a přístupové informace bez rozmyslu vepíše na jakoukoli internetovou stránku.

3.6 Trestní odpovědnost

3.6.1 Společenská nebezpečnost

Na rozdíl od ostatních typů internetové kriminality není u phishingu příliš složité zkoumání materiální stránky trestného činu. Osobně si dokážu představit jen velice málo situací, kdy by požadavek nebezpečnosti činu pro společnost nebyl naplněn. Drtivá většina útoků phishingu je společensky velmi nebezpečná, a to vzhledem k způsobu útoku (využívání lsti, úskoků a důvěřivosti obětí), místem činu (internet, resp. e-mail, tedy je obvyklá masovost páchání trestné činnosti) i způsobenými následky (účinky) v podobě vysoké hodnoty spáchaných škod.

3.6.2 Trestněprávní kvalifikace

Jednání pachatelů phishingu lze podle českého trestního zákona kvalifikovat nejčastěji jako trestný čin Podvodu dle ust. § 250 tr.zák.:

§ 250

Podvod

(1) Kdo ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu nikoli malou.

(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) způsobí-li takovým činem značnou škodu nebo jiný zvlášť závažný následek.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Tento trestný čin je systematicky zařazen do Hlavy deváté trestního zákona. Trestné činy proti majetku a řadí se mezi jednání obohacovací. Objektem je zde tedy cizí majetek a majetková práva.

V případě phishingu spočívá objektivní stránka tohoto trestného činu v jednání uvedeném výše, tzn., že pachatel uvede oběť phishingu v omyl (mylná představa oběti o tom, že ji kontaktoval skutečný poskytovatel služeb) a ta následně poskytne citlivé informace pachateli, který je ke škodě oběti využije a sebe tím obohatí.

K trestnosti tohoto jednání se bude vždy vyžadovat způsobení škody na cizím majetku nikoliv nepatrné, tj. částky alespoň 5.000,- Kč (§ 89 odst. 11 tr.zák.).

Pachatelem může být kdokoliv.

Trestný čin podvodu lze spáchat pouze úmyslně, to však ve vztahu k phishingu nečiní potíže, neboť jen těžko si lze představit, že by někdo rozesílal phishingové e-maily nedbalostně (nebereme-li v úvahu, pokud je něčí počítač využíván či ovládán k této trestné činnosti).

Naplnění kvalifikovaných skutkových podstat vyžaduje způsobení těžších následků nebo spáchání trestného činu jako člen organizované skupiny.

V případech, kdy pachatel nejedná v úmyslu způsobit někomu majetkovou škodu, ale například hodlá někoho díky phishingem ukradené identitě někoho poškodit na nemajetkových právech (veřejně zostudí, hanobí, pomlouvá, atd.), bude možné jeho jednání kvalifikovat podle ustanovení § 209 tr.zák. jako trestný čin Poškozování cizích práv:

§ 209

Poškozování cizích práv

(1) Kdo jinému způsobí vážnou újmu na právech tím, že

a) uvede někoho v omyl, nebo

b) využije něčího omylu,

bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

(2) Odnětím svobody až na tři léta bude pachatel potrestán, vydává-li se při činu uvedeném v odstavci 1 za veřejného činitele.

Trestný čin dle § 209 tr.zák. spadá pod Trestné činy hrubě narušující občanské soužití Hlavy páté trestního zákona. Objektem tohoto trestného činu jsou nemajetková práva subjektů.

Objektivní stránka spočívá v konkrétním případě v tom, že pachatel jednáním popsaným výše uvede oběť v omyl a způsobí ji tak vážnou újmu na nemajetkových právech (typicky právech osobnostních).

Subjektem může být opět kdokoli a po subjektivní stránce se vyžaduje zavinění.

Podle toho, jak pachatel phishingu neoprávněně obdržené údaje využije, může být jeho trestná činnost kvalifikována krom TČ podle § 250 tr.zák či § 209 tr.zák. i v rámci souběhu s různými jinými trestnými činy, např. Hanobení národa, etnické skupiny, rasy a přesvědčení dle § 198 tr.zák. (pod ukradenou identitou z phishingu pachatel veřejně hanobí občany židovské národnost).

3.7 Závěr

Phishing je kriminální jednání značně nebezpečné. K jeho uskutečnění postačí elementární znalost fungování elektronické pošty a šíře zasažených obyvatel bývá značná. Má obyčejně také velice závažné důsledky, když odcizení účtu může vést až k vyvedení všech finančních prostředků z účtu, k jeho zneužití (zastavení či ručení pro sjednávání úvěrové smlouvy) nebo dokonce k úplné ztrátě kontroly nad ním. 90 % všech pokusů o phishing v roce 2005 se týkalo bankovních a finančních služeb.[91] Bankovní ústavy by proto měli zvýšit osvětu mezi svými klienty, zejména pak těmi, kteří využívají služeb internetového bankovnictví a předcházet tím nejlépe tomuto typu podvodného jednání. Pokusům o phishing zřejmě nikdy nezamezíme a čas od času se budou objevovat nové způsoby a rafinované „finty", jak uživatele podvést. Pokud bude ale veřejnost dostatečně informována, drtivá většina těchto útoků nebude úspěšná a zamezí se tak obrovským škodám, které každoročně v této souvislosti vzniknou[92].

---

[91] Baudiš, P.: Staronové nebezpečí Rhybaření, časopis CHIP.CZ, č. 4/2006, str. 14

[92] Pro zajímavost je v příloze č. 4 zobrazení celosvětového rozložení phishingových útoků z hlediska původce v roce 2006.

4. Zneužívání (krádež) strojového času v souvislosti s internetem

4.1 Úvod

Problematice zneužívání strojového času[93] v souvislosti s internetem, obzvláště pak jeho trestněprávním aspektům, je ve společnosti věnována jen velmi malá pozornost. V praxi jsou tato jednání do značné míry tolerována a jejich postih končí nanejvýš soukromoprávní sankcí (okamžité zrušení pracovního poměru či žalobou na náhradu škody). Někdy je však následek této trestné činnosti natolik závažný, že postih soukromoprávní nepostačuje a nastupuje trestní represe.

4.2 Vymezení pojmu, původ a typy jednání

Krádeží počítačového času se rozumí neoprávněné užívání části nebo celé výpočetní kapacity počítače. V souvislosti s internetem lze tento pojem definovat jako neoprávněné užívání části nebo celé kapacity počítače pro přístup do sítě internet a krádež konektivity.

Krádež strojového času patří mezi nejstarší počítačové delikty vůbec, jelikož k němu docházelo již v dobách tzv. sálových počítačů[94]. Tento delikt tehdy spočíval v neoprávněném provádění výpočtů na počítačích zaměstnavatele. Tyto aktivity pak byly obvykle klasifikovány jako trestný čin Neoprávněného užívání věci z majetku v socialistickém vlastnictví dle § 133 tr.zák. ve znění platném do 1.7.1990 s hrozbou trestu odnětí svobody až na dvě léta v základní skutkové podstatě. Výsledky výpočtů mohly být využity různými způsoby od využití pro osobní potřebu až po tehdy zakázané soukromé podnikání za účelem obohacení. Zde se již pachatel dopustil výše uvedeného trestného činu v souběhu s trestným činem Nedovoleného podnikání dle § 118 tr.zák. v tehdy platném znění. Charakteristické pro trestný čin dle § 133 tr.zák. v tehdy platném znění byla však charakteristická vysoká latence tohoto druhu počítačové kriminality způsobená zejména vztahem občanů k „společnému, socialistickému vlastnictví". Novelou tr.zák. č. 175/1990 Sb. byl trestný čin podle § 133 z tr.zák. vypuštěn a krádeže počítačového času jsou od té doby kvalifikovány jako neoprávněné užívání cizí věci[95].

S příchodem internetu došlo i u zneužívání počítačového času k určitému vývoji. V souvislosti s internetem tak můžeme krádež strojového času dělit na dvě základní formy:

4.2.1 Vnitřní forma

Ta vychází z historické podoby tohoto jednání a je páchána typicky v pracovněprávním vztahu. Tato forma spočívá ve využívání svěřeného počítače s internetovým připojením

---

[93] Taktéž počítačového času.

[94] Sálové počítače byly prvním typem počítače v dnešním slova smyslu. Vyskytovaly se zejména ve výzkumných pracovištích a sálové se nazývají proto, že z důvodu menšího stupně rozvoje miniaturizace měly tyto počítače obrovské rozměry zabírající celé místnosti.

[95] Blíže v kapitole Trestní odpovědnost této hlavy Zvláštní části.

v rozporu s pokyny zaměstnavatele k soukromým účelům. Může se tak dít častým prohlížením stránek v pracovní době, využíváním zaplaceného internetového telefonování pro osobní potřebu, využívání zaměstnavatelem předplacených internetových služeb (webových serverů), vyřizování soukromé e-mailové korespondence v pracovní době, návštěvou placených pornografických stránek, stahování velkoobjemových souborů apod.

Prevalence této formy je vysoká, můžeme s jistotou tvrdit, že je to zdaleka nejčastěji páchaná forma internetové kriminality.[96] Je taktéž zřejmé, že tato forma je stižena velmi vysokou latencí. Ta vychází z historického vývoje krádeže strojového času (viz výše) a je zvýrazněna skutečností, že nehmotný charakter počítačového času vyvolává v pachatelích (a někdy i u orgánů činných v trestním řízení) pocit, že vlastně nic ukradeno nebylo.

K zamezení této kriminality má daleko vyšší význam prevence, než následná represe. Zaměstnavatel jako nejčastější poškozený z této trestné činnosti má v dnešní době mnoho efektivních prostředků, jak této činnosti zabránit. Mezi ně náleží zajištění tzv. supervizora. Dalším prostředkem jsou různé softwarové nástroje, které dávají zaměstnavateli možnost kontrolovat nežádoucí vstupy do www sítě, popř. omezit jejich rozsah. Toto řešení se však v některých případech může zdát až přehnané. Účelným se taktéž prokázalo ve velkých pracovních organizacích vyčlenit zaměstnanci určitý čas, který může věnovat např. „brouzdání po internetu". Takový bonus pro zaměstnance má navíc i jistou výhodu pro zaměstnavatele, neboť si tak zaměstnanec zvyšuje svou počítačovou (internetovou) gramotnost, a tedy i svojí kvalifikaci.

4.2.2 Vnější forma

Vnější forma krádeže počítačového času má dvě základní podoby. První z nich většinou bývá součástí hackerského jednání a projevuje se např. získáním kontroly nad počítačem cizí osoby nebo převzetím identity jiného[97].

Druhá varianta bývá obvykle označována jako krádež konektivity. Konektivita je vyjádřením schopnosti připojit se k síti internet a charakteristika tohoto připojení. Deliktní jednání zde spočívá v jakémsi parazitování na připojení jiného. K tomu pak slouží jednak hardwarové a jednak softwarové prostředky.

Nejčastějším případem krádeží konektivity je neoprávněné připojení se k internetu skrze cizí neveřejné Wi-Fi sítě. Tolerance společnosti k tomuto jednání je v České republice obrovská. Obecně totiž u nás panuje představa, že pokud někdo nevyužívá pro přístup do sítě šifrování, umožňuje, aby se „po právu" připojily i cizí osoby, a tudíž že se vlastně nemůže nic stát. Toto vnímání je však mylné. Nejlépe to vystihuje paralela s reálným životem. Zřejmě každý bude souhlasit, že pokud někdo ponechá nezamčené dveře od automobilu, jistě nebude srozuměn s tím, aby si ho někdo „půjčil", ujel s ním třeba 200 km a následně ho opět vrátil na stejné místo. U krádeže konektivity však k podobnému nazírání dochází.

---

[96] nezužujeme-li tento pojem pouze na trestnou činnost, ale zahrnujeme-li sem i přestupky a jiné správní delikty

[97] V konkrétních podrobnostech hackerského jednání a jeho trestní odpovědnosti odkazuji na výklad v hlavě 2 Hackerství

I zde ovšem platí, že nejlepší obranou proti krádežím konektivity je její prevence. K zamezení drtivé většině těchto jednání by bohatě postačovalo, kdyby oprávnění uživatelé přístup k tzv. přístupovým bodům (Access Points) šifrovali.

Jiný způsob krádeže konektivity bývá uskutečňován pomocí technických zařízení, kterými se pachatel hardwarově napojí na vysílač internetového připojení jiného uživatele. Rozdíl od prvního případu spočívá právě v prostředku ke spáchání trestného činu. V prvém případě se totiž používá prostředků softwarových (Accesse Points jsou vyhledány prostřednictvím oficiálního programu uloženého v počítači pachatele), v případě druhém se tak děje určitým hmotným technickým zařízením (obvykle podomácku vyrobeným, nicméně může být i sériově produkován), kterým se pachatel lidově řečeno napíchne na vysílač či přijímač legálního uživatele.

Oba dva případy se také od sebe liší různou délkou trvání trestného činu. Softwarová krádež konektivity je většinou dočasná, nedochází k trvalému odnětí i třeba části konektivity, ta je vrácena už jen při vypnutí počítače pachatele. Nelze proto mluvit o krádeži v trestněprávním slova smyslu, ale spíše o neoprávněném užívání cizí věci. Oproti tomu u hardwarové varianty je odnětí konektivity (či její části) oprávněnému uživateli většinou trvalé a je ukončeno pouze, pokud někdo technické zařízení k parazitování nalezne, což se děje většinou náhodou, např. při údržbě či opravách. V tomto případě můžeme již mluvit o krádeži, případně poškození a zneužití záznamu na nosiči informací[98].

4.3 Trestní odpovědnost

4.3.1 Nebezpečnost činu pro společnost

Jako u mnoha jiných druhů internetové kriminality bude i v případě zneužívání počítačového času v souvislosti s internetem nebezpečnost činu pro společnost významným korektivem pro určení, zda byla naplněna materiální stránka trestného činu a vznikla trestní odpovědnost pachatele. To platí zejména u vnitřní formy krádeže strojového času, neboť se zde bude uplatňovat zásada subsidiarity trestního stíhání vzhledem k tomu, že pachatel tohoto deliktu bude často již dostatečně potrestán soukromoprávní „sankcí" jako okamžitým zrušením pracovního poměru či povinností nahradit zaměstnavateli jím způsobenou škodu.

Tak například v jedné z mála kauz řešených českou justicí (jednalo se však o pracovněprávní spor)[99] došly postupně soudy všech instancí k názoru, že žalovaný v daném případě nemohl okamžitě zrušit pracovní poměr s žalobkyní proto, že zaměstnankyně porušila povinnost vyplývající z právních předpisů vztahujících se k jí vykonávané práci zvlášť hrubým způsobem, když umožnila v pracovní době svému synovi přístup a hraní na počítači zaměstnavatele internetové hry. I když jednání žalobkyně znamenalo závažné porušení pracovní kázně, nebylo dle soudu natolik významné, aby splnilo podmínku porušení pracovních povinností zvláště hrubým způsobem. Je zřejmé, že v tomto případě bychom

---

[98] viz dále

[99] Sp.zn.: 21 Cdo 84/2006

nemohli dovodit stupeň nebezpečnosti pro společnost vyšší než nepatrný, a tedy k naplnění materiální stránky trestného činu nedošlo.

V jiném případě vnitřní krádeže počítačového času řešeném ve Spolkové republice Německo Spolkový pracovní soud (Bundesarbeitsgericht) v Erfurtu svým rozsudkem č. 2 AZR 581/04 ze dne 7.7.2005 rozhodl, že prohlížení placených pornografických stránek v pracovní době na počítači zaměstnavatele je důvodem k okamžitému zrušení pracovního poměru. Při hodnocení, zda by v takovém případě byla naplněna i materiální stránka trestného činu a jednání pachatele by bylo možno kvalifikovat jako trestný čin, je nutné zvážit více aspektů. Určujícím dle mého názoru je jednak výše škody na straně zaměstnavatele a dále jaký cíl jednání mělo, zda pouze „osobní potěšení", či zda bylo činěno k tvorbě určitého hospodářského prospěch, např. podnikání. Dle mého názoru tak ani v posuzovaném německém případě nebyl stupeň společenské nebezpečnosti takový, aby zakládal trestní odpovědnost pachatele, i když jistě o něco vyšší než v popsané české kauze.

U krádeže konektivity bude určujícím kritériem společenské nebezpečnosti jednak doba trvání trestné činnosti a jednak opět účel aktivit pachatele. Proto bude hardwarová krádež konektivity většinou naplňovat materiální znaky trestného činu. U softwarové krádeže bude nutno posuzovat jednak délku a četnost „dílčích krádeží" a dále zdali bylo připojení např. poskytnuto dalším uživatelům, zejména za úplatu.

Česká trestní judikatura zná i jeden případ krádeže konektivity z poměrně nedávné doby. V této věci rozhodoval i Nejvyšší soud ČR (sp.zn.: 7 Tdo 64/2005), když odmítl dovolání obviněného proti odsuzujícímu rozsudku soudu 1. a 2. instance. Pachatel se měl dopustit trestného činu Poškození a zneužití záznamu na nosiči informací podle § 257a odst. 1 písm. a), c) tr. zák. a byl odsouzen k podmíněnému trestu odnětí svobody na šest měsíců se zkušební dobou stanovenou na osmnáct měsíců. Jeho skutek dle zjištění Obvodního soudu pro Prahu 4 spočíval v tom, že „obviněný v době od 1. 2. 2003 do 27. 2. 2003 prostřednictvím technického zařízení umístěného na nemovitosti v P., neoprávněně užíval IP adresu jednoho z klientů obchodní společnosti P. S., s. r. o., k získávání a užívání informací z internetové sítě a tímto jednáním způsobil obchodní společnosti P. S., s. r. o., škodu ve výši 145.731,- Kč."[100]

4.3.2 Trestněprávní kvalifikace

4.3.2.1 Vnitřní forma zneužívání počítačového času

Při vnitřní formě krádeže strojového času (zneužívání internetového připojení zaměstnancem) bývá nejčastěji naplněna základní skutková podstata trestného činu Neoprávněného užívání cizí věci dle § 249 odst. 1 alinea 2 tr.zák.:

§ 249

Neoprávněné užívání cizí věci

---

[100] Odvolací soud později výrok o náhradě škody zrušil a společnost byla se svým nárokem odkázána na řízení ve věcech občanskoprávních.

(1) Kdo se zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu jich přechodně užívat, nebo
kdo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takových věcí, které mu byly svěřeny, přechodně užívá, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 značnou škodu nebo jiný zvlášť závažný následek.

Tento trestný čin je systematicky zařazen mezi trestné činy proti majetku do Hlavy deváté Zvláštní části trestního zákona.

Objektem tohoto trestného činu je výkon některých oprávnění vlastníka, zejména právo věc užívat (ius utendi), v konkrétním případě je to pak zájem na tom, aby vlastník (zaměstnavatel) mohl svobodně rozhodovat o využití svého počítače a internetového připojení při jeho užívání zaměstnancem.

Objektivní stránka spočívá v neoprávněném přechodném užívání cizí věci, která je pachateli svěřena, a způsobení škody nikoliv malé tímto jednáním. Škodou nikoliv malou se dle § 89 odst. 11 tr.zák. rozumí škoda ve výši alespoň 25.000,- Kč. Tr.zák. tak vyjadřuje daleko nižší typovou nebezpečnost trestného činu spočívající v přechodném neoprávněném užívání svěřené věci (počítače a internetu), tím, že pro naplnění skutkové podstaty tohoto trestného činu vyžaduje způsobení škody nikoli malé.

Subjektem je v drtivé většině případů zaměstnanec. Po subjektivní stránce je vyžadován úmysl, který musí zahrnovat i způsobení škody nikoliv malé.

K naplnění kvalifikované skutkové podstaty TČ Neoprávněného užívání věci bude třeba způsobit značnou škodu (tj. minimálně v hodnotě 500.000,- Kč - § 89 odst. 11 tr.zák.) nebo jiný zvlášť závažný následek.

Z výše uvedeného tedy plyne, že vnitřní krádež počítačového času v souvislosti s internetem bude trestná jen v ojedinělých případech, např. když bude zaměstnanec využívat svěřený počítač a připojení k aktivitám, které jsou konkurenční k předmětu činností zaměstnavatele, či bude ve velkém rozsahu navštěvovat pro soukromé účely internetové služby placené zaměstnavatelem.

4.3.2.2 Krádež konektivity

Při krádeži konektivity bývá její trestní kvalifikace obtížnější, než je tomu v případě vnitřní krádeže počítačového času. Bude třeba odlišit ty případy, kdy jde pouze o připojení se k cizí nešifrované síti bez učinění zásahu do technického nebo programového vybavení počítače nebo telekomunikačního zařízení (vysílač a přijímač Wi-Fi) a kdy k takovému zásahu dochází (typicky u hardwarové krádeže konektivity, k takovému zásahu však může docházet i softwarově).

V případě, že k tomuto zásahu nedojde, můžeme kvalifikovat jednání krádeže konektivity buď jako TČ Neoprávněného užívání cizí věci dle § 249 odst. 1 alinea 1 tr.zák. (a to pokud se jedná pouze o krátkodobé jednání)[101], nebo jako Krádež dle § 247 odst. 1 písm. a) tr.zák.:

§ 247

Krádež

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a
a) způsobí tak škodu nikoli nepatrnou,
b) čin spáchá vloupáním,
c) bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí,
d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo
e) byl za takový čin v posledních třech letech odsouzen nebo potrestán, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu nikoli malou.

(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) způsobí-li takovým činem značnou škodu nebo jiný zvlášť závažný následek.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Jak vyplývá ze znění § 249 odst. 1 alinea 1 tr.zák., musí k naplnění skutkové podstaty být krátkodobě odcizena movitá věc nikoli malé hodnoty, tzn. o hodnotě minimálně 25.000,- Kč. Vzhledem k tomu, že si lze jen těžko představit, že by připojení k internetu jen po krátkou dobu mělo cenu 25.000,- Kč, je naplnění této skutkové podstaty při krádeži konektivity prakticky vyloučeno, přichází tak pouze v úvahu odpovědnost za přestupek, což také odpovídá míře škodlivosti tohoto jednání pro společnost.

Jiná je situace u zmiňované krádeže. V tomto případě dochází k dlouhodobému využívání konektivity či její části, čímž při dlouhodobějším využívání je jistě možné způsobit škodu nikoli nepatrnou, tedy dle § 89 odst. 1 tr.zák. škodu alespoň 5.000,- Kč, a to zejména pokud oprávněný přijde v důsledku pachatelova jednání o připojení k internetu zcela (např. ztráta zakázek, které jsou sjednávány e-mailovou poštou, nemožnost internetového telefonování, atd.)

Otázku, zda konektivita může vůbec být předmětem krádeže, lze zodpovědět interpretací § 89 odst. 13 věta 1, který stanoví, že věcí se rozumí i ovladatelná přírodní síla. Trestněprávní

[101] znění viz výše

nauka tak dovozuje, že věcí je i elektrická energie, parní energie, atd.[102] Vzhledem k tomu, že připojení k internetu je vlastně datový tok mezi koncovými zařízeními, je třeba i internetové připojení považovat za věc v právním slova smyslu, podobně jako teplo, chlad, elektřinu, atd.

Objektem krádeže je vlastnictví věci (internetového připojení), objektivní stránka zde spočívá v tom, že se pachatel zmocní cizí věci jednáním uvedeným výše a způsobí tak škodu nikoli nepatrnou. Subjektem může být kdokoliv a vyžaduje se úmyslné zavinění.

V případě krádeže konektivity spolu s provedeným zásahem do počítače či telekomunikačního zařízení pak toto jednání lze kvalifikovat jako TČ Poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. c) tr.zák.[103]

V daném případě, při naplnění obou skutkových podstat, se může jednat i o jednočinný souběh trestného činu krádeže a trestného činu poškození a zneužití záznamu na nosiči informací. Tyto dva trestné činy totiž postihují jiný objekt. V prvém případě je to vlastnictví konektivity, resp. ochrana před omezením nebo zbavením internetového připojení. V druhém případě je to ochrana počítače či telekomunikačního zařízení. Vztah speciality je proto zde dle mého názoru vyloučen.

4.4 Závěr

Zneužívání počítačového času v souvislosti s internetem a krádeže konektivity jsou, ač málo diskutované, v naší společnosti poměrně častým jevem, který se značně může lišit co do společenské nebezpečnosti. Případy tzv. vnitřního zneužívání počítačového času nejsou povětšinou společensky nebezpečné natolik, aby byly splněny podmínky trestní odpovědnosti, a většinou mohou být postižitelné nanejvýš jako přestupky. V případech dlouhodobých krádeží konektivity jsou tyto více nebezpečné a dají se přirovnat ke krádežím v materiálním světě (ostatně jsou i tak kvalifikována). Nejnebezpečnější formy jsou takové, kdy dochází k organizovaným krádežím internetového připojení, které je dále za úplatu sdíleno a pachatel (případně pachatelé) z nich může mít nemalé zisky.

---

[102] např. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 681

[103] znění a podrobnosti o tomto trestném činu viz hlava 2 Hackerství

5. Šíření a zpřístupňování pornografie na internetu

5.1 Úvod

Pornografie jako společenský jev je stará, dalo by se říci, jako lidstvo samo, neboť lidé byli vždy fascinováni vlastní sexualitou. Bývala součástí náboženských rituálů a praktik popřípadě uměleckých znázornění. Jelikož předmětem této práce není kriminologická a trestněprávní analýza pornografické kriminality jako celku, ale rozbor internetové kriminality, bude se tato hlava krátce zabývat zejména těmi aspekty pornografie, které jsou podmíněny právě internetem, a jejichž sankcionováním se trestní právo zabývá.

5.2 Vymezení pojmu pornografické dílo

Pornografické dílo není u nás legálně definováno a ani návrh nového trestního zákona takovou definici neobsahuje, ač je v důvodové zprávě k tomuto zákonu uvedena[104]. Dle usnesení Ústavního soudu sp.zn.: IV.ÚS 606/03, U 23/33 SbNU 453 ze dne 19.04.2004 je pornografickým dílem *„jakákoliv věc, pokud uráží způsobem, který lze stěží akceptovat, cit pro sexuální slušnost. Pornografické dílo může u normální osoby vyvolávat sexuální vzrušení, vedle toho však může tuto osobu sexuálně znechucovat či odpuzovat. Test pornografické povahy díla, který by měl být aplikován obecným soudem, spočívá na posouzení, zda celkový dojem díla způsobuje morální pohoršení osobě s běžným cítěním*". Tato definice založená zejména na morálních aspektech (vzbuzení morálního pohoršení), plně koresponduje s podstatou chráněného zájmu společnosti v případě postihu pornografie, tj. veřejné morálky. Tato definice, vzhledem k posunu obsahu obecné morálky v čase (to, co je obecně považováno za morální, se v čase vyvíjí), tak může přetrvat a platit i do budoucna.

Oproti definici Ústavního soudu používá slovenský trestní zákon definici pornografického díla poněkud jinou, která není tak striktně vázána na obecné pojetí morálky (§ 132 odst. 2 slovenského trestního zákona): „Pornografií se pro účely tohoto zákona rozumí zobrazení soulože, jiného způsobu pohlavního styku anebo jiného obdobného sexuálního styku anebo zobrazení obnažených pohlavních orgánů směřující k vyvolání sexuálního uspokojení jiné osoby." Podobně se k tomuto vyjadřuje i česká trestněprávní nauka[105].

Samotné zobrazení nahého lidského těla není pornografie. O pornografickém charakteru pak musí rozhodovat obsah celého díla, tedy objektivní celková tendence, nikoli výseč, úryvek, tedy část celku. Nepochybně bude také záležet na povaze díla a způsobu jeho použití. Předměty určené k vědeckým, uměleckým, osvětovým cílům nelze považovat za pornografická díla (např. schématické znázornění pohlavního ústrojí pro výukové účely).[106]

---

[104] viz důvodová zpráva k vládnímu návrhu nového trestního zákona

[105] Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 600, kde je pornografické dílo definováno jako: „takové dílo, jehož jediným účelem je vyvolat (zvyšovat) sexuální vzrušení."

[106] tamtéž

Co se týká kriminologického nazírání na téma pornografie, je třeba si uvědomit, že ne vždy je pornografie vnímána jako společensky nebezpečný jev. Existují různé praktiky a stupně pornografie (od erotických děl a tzv. lehkého porna reprezentovaných obrázky a texty, někdy i videem, neukazující přímo soulož a jiný sexuální styk, přes „hardcore" zobrazující pohlavní styk v nejrůznějších polohách (někdy i počtech osob) až po extrémně tvrdou pornografii, do které jednoznačně patří všechny druhy dětské pornografie, sadistické a sadomasochistické praktiky, nekrofilie, zoofilie, aj. Všechny tyto projevy se v prostředí internetu vyskytují a je k nim více či méně možný přístup.

Při kriminalizaci pornografie je však nutné zvážit i některá sexuologická hlediska. Je totiž obecně známo, že pornografie obvykle uvolňuje sexuální frustraci jedinců, obzvláště pak deviantních, což může znamenat snížení výskytu sexuálně motivovaných trestných činů ve skutečnosti. Toto nazírání však nemůže ospravedlnit výrobu a šíření dětských či sadistických pornografických děl.

5.3 Typy jednání v prostředí internetu

5.3.1 Šíření zvrácených praktik

V prostředí sítě internet se můžeme setkat se dvojím typem kriminálních jednání v souvislosti s pornografií. Prvním z nich je šíření zakázaných extrémních až zvrácených praktik, resp. jejich zpřístupňování a prodej. Pachatelé tedy dílo ukazující tyto extrémní praktiky, které si obstarali jakýmkoliv způsobem (výrobou, koupí, neoprávněným rozmnožením, atd.), umístí na webový server, nabízí na svých stránkách k prodeji popř. k stažení nebo je sdílí v peer to peer sítích.

Internet tak umožňuje nevídanou přístupnost těchto zvrácených praktik, když podle některých studií[107] vzrostl počet vyobrazení dětské pornografie dostupných na internetu o 1.700 %! Pornografie, ať už dětská či obsahující jiné bizardní praktiky už tak, na rozdíl od dob éry bez internetu, není pouze věcí a aktivitou pedofilů a jiných deviantů, ale stala se velice výnosným byznysem, jež je často ovládán organizovaným zločinem.[108]

Boj proti této kriminalitě velice stěžuje (stejně jako u porušování autorských práv) mezinárodní charakter internetu umožňující uložit pornografický materiál kdekoliv na světě. Zabránit sdílení takovýchto pornografických děl v peer to peer sítích je taktéž nemožné. Jediným východiskem z tohoto problému tak je prevence a represe samotné výroby

---

107

http://www.ncmec.org/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2064 "CHILD PORN AMONG FASTEST GROWING INTERNET BUSINESSES". National Center for Missing and Exploited Children, USA (2005-08-05). Zobrazeno 19.6.2008, 19:18

108 http://www.parade.com/articles/editions/2006/edition_02-19-2006/Andrew_Vachss, zobrazeno 19.6.2008, 20:15

zvrácené pornografie, neboť snahy o omezení šíření prostřednictvím internetu se prozatím ukázaly jako žalostně neúspěšné.

Se zajímavým projektem omezení dětské pornografie na internetu přišla americká společnost Google, Inc., která poskytla National Centre for Missing and Exploited Children (Národní centrum pro ztracené a zneužívané děti) technologii sloužící k rychlému a efektivnímu vyhledávání serverů s tématikou dětské pornografie a dále usnadňuje práci pracovníků centra, kteří mají za úkol procházet statisíce fotografií a dávat k sobě stejné nebo podobné za účelem identifikace obětí zneužívání.

5.3.2 Zpřístupňování pornografie dětem a mladistvím

Druhým případem kriminálních aktivit na internetu je zpřístupňování pornografických materiálů dětem. Právě tento druh jednání je z pohledu kriminologie v současné době nejvíce kontroverzní. Není sporu o tom, že zpřístupňování pornografie dětem je jevem společensky značně škodlivým. Pornografie může (obzvláště u tvrdších forem) narušit mravní vývoj nedospělého jedince. Problematické však je, že i při veškeré snaze nelze izolovaně dětem omezit přístup k pornografickým dílům dostupných na internetu. Jakékoliv umístění pornografického díla na internetu (ať už na serveru či sdílením) pak splňuje podmínku kriminalizovaného zpřístupňování pornografie osobám mladším osmnácti let. Nabízí se tak ovšem otázka, zdali je správné a spravedlivé, pokud společnost aprobuje jednání spočívající ve výrobě a neinternetovou distribuci pornografických děl (nikoliv extrémních praktik – viz výše), ale zároveň považuje za trestnou distribuci prostřednictvím internetu.

Osobně nevnímám jako velký rozdíl mezi tzv. erotickými filmy vysílanými v televizi na některých kanálech po desáté hodině večerní, které zobrazují celý pohlavní styk (a to i lesbický, polygamní, atd.) krom samotného detailního pohledu na „průnik" pohlavních orgánů aktérů, a podobnou produkci průnik zobrazující, pokud neukazují praktiky obecně vnímané jako perverzní. Je dle mého názoru zbytečné si vnucovat představu, že například dvanáctileté dítě nepochopí, co se v erotickém filmu skutečně odehrává. Stejně tak je zřejmé, že dvanáctileté dítě bude občas v dobu vysílání takového pořadu vzhůru. Jiná je samozřejmě situace u dětí daleko mladších, těm by nemělo být umožněno přístup k takovým materiálům za žádnou cenu.

Na tomto místě je důležité se taktéž zmínit o tom, že drtivá většina pornografických[109] děl na internetu není zpřístupněna za účelem jejich zhlédnutí dětmi. Na rozdíl od serverů poskytujících např. neoprávněně hudbu či odkazy na tyto servery[110] stránky věnované pornografii, i když jsou zde taktéž umístěny reklamy, týkají se buď určitých sexuálních pomůcek, nebo např. různých preparátů na potenci, které samozřejmě primárně určené dětem nejsou. Hlavní příjem z těchto serverů je však z prodeje samotných pornografických

[109] dále v tomto oddíle ve významu pornografie bez zvrácených praktik

[110] viz hlava 1 Zvláštní části

děl, který se uskutečňuje výhradně elektronickými (internetovými) platebními kartami, ke kterým děti nemají obvykle přístup.[111]

Dle mého názoru by neměla prevence zpřístupňování pornografických děl dětem být uskutečňována tím, že budou kriminalizovány šíření či obecně dostupnost pornografického díla na internetu jako takové (opak platí v případě záměrného zpřístupnění), ale tím, že rodiče, případně jiné osoby zodpovědné za výchovu jedince budou činit dostatečná opatření k zamezení přístupu dětí k takovým dílům (např. omezením rozsahu stránek, které dítě navštěvuje, kontrolou celkového času stráveného dítětem na internetu, výchovou, atd.). Tento náhled na prevenci je odrazem jednak ve velké míře tolerance sexu, erotiky i pornografie v naší společnosti (zřejmě z důvodu historicky podmíněného odmítání ortodoxních církevních předsudků a prudérií)[112] a dále v obecné tendenci přechodu od kolektivního pojímání ochrany společnosti přežité z minulé doby k požadavku individuální odpovědnosti osob (resp. v tomto případě rodičů za mravní vývoj svých dětí).

5.4 Trestněprávní aspekty

5.4.1 Společenská nebezpečnost

Jak plyne z výše uvedeného výkladu, je pojímání společenské nebezpečnosti třeba pojímat různě u odlišných typů jednání vztahujících se k pornografii na internetu. Jako spolehlivě nejnebezpečnější musí být pokládána jakákoliv pornografie zobrazující dítě. I zde je však možné uvažovat o výjimkách. Jedním z příkladů je animovaná dětská pornografie, jejímž typickým zástupcem je japonský Lolicon (Roricon, anime...). V těchto případech totiž nedochází při výrobě těchto pornografických děl k zneužívání dětí, což je hlavní důvod kriminalizace dětské pornografie. Jelikož pedofilie jako taková nelze ani vyléčit ani potlačit, je zcela zásadní, aby bylo zamezeno jejím projevům (zejména sadistickým, tzv. nepravým pedofilům[113]) v reálném světě, tedy sexuálnímu zneužívání dětí a dalším sexuálně motivovaným útokům. Jak je zmíněno výše, některé studie uvádějí, že stíhání produkce animované pornografie nezvyšuje prevalenci sexuálních deliktů spáchaných na dětech, popř. tvrdí opak.[114] V Evropě se obvykle animovaná dětská pornografie posuzuje stejně jako reálné zneužívání dětí a je trestná. Podobně k ní přistupuje i návrh nového trestního zákona.[115]

---

[111] podobně probíhá i nákup zboží, které jsou předmětem reklam umístěných na pornografických serverech.

[112] Musil, S.: Počítačová kriminalita. IKSP, Praha 2000, str. 276

[113] blíže k problematice pedofilního pachatele např. Čírtková, L.: Forenzní psychologie. Nakl. Aleš Čeněk, s.r.o., Plzeň 2004, str. 185 a násl.

[114] Diamond, M., Uchiyama, A.: Pornography, Rape and Sex Crimes in Japan, International Journal of Law and Psychiatry 22(1): 1-22. 1999

[115] blíže v části III Úvahy de lege lata a de lege ferenda

5.4.2 Trestněprávní kvalifikace zpřístupňování pornografie dětem

Obě kriminalizované formy jednání uvedených v předcházejícím oddíle (tedy distribuce zvrácené pornografie a zpřístupňování pornografie dětem prostřednictvím internetu) je v českém trestním právu kvalifikováno jako trestný čin Šíření pornografie dle § 205 odst.1, 2, 3, 4 tr.zák.:

§ 205

Šíření pornografie

(1) Kdo pornografické dílo písemné, fotografické, filmové, počítačové, elektronické nebo jiné takové dílo
a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo
b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje,
bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo,
a) které zobrazuje nebo jinak využívá dítě,
b) v němž se zobrazuje násilí či neúcta k člověku, nebo
c) které zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem,
anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) jako člen organizované skupiny,
b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo
c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) jako člen organizované skupiny působící ve více státech, nebo
b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

Tento trestný čin byl zásadně pozměněn novelou trestního zákona č. 271/2007 (dříve se tento trestný čin nazýval Ohrožování mravnosti a dále byly zavedeny speciální skutkové podstaty Přechovávání dětské pornografie dle § 205a a Zneužití dítěte k výrobě pornografie dle § 205b). Tato novela přinesla zejména značné zpřísnění trestní sankce (dříve bylo jednání naplňující skutkovou podstatu odst. 2 cit. ustanovení sankcionováno maximálně jedním rokem trestu odnětí svobody. Tato novela tak navazuje na Opční protokol k Úmluvě o právech dítěte proti prodeji dětí, dětské prostituci a dětské pornografie ze dne 25. května 2000 a na Úmluvu o počítačové kriminalitě, Budapešť, ze dne 23. listopadu 2001 (článek 9).

Dle mého názoru však není v ustanovení tohoto trestného činu (zejména pak ustanovení § 205 odst. 3 písm. b) tr.zák., které se týká právě internetu) dostatečně rozlišena typová nebezpečnost jednotlivých sankcionovaných jednání zejména v tom, že stejnou trestní sankcí je postiženo zpřístupnění dětské pornografie v internetovém prostředí jako zpřístupnění pornografie nezvrácené, neboť zpřístupnění internetem je logicky pornografie zpřístupněna i dětem.

K pojmu pornografické dílo viz výše. Objektem tohoto trestného činu je mravní výchova mládeže, lidská důstojnost a ochrana psychické integrity jedince, obecně také občanské soužití.

Objektivní stránka spočívá v jednání uvedených v kapitole 5.3 této hlavy Zvláštní části. Pachatelem může být kdokoli.

Subjektivní stránka vyžaduje zavinění úmyslné. Problematické bude zejména stanovit formu zavinění v případě zpřístupnění pornografie mladistvému prostřednictvím internetu. Mnoho provozovatelů serverů pornografií se zabývajících totiž zpřístupňovat pornografii mladistvým nechce a ani s tím nejsou srozuměni. Jelikož ale nemůžou servery ověřovat totožnost koncových uživatelů, uchylují se pouze k „šalamounskému řešení", a to že před vstupem na stránky s explicitně pornografickým materiálem se nejdříve zobrazí stránka s informací, že další obsah stránek je určen pouze osobám starším osmnácti (případně 21 let), a tedy že odkliknutím tlačítka vstoupit uživatel prohlašuje, že zletilosti dosáhl[116]. Je zřejmé, že tato stránka neodradí „zvídavé" děti od vstupu, dle mého názoru však může mít toto řešení vliv na posouzení zavinění pachatele.

5.5 Závěr

Pornografie byla vždy fenoménem značně diskutovaným. Není se čemu divit, neboť vnímání míry škodlivosti pornografie pro společnost se značně liší u každé osoby. Autor této práce zastává spíše liberální názory ohledně kriminalizace pornografie, s výjimkou pornografie dětské a zvrácených forem či provozovaných praktik. Tyto formy by měly být trestné vždy, a to ať už jde o jejich výrobu, distribuci či sdílení prostřednictvím internetu. Nejpřísnější tresty by měly být ukládány v případě reálných dětských pornografických děl, neboť při jejich výrobě nedochází jen k ohrožení obecné morálky, ale často k závažnému zásahu do integrity osobnosti a narušení psychického vývoje dětí, které lze jen málokdy úspěšně napravit. Je na zvážení legislativců, zda by neměla být do budoucí právní úpravy zahrnuta i možnost trestu odnětí svobody nad deset let v případě, že k výrobě a obchodu s dětskou pornografií dochází v rámci organizovaného zločinu.

---

[116] ukázka viz příloha č. 5

III. část Úvahy de lege lata a de lege ferenda

1. Úvod

S bouřlivým rozvojem počítačů a počítačových sítí a následně i rozvojem internetové kriminality vznikla situace, kdy na některé nové jevy nebylo možno užít stávající právní úpravu. Právo ostatně nikdy nedokáže absolutně pružně reagovat na zásadnější společenské změny, vždy bude mezi společenskou změnou a jejím zobrazením v právu určitá prodleva. U počítačů a internetu je tomu tak doposud. Jako reakce na tuto situaci vznikl nový průřezový obor nazvaný počítačové právo a později tzv. informační právo, který se danou problematikou úžeji zabýval. V rámci vyskytujících se kriminálních jednání bylo určeno, na které lze i nadále použít ustanovení stávající právní úpravy, zejména s ohledem na dodržování zásady nullum crimen sine lege (scripta), a u kterých bude třeba do právní úpravy zahrnout nové skutkové podstaty, které by dostatečně reflektovaly nové typy kriminálních jednání související s internetem. Vzhledem k celosvětovému charakteru internetu pak i na mezinárodní scéně byly přijaty nové právní předpisy, které slouží k unifikaci postihu nejzávažnějších forem trestné činnosti související s internetem. Analýze všech těchto úrovní se bude věnovat právě tato závěrečná část práce, ovšem s přihlédnutím k možným úpravám daných institutů do budoucna (de lege ferenda).

2. Vnitrostátní úprava

2.1 Stávající úprava trestního zákona z pohledu internetové kriminality

Jelikož jsou trestné činy (až na výjimky jako je např. trestný čin upravený v zákoně na ochranu míru) v českém právním řádu kodifikované v jednom zákoníku, kterým je zákon č. 140/1961 Sb., Trestní zákon. Tento zákon prošel za dobu své existence bouřlivým vývojem, když přečkal i přerod ze socialistického právního systému, který jej i přes provedené změny poznamenal co do struktury a ideologických východisek, k systému založenému na demokratických hodnotách, tržní ekonomii a doktríně právního státu. Během posledních let byla snaha i do trestního zákona promítnout závazky vyplývající z mezinárodních smluv a našeho členství v Evropských strukturách (např. úprava extradice vlastních občanů na základě eurozatykače, promítnutí v podmínkách ukládání trestu vyhoštění, atd.).

Co se týče internetové kriminality, byly v trestním zákoně provedeny některé změny, které měly reagovat na rozvoj kybernetické kriminality. V případě některých jednání zákonodárce vložil do znění zákona nové trestné činy, v jiných například doplnil kvalifikované skutkové podstaty trestných činů o páchání jednání prostřednictvím „veřejně přístupné počítačové sítě" jako zvláště přitěžující okolnosti. V některých případech bylo usouzeno, že určitá jednání spadající pod internetovou kriminalitu nejsou ničím jiným, než jinak obvyklým trestným činem v reálném světě, a tak nebyla do úpravy promítnuta. Osobně jsem zastáncem spíše metody, kdy jsou na internetové delikty využity stávající skutkové podstaty, neboť je tak zamezeno přílišné právní kazuistice. Tak je tomu například u většiny internetových podvodných jednání jako např. Phishing, úvěrové a bankovní podvody aj. nebo u krádeže konektivity (viz výše)

2.1.1 Postih hackerství

Jiná je ovšem situace u trestných činů, kde internet (či jeho složka) je předmětem útoku. To platí zejména pro hackerství, které nemá svůj předobraz v reálném životě. I když mohou tato jednání naplňovat skutkové podstaty i jiných trestných činů, samotný akt útoku hackera žádná skutková podstata trestného činu do roku 1991 nepostihovala. Novela trestního zák. č. 557/1991 zavedla trestný čin Poškození a zneužití záznamu na nosiči informací dle § 257a tr.zák.[117]

Ve vztahu k internetu je zapotřebí si uvědomit, že platná úprava tohoto trestného činu byla do trestního zákona vložena v době, kdy v českém prostředí internet takřka nikdo neznal, ostatně v dnešní podobě (zejména webu) ani tehdy neexistoval. Překvapivě však tento paragraf přetrval v jen málo pozměněném znění až doposud. V průběhu času byl totiž přidán odst. 3, aby byla lépe postihnuta typová nebezpečnost činu pro společnost v případě spáchání škody velkého rozsahu, popř. zisku velkého rozsahu, a další změna už nevázala trestnost tohoto činu na skutečnost, že pachatel nemusí získat přístup k nosiči informací v úmyslu způsobit škodu či jinou újmu nebo získat neoprávněný prospěch (tak tomu je pokud pachatel získá přístup např. od zaměstnavatele a až po získání tohoto přístupu se rozhodne pro jednání uvedené v písm. a) – c) odst. 1 cit. ust.). Poslední změnou pak bylo doplnění výčtu zařízení v písm. c) cit. ust. o „jiné telekomunikační zařízení", aby mohl být postižitelný nejen zásah do počítačů, ale i dalších technických prostředků komunikace jako jsou telefonické a mobilní sítě, telefaxové sítě a zejména internetové sítě. Poslední dvě jmenované změny byly provedeny novelou trestního zákona č. 134/2002 s účinností od 1.7.2002 jako reakce (jak to u právních předpisů bývá se značným zpožděním) na rozmach internetové kriminality.

Skutková podstata trestného činu podle § 257a tr.zák. dovoluje postihovat většinu pro společnost nebezpečných jednání týkajících se hackerství a hardwarové krádeže konektivity, přesto však vývoj v oblasti počítačů a informatiky ukázal, že některé zjevně společensky škodlivé aktivity postihnout nedokáže. Jsou jimi zejména některé formy přípravy k samotnému trestnému činu dle § 257a tr.zák. Mezi tyto aktivity patří překonání bezpečnostních opatření k získání přístupu do počítače (nekalá kryptoanalýza), vytváření a distribuce programů či rozšiřování návodu k usnadnění získání přístupu a kontroly nad cizím počítačem, atd. Jelikož trestný čin dle § 257a tr.zák. není uveden v taxativním výčtu trestných činů uvedených v § 62 tr.zák. ani není horní hranice trestní sazby u tohoto trestného činu nejméně osm let, nepovažuje se tento trestný čin za zvlášť závažný trestný čin, a proto jeho příprava není trestná (§ 7 odst. 1, 2 in fine § 41 odst. 2 tr.zák.).

Zákonodárce taktéž u tohoto TČ dle mého názoru nedostatečně rozlišil typovou nebezpečnost různých jednání, která mohou naplnit skutkovou podstatu trestného činu. Toto ustanovení totiž trpí nedostatečným množstvím okolností podmiňujících použití vyšší trestní sazby a dále poměrně nízkou horní hranicí trestní sazby. Je tomu tak zřejmě proto, že donedávna ve společnosti panovala představa, že počítačová, resp. internetová trestná

[117] Znění je uvedeno v hlavě 2 Hackerství Zvláštní části

činnost se odehrává v jiném, nereálném světě, a proto i případný následek nemůže být závažný. Opak je však pravdou, v dnešní době lze pouze prostřednictvím počítače spáchat řadu velice nebezpečných činů (za vše hovoří kyberterorismus), jejichž náprava je často nemožná.

V neposlední řadě také toto ustanovení neumožňuje postih „odposlouchávání" elektromagnetického vyzařování z počítačového systému v rámci přenosu dat.

2.1.2 Postih porušování autorských práv

Jak je zevrubně vysvětleno v hlavě 1 Zvláštní části, je úprava trestního postihu porušování autorských práv řešena blanketní normou, která odkazuje na soukromoprávní úpravu autorských práv. Toto pojetí v sobě nese některá rizika. Nejvýznamnější z nich je určitá kolize s požadavkem principu právní jistoty zostřeného v trestním právu hmotném zásadou nullum crimen sine lege. Naplnění formálních znaků skutkové podstaty trestného činu dle § 152 tr.zák. bude tak splněno i u sebebanálnějších jednání a jediným korektivem trestní odpovědnosti tu bude posouzení nebezpečnosti činu pro společnost a splnění požadavku subsidiarity trestního postihu.

I zde zřejmě zákonodárce nereagoval na expanzi tohoto trestného činu v internetové síti a nevložil do tohoto paragrafu jako zvláště přitěžující okolnost spáchání TČ prostřednictvím veřejně přístupné počítačové sítě a v rámci organizované skupiny.

2.1.3 Úprava šíření pornografie

Úprava trestného činu Šíření pornografie podle § 205 tr.zák., ač v nedávné době novelizována (zřejmě jako reakce na nepřijetí návrhu nového trestního zákona, a tedy vzniklým problémem nedodržení závazků na ochranu dítěte vyplývající z mezinárodních a evropských norem), stále trpí některými nedostatky.

Asi nejdůležitějším je neodlišení dětské pornografie od ostatních druhů zvrácených pornografických děl a tedy nezdůraznění zvláštního zájmu na potírání tohoto druhu kriminality. Taktéž v nyní platné úpravě chybí legální definice pojmu pornografického díla, která by sjednotila výklad judikatury a doktríny ve směru definice pornografického díla předloženou Ústavním soudem ČR (viz hlava 5 Šíření a zpřístupňování pornografie na internetu Zvláštní části).

Co se týká zpřístupňování „nezvrácené" pornografie dětem v odst. 1 platné úpravy § 205 tr.zák., je na škodu, že při poslední novele nebyla zohledněna aktuální diskuse na téma snížení spodní hranice trestní odpovědnosti na 14 let (stejně jako hranice trestnosti pohlavního styku s osobou mladší 15 let) v tom smyslu, že namísto zákazu tohoto zpřístupnění do 18 let by tato hranice byla snížena na 17 či 16 let.

Stávající pojetí trestného činu dle § 205 nepočítá s trestní odpovědností za držení či přechovávání zvrácené pornografie. Z důvodu zmíněných v hlavě 5 Zvláštní části[118], avšak s přihlédnutím k prevenci výroby dětské pornografie, je třeba uvážit umožnění držby pouze „virtuální" dětské pornografie.

2.1.4 Úprava porušování tajemství dopravovaných zpráv

E-mail a jiné zasílání datových zpráv v dnešní době v mnohém plně nahrazuje „klasické" poštovní služby. Tento trend je ještě umocněn příchodem elektronického podpisu, který umožňuje např. zasílat podání státním úřadům a soudům pouze v elektronické podobě. Elektronické zprávy proto mohou mít stejnou důležitost, jako zprávy v listinné podobě. Je tedy důležité, aby byla i elektronickým (datovým) zprávám poskytována stejná ochrana trestním právem, jako je tomu v případě zpráv listinných. Trestněprávní ochranu e-mailovým zprávám je možné dovodit z ustanovení § 239 odst. 1 písm. b) tr.zák., když jako trestný čin Porušování tajemství dopravovaných zpráv je kvalifikován i případ úmyslného porušení tajemství zprávy podané telefonem, telegrafem nebo jiným takovým veřejným zařízením. Je pravděpodobné, že normotvůrce měl na mysli pod pojmem „ jiné takové veřejné zařízení" zejména Telefax, dálnopis či Postfax, Dle mého názoru však lze výklad tohoto pojmu rozšířit i na e-mailovou službu internetu. Opět však z hlediska právní jistoty a základních zásad trestního práva by bylo záhodno do výčtu zahrnout i pojem „veřejně přístupná počítačová síť" a dále rozšířit tuto ochranu na jakýkoli přenos dat.

2.2 Trestní zákon a internetová kriminalita de lege ferenda

Úvahy o budoucí právní úpravě trestání internetové kriminality jsou nyní zvláště aktuální vzhledem k návrhu nového trestního zákoníku. Tento návrh nebyl dosud Parlamentem ČR přijat a o jeho podobě se vedou vášnivé diskuse.

Nový trestní zákoník (dále také „nov.tr.zák." nebo „NTZ") totiž přináší mnoho změn, a to i v samotné podstatě definice trestného činu. Nov.tr.zák. zcela nově opouští od formálně materiálního pojetí trestného činu a přiklání se, podobně jako je tomu v Polsku, pouze k formálnímu pojetí. Jeho korektivem je jednak využívání procesních odklonů, aplikace zásady subsidiarity trestní represe a určení společenské škodlivosti jednání pachatele (§ 12 odst. 2 nov.tr.zák.)[119]

Tento zákoník taktéž reaguje na některé specifické projevy internetové kriminality a uvádí v soulad znění trestně právních norem s normami práva Evropských společenství a mezinárodních smluv[120]. Z ustanovení, která se týkají internetové kriminality lze zmínit zejména následující:

---

[118] saturace sexuálních potřeb devianta a snížení rizika fyzického sexuálně motivovaného útoku ve skutečnosti

[119] Blíže k tomu viz důvodová zpráva k návrhu nového trestního zákoníku.

[120] tamtéž

- Nová právní úprava ve výkladovém ustanovení § 115 písm. a) nov.tr.zák je výslovně uvedeno, že trestný čin je spáchán veřejně, pokud je spáchán veřejně přístupnou počítačovou sítí, na místo původního podřazení pod pojem „jiným podobně účinným způsobem, což je více v souladu s požadavkem právní jistoty.

- Zařízení a sítě elektronických komunikací jsou výslovně označeny v § 130 nov.tr.zák. jako obecně prospěšné zařízení.

- V § 180 NTZ upravující TČ porušování tajemství dopravovaných zpráv je poskytována ochrana i elektronickým zprávám a neveřejným přenosům počítačových dat včetně elektromagnetického vyzařování a dále pozměnění těchto dat osobou vykonávající komunikační činnosti

- § 181 NTZ upravuje nový trestný čin Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí, který postihuje porušení tajemství i dokumentů (včetně elektronických dat) uchovávaných v soukromí

- Trestný čin Neoprávněné opatření, padělání a pozměnění platebního prostředku nyní poskytuje ochranu taktéž elektronickým platebním prostředkům

- Ve více trestných činech bylo spáchání trestného činu veřejně přístupnou počítačovou sítí zavedeno jako okolnost použití vyšší trestní sazby, a to konkrétně u TČ Šíření pornografie (§ 188 odst. 3 písm. b) NTZ), TČ Výroba a jiné nakládání s dětskou pornografií (§ 189 odst. 3 písm. b) NTZ), TČ Šíření toxikomanie (§ 285 odst. 2 písm. c) NTZ), TČ Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 352 odst. 2 písm. b) NTZ), TČ Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 353 odst. 3 písm. a) NTZ), TČ Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka (§ 400 odst. 2 písm. a) NTZ) a další.

2.2.1 nová úprava postihu hackerství

Nejvýznamnější změnu, co se týče internetové kriminality, ovšem přináší ustanovení §§ 228 – 230 nov.tr.zák. V těchto paragrafech jsou upraveny trestné činy, které spadají v nyní platné úpravě pod trestný čin Poškození a zneužití záznamu na nosiči informací dle § 257a tr.zák., popř. postihují korespondující jednání přípravná či nedbalostní:

§ 228

Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3)Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo
b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4)Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) způsobí-li takovým činem značnou škodu,
c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,
d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5)Odnětím svobody na tři léta až osm let bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 229

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 180 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 228 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačového systému nebo jeho části,
bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 230

Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté
a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,
a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

K § 228 NTZ:

V odst. 1 cit. ust. je nově stanovena trestní odpovědnost již za získání neoprávněného přístupu k počítači překonáním bezpečnostních opatření, je tedy sankcionováno i takové jednání, které by dříve mělo charakter pouze přípravného jednání a z důvodů výše zmíněných nemohlo být posouzeno jako trestný čin. Toto ustanovení taktéž postihuje i tzv. Hackerství pro zábavu, jehož znakem není způsobení škody.

V odstavci druhém cit. ust. je upravena skutková podstata trestného činu, která je detailnějším rozpracováním původní skutkové podstaty § 257a tr.zák. Zákonodárce se zde, zřejmě ve snaze podchytit všechny možné varianty pachatelova jednání, dopouští jistého „legislativního pochybení", když skutková podstata vyhlíží poněkud hypertroficky, až kasuisticky. Některá postihovaná jednání jsou pak zbytečně zdvojena. Například v písm. b) tohoto odstavce by k dostatečné úpravě stačilo znění v tomto tvaru:
„b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně poškodí, změní, vymaže nebo jinak zničí." Zde vypuštěné formy jednání totiž nejsou ničím jiným než variantami forem uvedených a nejsou tudíž zapotřebí.

Ze stejného důvodu je dle mého názoru nadbytečné celé písm. c) odst. 2 cit. ust., neboť se jedná vždy o změnu informace.

Zbylé odstavce tohoto paragrafu pak obsahují obvyklé kvalifikované skutkové podstaty trestného činu dle § 228 NTZ.

K § 229 NTZ:

Tento trestný čin upravuje dříve často nepostižitelná přípravná jednání k TČ dle § 228 NTZ. Jsou jimi např. vytváření a distribuce programů či rozšiřování návodu k usnadnění získání

přístupu a kontroly nad cizím počítačem nebo nedovolená manipulace a uchovávání cizích hesel, přístupových kódů, postupů k jejich překonání, atd.

K § 230 NTZ:

Zákonodárce tímto trestným činem zavedl taktéž trestní odpovědnost za nedbalostní alternativu TČ podle § 228 NTZ, zřejmě jako reakci na skutečnost, že i tato nedbalostní forma jednání může znamenat rozsáhlé a těžko napravitelné škody a je tak společensky škodlivá. K trestnosti je třeba hrubé nedbalosti[121] a pachatel musí porušit svou zvláštní povinnost.

V souvislosti s touto novou úpravou postihu hackerství se ozývají mnohé kritiky, zejména ze strany IT specialistů, ale bohužel i některých právníků[122]. Ti totiž v nové úpravě spatřují kriminalizaci vědecké kryptoanalýzy a testování bezpečnosti počítačových systémů[123] (tzv. penetrační testování).

Tyto obavy jsou dle mého názoru nepodložené, neboť kritici této úpravy neberou v potaz ust. § 12 odst. 2 nov.tr.zák., který vyžaduje k trestní odpovědnosti pachatele splnění zásady subsidiarity trestní represe a zejména společenské škodlivosti činu. Je zřejmé, že vědecká kryptoanalýza, stejně jako penetrační testování dodavatelem na základě objednávky vlastníka testovaného informačního systému, společensky škodlivá není, ba naopak, a proto nemůže v těchto případech vzniknout trestní odpovědnost. U penetračního testování lze navíc nalézt podporu pro tento argument v § 30 NTZ, který stanoví, že svolení poškozeného je okolností vylučující protiprávnost činu. U Kryptoanalýzy pak lze dle § 31 NTZ dovodit také okolnost vylučující protiprávnost činu v podobě přípustného rizika.

Celkově lze říci, že nová úprava TČ dle §§ 228 – 230 NTZ je poměrně zdařilá (s výhradou výše uvedeného) a odráží ve své podstatě mnohá jednání hackerů, která jsou jistě škodlivá pro společnost, ale nelze je dle stávající úpravy stíhat.

2.2.2 „Staronová" úprava postihu autorských práv

Dle důvodové zprávy k novému zákoníku je úprava TČ Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 152 tr.zák. prakticky totožná s původním zněním trestního zákona. I když do textu základní skutkové podstaty § 268 nov.tr.zák. bylo přidáno (s ohledem na pouze formální pojetí trestného činu) pouze sousloví „závažným způsobem", úprava tohoto trestného činu není ve výsledku úplně podobná. Důvod tohoto rozdílu je však nutné hledat systematicky na úplně jiném místě NTZ, a to v ustanovení o právním omylu (§ 19 NTZ). Nový trestní zákoník totiž zcela diskontinuitně k předchozí, ale i historické úpravě, stanoví, že omyl o normách právních (pokud jejich

---

[121] Trestný čin je dle § 16 odst. 2 NTZ spáchán z hrubé nedbalosti, *jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.*

[122] např. článek: „Bude podle navrhované novely trestního zákona věda (kryptoanalýza) trestná?", http://www.itpravo.cz/index.shtml?x=694071, zobrazeno 9.6.2008, 20:14

[123] K vymezení těchto pojmů tamtéž.

s původním zněním trestního zákona. I když do textu základní skutkové podstaty § 268 nov.tr.zák. bylo přidáno (s ohledem na pouze formální pojetí trestného činu) pouze sousloví „závažným způsobem", úprava tohoto trestného činu není ve výsledku úplně podobná. Důvod tohoto rozdílu je však nutné hledat systematicky na úplně jiném místě NTZ, a to v ustanovení o právním omylu (§ 19 NTZ). Nový trestní zákoník totiž zcela diskontinuitně k předchozí, ale i historické úpravě, stanoví, že omyl o normách právních (pokud jejich znalost nebyla pachateli stanovena zvláštní povinností či nemohl-li pachatel protiprávnost činu rozpoznat bez zřejmých obtíží) nejenom že vylučuje úmyslné zavinění, ale dokonce zavinění jako takové, tedy i nedbalostní. Dle důvodové zprávy se toto ustanovení týká zejména trestných činů s blanketní skutkovou podstatou, kterým ovšem TČ podle § 268 NTZ je. Tímto, dle mého názoru zcela nevhodným ustanovením, je prolomena zásada ignoratia legis non excusat[124] a hrozí tak, že velkou většinu trestných činů týkající se porušování autorských práv nebude možno vůbec trestně stíhat. Pokud zákonodárce zamýšlel, aby nebyl trestně postižen pachatel jen proto, že nezná určité speciální ustanovení právního předpisu, na který blanketní norma také odkazuje a který není příliš v obecném povědomí, měl namísto blanketních norem použít standardní normy trestní, což by ostatně i lépe vyhovovalo požadavku právní jistoty.

3. Mezinárodní úprava ochrany před internetovou kriminalitou

Jelikož internetová kriminalita se neomezuje pouze na území jednoho státu, ale díky celosvětovému rozšíření má typicky mezinárodní charakter, je třeba i v nadnárodním měřítku upravit a sladit alespoň základy těch nejzávažnějších trestných činů. Mezi mezinárodními smlouvami upravujících počítačovou, ale hlavně i internetovou kriminalitu, má největší význam Úmluva o počítačové kriminalitě (dále také jen „úmluva"), sjednaná dne 23.11.2001 v Budapešti na půdě Rady Evropy, ve znění dodatkového protokolu ze dne 28.11.2003 ve Štrasburku o kriminalizaci jednání rasistické a xenofobní povahy spáchaných počítačovými systémy.

Podmínkou vstupu této úmluvy v platnost byla ratifikace úmluvy alespoň 5 smluvními stranami včetně tří členů Rady Evropy. Tato podmínka byla splněna 1.7.2004, kdy tato úmluva vstoupila v platnost. Dodatkový protokol vstoupil v platnost dne 1.3.2006. K dnešnímu dni podepsalo tuto smlouvu 55 států, z toho 23 ji již ratifikovalo.

Je smutnou realitou, že Česká republika, ač přistoupila k této úmluvě 9.2.2005, doposud nedokázala tuto mezinárodní smlouvu ratifikovat. K dodatkovému protokolu pak doposud vůbec nepřistoupila.

Smlouva samotná je tvořena preambulí a vlastním normativním textem smlouvy členěným do čtyř kapitol, ty pak na sekce, hlavy a jednotlivé články. Celkem úmluva obsahuje 48 článků.

V preambuli je vyjádřena obecná potřeba mezinárodní úpravy postihu kybernetické kriminality jako prostředku efektivní spolupráce mezi státy v boji proti počítačové kriminalitě,

---

[124] Neznalost zákona neomlouvá.

Kapitola II je nazvána jako opatření, která mají být přijata na národní úrovni („Measures to be taken at the national level"). Její první sekce se nazývá hmotné trestní právo a upravuje jednání, která by měla být národní úpravou postihována trestním právem. Jedná se o Neoprávněný přístup („Illegal access") – čl. 2, Nelegální zachycení přenosu počítačových dat („Illegal interception") – čl. 3, Neoprávněný zásah do počítačových dat („Data Interference") – čl. 4, Neoprávněný zásah do počítačového systému („System Interference") – čl. 5, Zneužití zařízení k páchání činů dle čl. 2 – 5 („Misuse of device") – čl. 6, Padělání počítačových dat („Computer related forgery") – čl. 7, Počítačový podvod („Computer related fraud") - čl. 8, trestné činy týkající se dětské pornografie („Offences related to child pornography") – čl. 9, přičemž pojem dětská pornografie zahrnuje i virtuální dětskou pornografii a ta pornografická díla, ve kterých sice účinkuje osoba starší 18 let, ale budí zdání či spíše vypadá, že je osobou mladší. Posledním kriminalizovaným jednáním je Porušování autorských práv a práv souvisejících („Offences related to infringements of copyright and related rights") – čl. 10.

Tato úmluva taktéž stanoví povinnost, aby smluvní strany zajistily trestnost jednání spočívajícím v účastenství na výše uvedených trestných činech a dále v jejich pokusu (čl. 11).

Úmluva taktéž zavádí trestní (popř. efektivní správní) odpovědnost právnických osob (čl. 12).

Druhá sekce úmluvy (čl. 14 – 21) upravuje procedurální otázky (aspekty efektivního trestního stíhání pachatelů), zejména způsoby získávání a obstarávání důkazů při respektování základních lidských práv, jako je uchování a získání uložených dat, sběr přenosových dat.

Třetí sekce úmluvy (čl. 22) je nazvána „Pravomoc" („Jurisdiction") a má zajišťovat, aby nenastala situace, kdy z důvodu rozdílné národní právní úpravy by nebyla jednání postihovaná touto smlouvou vůbec trestně stíhána.

Kapitola II úmluvy upravuje oblast justiční spolupráce. Výše uvedené trestné činy mají být stranami smlouvy považovány za extradiční (čl. 24) a smluvní strany si při stíhání počítačových trestných činů mají poskytovat nejširší možnou právní pomoc, stejně jako si vzájemně poskytovat podstatné informace spojené s kybernetickou kriminalitou. K této činnosti by měla přispět speciální informační síť provozovaná 24 hodin denně, sedm dní v týdnu zřízená mezi státy, které jsou stranami úmluvy (čl.35).

Poslední kapitola IV upravuje obvyklá závěrečná ustanovení jako vstup v platnost, přístup ke smlouvě, místní působnost a účinky smlouvy.

Celkově lze říci, že úmluva, pokud bude počet ratifikujících států dostatečně rozšířen, může významně přispět k efektivnímu stíhání a následně trestání internetové kriminality, neboť jednak sjednocuje náhled na trestnost určitých jednání spojených s internetem (potírá např. vznik tzv. internetových oáz, kde je páchána internetová kriminalita ve velkém) a dále zamezuje díky úpravě užší spolupráce mezi státy případům, kdy určité zjevně trestné jednání není sankcionováno proto, že se o něm ze zahraničí orgány činné v trestním řízení nedozví nebo je jim dokonce identita pachatele tajena.

Závěr

Internetová kriminalita je jevem poměrně novým, přesto však v žádném případě nelze říci, že vedle jiných typů kriminality je její význam zanedbatelný. S rostoucím rozvojem internetových technologií, elektronických způsobů komunikace a také s naší stoupající závislostí na těchto technických vymoženostech význam internetové kriminality roste takřka geometrickou řadou.

Internetová kriminalita je již také ovládána organizovaným zločinem, který díky charakteristickým atributům internetu jako je anonymita, masovost a minimální nákladnost může provádět a rozšiřovat svou nelegální činnost v dříve nemyslitelných rozměrech. Přesto však společností tento typ kriminality není pojímán jako výrazně nebezpečnější a není mu dávána taková pozornost, jakou by si zasloužil.

Jedním z důvodů, proč se veřejnost této kriminality příliš neobává, je její nemateriální (kybernetický) základ, který budí zdání, že se vlastně nic neděje, když to není v „reálném" světě. Opak je ovšem pravdou a internetovými trestnými činy je často způsobena škoda dosahující astronomických částek. Ochraně před internetovou kriminalitou by proto měla být věnována daleko vyšší pozornost a publicita. Jediný televizní spot upozorňující na porušování autorských práv stvrzuje poněkud žalostnou situaci v oblasti informování veřejnosti o internetové kriminalitě, obzvláště když se jednotlivá jednání spadající pod tento fenomén od sebe výrazně liší. Přitom dostatečná informovanost je nejúčinnějším nástrojem prevence, neboť drtivá většina trestněprávních jednání spojených s internetem těží z neznalosti, nepozornosti, popř. přehnané důvěry obětí.

S kybernetickou podstatou internetové kriminality souvisí i její další typický rys, a sice že samotní pachatelé nevnímají svou činnost jako příliš společensky škodlivou, vždyť přeci jen používají počítač a nikomu přímo neubližují. To je patrné zejména u porušování autorských práv, která ve společnosti nejsou příliš akceptována. Z toho důvodu by měla osvětová činnost upozorňovat na závažnost jednotlivých nelegálních aktivit spadajících pod internetovou kriminalitu a ukazovat, jaké škody mohou tyto aktivity způsobovat.

Co se týká trestněprávních aspektů, je internetová kriminalita charakteristická tím, že pokud ji nelze postihnout podle stávajících skutkových podstat, nelze ji dlouho trestat vůbec, neboť legislativa na kriminální jevy spojené s novými technologiemi reaguje často s velkým zpožděním. To je i případ české trestněprávní úpravy, která již několik let neúspěšně očekává modernizaci úpravy trestního práva hmotného, která by zohledňovala i nejnovější trendy na poli internetové kriminality.

Jiným problémem internetové kriminality bývá neexistence spolupráce mezi jednotlivými státy, kterých se internetová kriminalita v konkrétním případě týká. Pachatelé internetové kriminality jsou si totiž dobře vědomi rozdílů v právních úpravách států, kdy v jedné zemi je určité jednání trestné a v druhé nikoliv. Stejně tak si i dobře uvědomují absenci nebo chabou sílu mezinárodních norem upravujících spolupráci mezi státy, a tak využívají tzv. internetové ráje, tedy země, které (podobně jako v oblasti daní), jsou někdy k internetové kriminalitě až překvapivě shovívavé. Proto by měl být zesílen mezinárodní tlak na tyto státy, aby internetovou kriminalitu potíraly, popřípadě spolupracovaly na extradici pachatelů internetové kriminality. Před několika lety přijatá Úmluva o počítačové kriminalitě je prvním významným krokem v této oblasti, neboť zavádí systémy spolupráce v boji proti internetové kriminalitě. Je jen škoda, že počet států, které tuto smlouvu nejen podepsaly, ale i ratifikovaly, není vyšší.

Z toho hlediska je nepochopitelné, že mezi zeměmi, které tuto smlouvu doposud neratifikovaly, je i Česká republika.

Internetová kriminalita v současnosti stále prodělává bouřlivý vývoj a nelze očekávat, že by se na tomto směřování mělo v nejbližší době něco změnit. Kromě technických prostředků obrany by se proto nemělo zapomínat na prostředky osvětové (informační) a v neposlední řadě i prostředky právní.

Seznam literatury a jiných zdrojů informací

A. Seznam literatury

1.) Monografie, učebnice a komentáře:

1. Čermák J.: Internet a autorské právo. Linde Praha, a.s., Praha 2003
2. Čírtková, L.: Forenzní psychologie. Nakl. Aleš Čeněk, s.r.o., Plzeň 2004
3. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006
4. Jirovský, V.: Kybernetická kriminalita. Grada, Praha 2007
5. Matějka, M.: Počítačová kriminalita. Computer press, Praha 2002
6. Musil, S.: Počítačová kriminalita. IKSP, Praha 2000
7. Novotný, O., Dolenský, A., Jelínek, J., Vanduchová, M.: Trestní právo hmotné. I. Obecná část. 3. vydání. Codex, Praha 1997
8. Novotný, O., Vanduchová, M. a kol.: Trestní právo hmotné. I. Obecná část. 5. přepracované vydání. ASPI, a.s., Praha 2007
9. Novotný, O., Zapletal, J. a kol.: Kriminologie. 2. přepracované vydání. ASPI Publishing, Praha 2007
10. Šámal, P., Púry, F., Rizman, S.: Trestní zákon. Komentář. 6. vydání. C.H.Beck, Praha 2004
11. Telec, I.: Autorský zákon. Komentář. 1. vydání. C. H. Beck, Praha 1997
12. Wiener, N.: Kybernetika a společnost. Academia, Praha 1963

2.) Články v časopisech a sbornících:

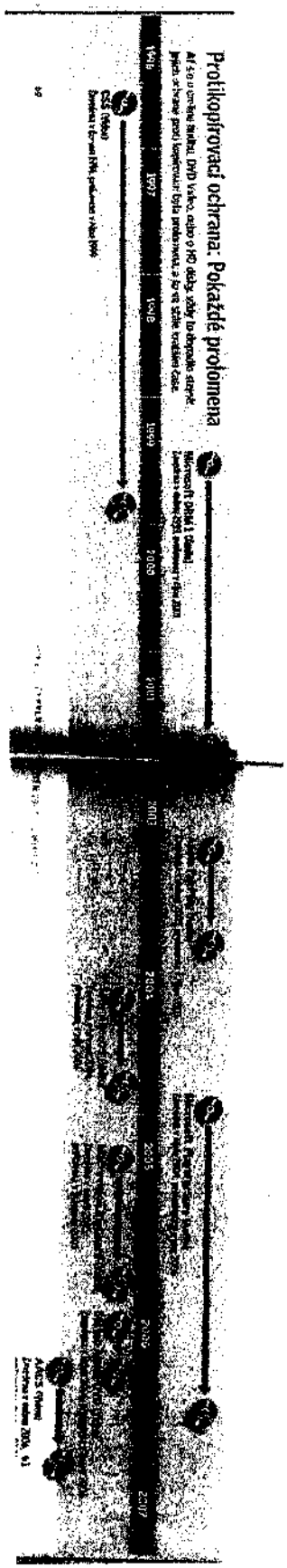
1. Adamski A.: Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI) v HEUNI's publication Series No. 34, 1998
2. autor@chip.cz, Internetové mafii na stopě, časopis CHIP.CZ, č. 1/2008, str. 157 a násl.
3. Baudiš, P.: Staronové nebezpečí Rhybaření, časopis CHIP.CZ, č. 4/2006, str. 14
4. Čepička, D., Arnold, A., Behrens, D.: Odhalte triky hackerů, časopis PC WORLD, č. 12/2007, str. 68 a násl.
5. Dastych, J.: Počítačová kriminalita – stručný přehled v Musil, S.: Počítačová kriminalita. IKSP, Praha 2000, příloha 2
6. Diamond, M., Uchiyama, A.: Pornography, Rape and Sex Crimes in Japan, International Journal of Law and Psychiatry 22(1): 1-22., 1999
7. Dolenský, A.: Pojem, povaha a stupeň nebezpečnosti činu pro společnost v Diferenciace trestní odpovědnosti, sborník, Univerzita Karlova, Praha 1983, str. 172
8. Jaishankar, K.: Cyber Criminology: Evolving a novel discipline with a new journal, International Journal of Cyber Criminology, Vol 1 Issue 1, Editorial, January 2007
9. Nádeníček, P.: Počítačové viry známé a neznámé. 1. díl Úvod do problematiky & souborové viry, časopis PC WORLD, č. 11/2005
10. Nádeníček,P.: Počítačové viry známé a neznámé. 2. díl E-mailový červ, starý dobrý známý, časopis PC WORLD, č. 1/2006

11. Nádeníček, P.: Počítačové viry známé a neznámé. 3. díl Síťový červ – zatraceně rychlý chlapík, časopis PC WORLD, č. 2/2006
12. Nádeníček, P.: Počítačové viry známé a neznámé. 5. díl Trojský kůň: schopný podvodník schopný všeho, časopis PC WORLD, č. 4/2006
13. Přibyl, T.: Causa rootkit, časopis PC WORLD, č. 3/2006, str. 52 a násl.
14. Přibyl, T.: Druhý dech trojských koní, časopis PC WORLD, č. 2/2008, str. 110 a násl.
15. Redakce, časopis CHIP.CZ, č. 2/2006, str. 16
16. Záh, S.: Nesahejte na to! Vše o nebezpečí, které na vás číhá na internetu, časopis PC WORLD, č. 10/2006
17. Zpráva společnosti McAfee o internetové kriminalitě, časopis CHIP.CZ, č. 5/2007, str. 16 a násl.

B. Internetové zdroje:

1. Bude podle navrhované novely trestního zákona věda (kryptoanalýza) trestná?, http://www.itpravo.cz/index.shtml?x=694071, zobrazeno 9.6.2008, 20:14
2. http://blog.jancermak.cz/phishing-ceska-sporitelna-sbirka-nejpopularnejsiho-spam-phishingu-poslednich-dni/2008/03/19/, zobrazeno 17.6.2008, 16:23
3. http://www.cpufilm.cz/rozsudky.html, zobrazeno 31.7.2008, 16.40
4. http://www.ncmec.org/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2064 "CHILD PORN AMONG FASTEST GROWING INTERNET BUSINESSES". National Center for Missing and Exploited Children, USA (2005-08-05). Zobrazeno 19.6.2008, 19:18
5. http://www.novinky.cz/clanek/93889-pocitacovi-pirati-uz-obrali-banky-o-stovky-milionu.html, zobrazeno 15.7.2008, 13:05
6. http://www.parade.com/articles/editions/2006/edition_02-19-2006/Andrew_Vachss, zobrazeno 19.6.2008, 20:15
7. http://www.snopes.com/crime/fraud/nigeria.asp, zobrazeno 21.7.2008, 13:40
8. https://akela.mendelu.cz/~lidak/bis/seminar2004/seminarky/makovsky.doc., zobrazeno: 15.7.2008, 16:40
9. Matejka Ján, Čermák Jiří: Odpovědnost poskytovatelů volného prostoru na Internetu za cizí obsah, www.itpravo.cz, zobrazeno 19.7.2000, 13:25
10. Watson Business Systems Ltd: A Guide To Computer Crime - An Introduction To Computer Crime and Internet Fraud, http://legal.practitioner.com/computer-crime/, zobrazeno 20.6.2008, 16:22
11. Wikipedia; http://en.wikipedia.org
12. World Internet Usage Statistics News and Population Stats, http://www.internetworldstats.com/stats.htm, zobrazeno 20.7.2008, 14:50

Příloha č. 1 – Prolamování softwarových účinných prostředků ochrany autorských práv v časové ose (převzato z časopisu CHIP.CZ, č. 6/2007):



Příloha č. 2 – Rozsudek Okresního soudu ve Znojmě ("obalycd.cz") ze dne 24.7.2002 ve věci trestného činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 tr. zákona:

ČESKÁ REPUBLIKA

ROZSUDEK JMÉNEM REPUBLIKY

Okresní soud ve Znojmě rozhodl v hlavním líčení konaném dne 24.července 2002 samosoudcem

takto :

Obžalovaný

R. D.

je vinen, že

od 23.1.2001 do 10.8.2001 v O. okres Znojmo i jinde na internetové adrese www.obalycd.cz nabízel bez souhlasu vlastníků práv k bezplatnému poskytování rozmnoženiny projiné než vlastní užití ke stažení doprovodné grafické materiály, booklety a traye, které jsou ve své původní podobě součástí vydaných nosičů zvukových záznamů, čímž porušil § 12 odst. 1 zákona č. 121/2000 Sb. (autorského zákona), tedy porušil právo na sdělování díla veřejnosti dle § 12 odst. 4 písm. f) ve spojení s § 18 odst. 2 téhož zákona,

tedy — neoprávněně zasáhl do zákonem chráněných práv k autorskému dílu,

tím spáchal

trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 tr. zákona

a odsuzuje se

podle § 152 odst. 1 tr.zákona k trestu **odnětí svobody v trvání 4 (čtyř) měsíců.**

Podle § 58 odst. 1 tr. zákona a § 59 odst. 1 tr. zákona se výkon trestu **podmíněně odkládá na zkušební dobu v trvání 18-ti (osmnácti) měsíců.**

Odůvodnění:

Po provedeném hlavním líčení a dokazování vzal soud za prokázaný tento skutkový stav:

Obžalovaný provozoval v období od 23.1.2001 do 10.8.2001 internetové stránky na adrese www.obalycd.cz, které umístil na serveru PES.CZ, jehož provozovatelem je společnost P.E.S. consulting s.r.o. Na svých stránkách, do kterých měl vstup pouze on, nabízel bez souhlasu vlastníků práv k bezplatnému poskytování rozmnoženiny pro jiné než vlastní užití ke stažení doprovodné grafické materiály, booklety a traye, které na stránky zasílaly jiné

osoby, přičemž k zařazování docházelo automaticky pomocí obžalovaným vytvořeného skriptu, kdy grafické materiály jsou ve své původní podobě součástí vydaných nosičů zvukových záznamů, čímž porušil § 12 odst. 1 zákona č. 121/2000 Sb. (autorského zákona), tedy porušil právo na sdělování díla veřejnosti dle § 12 odst. 4 písm. f) ve spojení s § 18 odst. 2 téhož zákona.

Obžalovaný se necítil být vinen. V rámci posledního slova uvedl, že všeho lituje, stránky vytvořil proto, aby se zdokonalil ve svém oboru. Nevěděl, že grafické ztvárnění obalů, které zasílaly jiné osoby, jsou kopiemi původních originálů. Nevěděl, že by mohl porušovat autorský zákon. Některé obaly, pokud si myslel, že by nemusely být v pořádku, odstranil. Stránky odstranil ihned, jak se o věc začala zajímat policie. Žádný obal do stránek neumísťoval ze své mailové adresy.

Z výpovědi obžalovaného, úředního záznamu Kriminálního úřadu Policejního prezidia ČR z 24.5.2001 a 6.2.2002 je nepochybné, že obžalovaný provozoval v období od 23.1.2001 do 10.8.2001 internetové stránky na adrese www.obalycd.cz, které umístil na serveru PES.CZ, jehož provozovatelem je společnost P.E.S. consulting s.r.o. Ta mu umožnila provoz svých stránek zadarmo. Na těchto stránkách byly mimo jiné nabízeny ke stažení doprovodné grafické materiály, booklety a traye, které jsou ve své původní podobě součástí vydaných nosičů zvukových záznamů, tedy jedná se o kopie originálních obalů, což vyplývá z označení ©, čárových kódů, firmy, k čemuž se vyjádřil svědek V., jenž měl k dispozici vytištěné stránky založené ve spisu na čl. 10-36, které byly pořízeny ze zálohovaných stránek (vyjádřila též svědkyně K.), přičemž CD na nichž je záloha uložena je též součástí spisového materiálu. O charakteru kopií obalů vypovídá i zpráva Mezinárodní federace fonografického průmyslu z 17.4.2001. Zní též vyplývá, že obžalovaný neměl souhlas autorů děl k jejich šíření, k užití díla. Svědkyně K. potvrdila verzi obžalovaného v tom, že je možné, aby na stránky byly zasílané obaly umísťovány automaticky. Nemuselo dojít k ručnímu umísťování, což se nepodařilo prokázat žádným předloženým důkazem. Již nelze zjistit, jak stránky ve skutečnosti pracovaly, neboť skript byl již vymazán. Z vytištěného obsahu stránek, jakož i výpovědi obžalovaného dále soud zjistil, že tento obsah stránek kontroloval, měl přehled o jejich obsahu, tedy i o existenci zasílaných obalů a jejich provedení. Z výpovědi svědkyně K. též bylo zjištěno, že internet je mezinárodní sítí, kdy přístup na ni je kdykoliv možný, pokud je internetové připojení, lze nalézt a stáhnou cokoliv možného. Pro zřízení domény (stránek) je nutné mít vlastní server, nebo využít volný prostor na jiných serverech (zjištěno - PES.CZ).

Obžaloba vinila obžalovaného z toho, že neoprávněně zasáhl do zákonem chráněných práv k zvukovému záznamu. Dle § 75 odst. 1 zákona č. 121/2000 Sb. (autorský zákon) je zvukový záznam výlučně sluchem vnímatelný záznam zvuků výkonu výkonného umělce či jiných zvuků, nebo jejich vyjádření. Soud je toho názoru, že na stránkách byly publikovány kopie obalů, které jsou ve své původní podobě součástí vydaných nosičů zvukových záznamů. Na ně je třeba pohlížet jako na dílo dle § 2 odst. 1 autorského zákona (dílo vytvořené postupem podobným fotografii, grafické).

Nebyl tedy dán souhlas autora k šíření, užití díla dle § 12 odst. 1 autorského zákona, kdy není dán případ pro užití bez svolení. Bylo porušeno ust. § 12 odst. 4 písm. f) autorského zákona, právo na sdělování díla veřejnosti. Dle § 18 odst. 2 autorského zákona se sdělováním rozumí zpřístupňování díla způsobem, že kdokoli může mít k němu přístup na místě a v čase podle své vlastní volby zejména počítačovou nebo obdobnou sítí, což je v

daném případě. Dle odstavce 3 téhož ustanovení se za sdělování nepovažuje pouhé provozování zařízení umožňujícího nebo zajišťujícího takové sdělování. V daném případě obžalovaný neprovozoval takové zařízení, neboť tímto byl server společnosti P.E.S. consulting s.r.o. Tvrzení obžalovaného, že kopie obalů na stránky neumísťoval, není relevantní, neboť tím, že vytvořil stránky právě za účelem výměny, publikace a s jeho vědomím mohly další osoby zasílat právě i kopie původních originálů, díla užíval a šířil.

Ustanovení § 152 odst. 1 tr. zákona je trestněprávní normou s blanketní dispozicí a odkazuje na ustanovení autorského zákona (použitá ustanovení jsou uvedena výše). Pokud obžalovaný uváděl, že nevěděl, že se jedná o kopie originálních obalů, že porušuje autorský zákon, je třeba uvést, že jeho případný omyl jej neomlouvá, neboť ten je třeba posuzovat jako omyl právní a neznalost trestního zákona a norem blanketních neomlouvá. Obžalovaný jednal úmyslně dle § 4 písm. b) tr. zákona, neboť musel vědět, zajímá se o informační technologie, nežije ve vzduchoprázdnu, problematika nelegálního kopírování je všeobecně známa, že porušuje právě autorská práva a s tímto byl srozuměn. Po stránce subjektivní i objektivní naplnil zákonné znaky skutkové podstaty trestného činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 tr. zákona.

Při úvaze o tom, jak obžalovaného za jeho jednání potrestat vzal soud v úvahu společenskou nebezpečnost jednání pro společnost, míru zavinění, způsob provedení, následek, možnost nápravy a poměry obžalovaného. Porušování autorských práv je aktuálním společenským problémem. Bylo však nutno přihlédnout ke zprávě Obecního úřadu O., že se jedná o řádně se chovajícího občana, taktéž dle opisu rejstříku trestů nebyl doposud soudně trestán. (§33 písm. g), h) tr. zákona). Taktéž hodnotící zpráva zaměstnavatele je pro obžalovaného velice kladná, je zařazen jako systémový inženýr, správce aplikace, administrátor výpočetních systémů, jeho práce je pro něj i koníčkem. Škoda nebyla stanovena. Soud dospěl k závěru, že účelu trestu a nápravy obžalovaného bude dosaženo uložením podmíněného tretu odnětí svobody v 1/6 rozpětí zákonné trestní sazby s odkladem též na kratší zkušební dobu, v které prokáže, zda je schopen dodržovat pravidla, která mimo jiné upravují i respektování duševního vlastnictví.

POUČENÍ: Proti tomuto rozsudku lze podat odvolání do 8 dnů od doručení opisu rozsudku ke Krajskému soudu v Brně, prostřednictvím soudu podepsaného. Rozsudek může odvoláním napadnout státní zástupce pro nesprávnost kteréhokoli výroku, obžalovaný pro nesprávnost výroku, který se ho přímo dotýká, zúčastněná osoba pro nesprávnost výroku o zabrání věci, poškozený, který uplatnil nárok na náhradu škody, pro nesprávnost výroku o náhradě škody, přičemž osoba oprávněná napadat rozsudek pro nesprávnost některého jeho výroku může jej napadat také proto, že takový výrok učiněn nebyl, jakož i pro porušení ustanovení o řízení předcházejícím rozsudku, jestliže toto porušení mohlo způsobit, že výrok je nesprávný nebo že chybí. Ve prospěch obžalovaného mohou rozsudek odvoláním napadnout i osoby uvedené v § 247 odst. 2 tr. řádu. Ve výše uvedené lhůtě musí být odvolání také odůvodněno tak, aby bylo patrno, v kterých výrocích je rozsudek napadán a jaké vady jsou vytýkány rozsudku nebo řízení, které rozsudku předcházelo, dále je třeba je podepsat a datovat. Odvolání je třeba předložit v takovém počtu stejnopisů a příloh, aby jeden stejnopis zůstal u soudu a aby každá osoba dotčená takovým podáním (ostatní strany) dostala jeden stejnopis. Státní zástupce je povinen v odvolání uvést, zda je podává, byť i

zčásti, ve prospěch nebo v neprospěch obviněného. Odvolání lze opřít o nové skutečnosti a důkazy.

Okresní soud ve Znojmě dne 24. července 2002

Zdroj: http://www.itpravo.cz/index.shtml?x=102705, zobrazeno 25.6.2008, 16:34

Příloha č. 3 – Oznámení Úřadu obchodního zmocněnce USA (USTR - Office of the United States Trade Representative) o opětovném umístění České republiky na tzv. Special 301 Watch List.

USTR Announces Results of Out-of-Cycle Review for the Czech Republic 01/22/2008

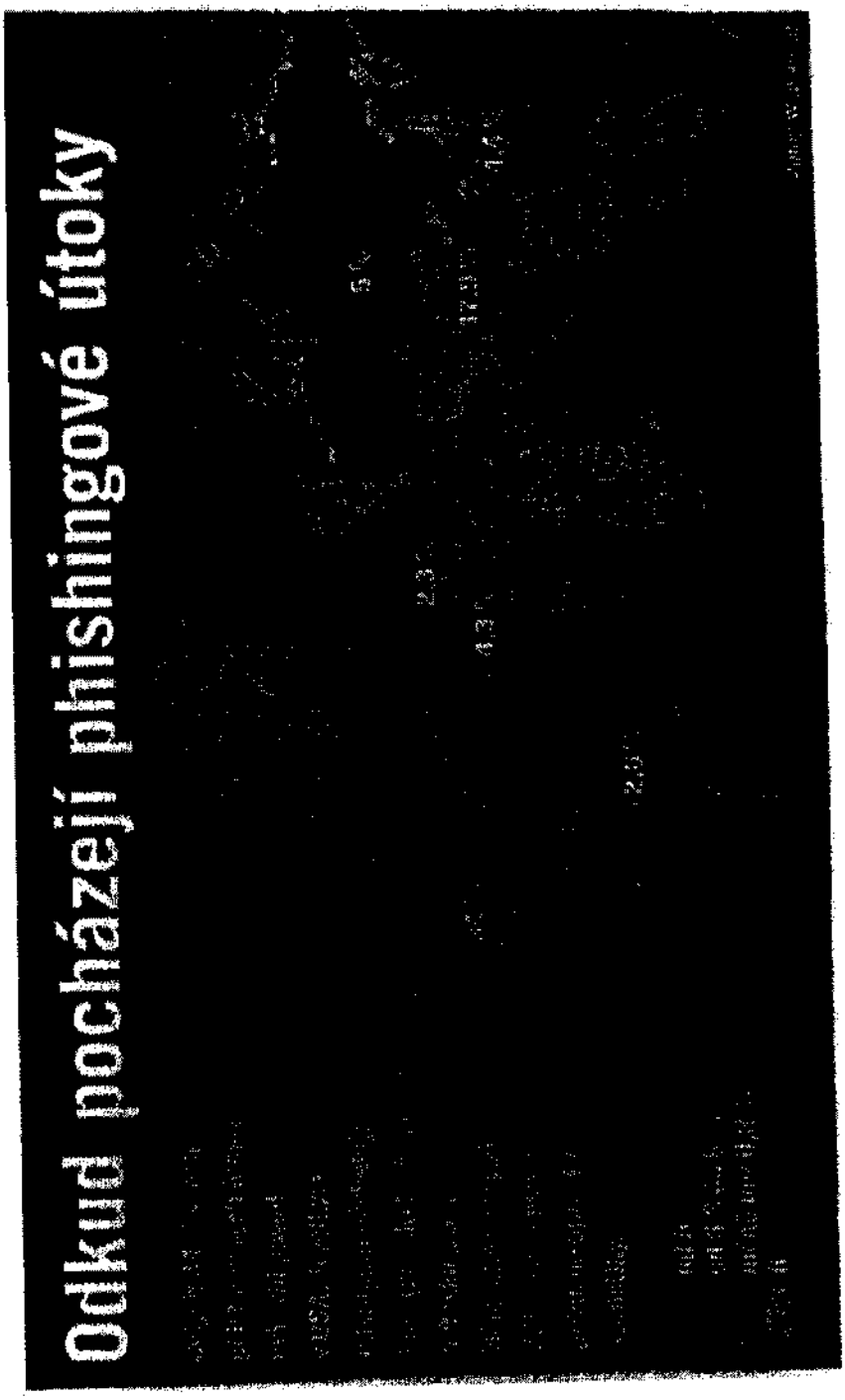
Washington, D.C. - U.S. Trade Representative Susan C. Schwab today announced the results of USTR's Out-of-Cycle Review of intellectual property rights (IPR) protection and enforcement in the Czech Republic under the "Special 301" provisions of U.S. trade law. As a result of the review, the Czech Republic will be placed on the Special 301 Watch List.

"We remain concerned at the continuing lack of effective enforcement measures against traders openly selling pirated and counterfeit goods in the notorious border markets," said Ambassador Schwab. "Intellectual property rights are critical to the continued growth of our economy, and we will vigorously press our trading partners to follow and enforce the rules to protect American creativity, innovation and technology. We are encouraged that the Czech Republic has started developing legal and enforcement measures to address long-standing concerns over piracy and counterfeiting, and look forward to continuing to work with the Czech Republic to achieve concrete results in IPR enforcement, both bilaterally and globally."

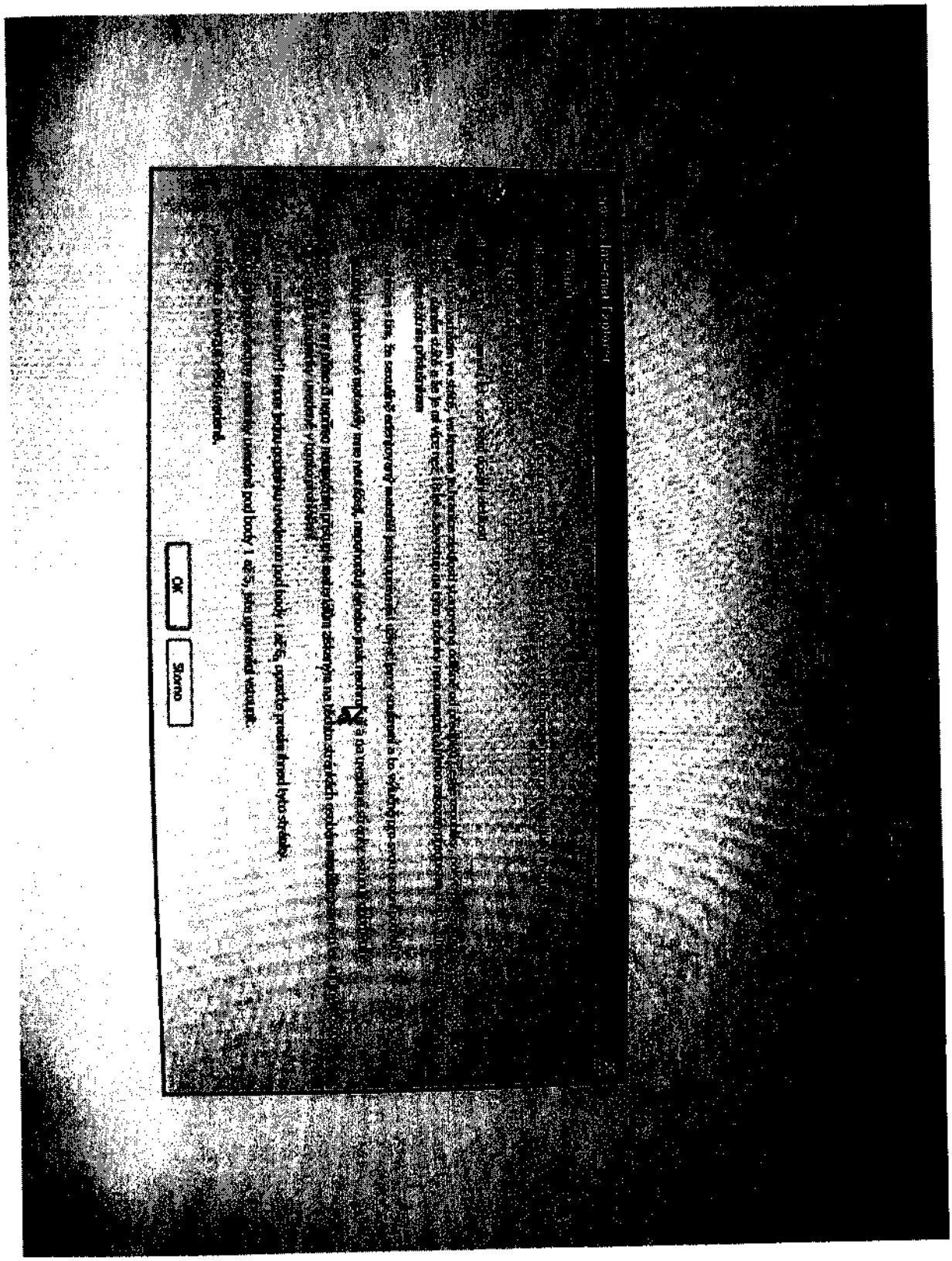
The Czech Republic was not included on the Watch List or the Priority Watch List in the 2007 Special 301 Report, released in April 2007, but USTR announced that it would conduct an Out-of-Cycle Review to monitor progress in addressing concerns regarding the lack of adequate protection and enforcement of intellectual property in the Czech Republic, especially with respect to sales of pirated and counterfeit goods in its notorious markets.

Zdoj:
http://www.ustr.gov/Document_Library/Press_Releases/2008/January/USTR_Announces_Results_of_Out-of-Cycle_Review_for_the_Czech_Republic.html?ht=, zobrazeno 8.7.2008, 17:28

Příloha č. 4 - Zobrazení celosvětového rozložení phishingových útoků z hlediska původce v roce 2006 (převzato z časopisu CHIP.CZ, č. 5/2006)



Příloha č. 5 – Ukázka oznámení před vstupem na stránky obsahující pornografický materiál



Zdroj: http://www.freevideo.cz, zobrazeno 4.7.2008, 21:43